CENTRO UNIVERSITÁRIO DE BRASÍLIA – UniCEUB
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS – FAJS
PROGRAMA DE MESTRADO EM DIREITO

BRUNO LUNARDI GONÇALVES

O DIREITO À PROTEÇÃO DE DADOS NA ERA DA HIPERCONEXÃO: UMA ANÁLISE EMPÍRICA DOS TERMOS DE USO E DE PRIVACIDADE DOS APLICATIVOS DE CELULAR

BRASÍLIA
2021

CENTRO UNIVERSITÁRIO DE BRASÍLIA – UniCEUB
FACULDADE DE CIÊNCIAS JURÍDICAS E SOCIAIS – FAJS
PROGRAMA DE MESTRADO EM DIREITO

BRUNO LUNARDI GONÇALVES

O DIREITO À PROTEÇÃO DE DADOS NA ERA DA HIPERCONEXÃO: UMA ANÁLISE EMPÍRICA DOS TERMOS DE USO E DE PRIVACIDADE DOS APLICATIVOS DE CELULAR

Dissertação apresentada como requisito para a obtenção do título de Mestre em Direito – Área de Concentração 2 (Políticas Públicas, Relações Privadas e Desenvolvimento), Linha de Pesquisa I (Políticas Públicas, Sociedade Civil e Proteção da Pessoa) do Programa de Pós-Graduação *Stricto Sensu* do Centro Universitário de Brasília (UniCEUB).
Orientador: Prof. Dr. Leonardo Roscoe Bessa.

BRASÍLIA
2021

BRUNO LUNARDI GONÇALVES

O DIREITO À PROTEÇÃO DE DADOS NA ERA DA HIPERCONEXÃO: UMA ANÁLISE EMPÍRICA DOS TERMOS DE USO E DE PRIVACIDADE DOS APLICATIVOS DE CELULAR

Dissertação apresentada como requisito para a obtenção do título de Mestre em Direito – Área de Concentração 2 (Políticas Públicas, Relações Privadas e Desenvolvimento), Linha de Pesquisa I (Políticas Públicas, Sociedade Civil e Proteção da Pessoa) do Programa de Pós-Graduação *Stricto Sensu* do Centro Universitário de Brasília (UniCEUB).

Brasília/DF, 23 de junho de 2021

Banca Examinadora

_____

Prof. Dr. Leonardo Roscoe Bessa
Orientador

_____

Prof. Dr. Paulo Afonso Cavichioli Carmona
Examinador Interno

_____

Prof.ª Dra. Amanda Flávio de Oliveira
Examinador Externo

AGRADECIMENTOS

Meus agradecimentos são a todos que, direta ou indiretamente, contribuíram de alguma forma com meu aprendizado durante a trajetória pelo Mestrado. Primeiramente, a Deus, por tudo o que Ele tem fornecido à minha vida.

*Seguindo-se, talvez as mais importantes contribuições tenham vindo do sustentáculo oferecido por meus pais, Maria Helena e Cristiano, e pela minha esposa, Izabella – com quem hoje compartilho a rotina acadêmica e, em tempos pandêmicos, a profissional; e espero compartilhar pelo resto da vida –, que sempre auxiliaram a passar por todos os desafios do curso. E não foram poucos os desafios: embora o período mais recente da pandemia até tenha sido de menor carga laboral, conciliar os estudos acadêmicos com o gabinete do Senador Randolfe, que trabalha quase 16 horas por dia, não é tão fácil. Não menos importantes, agradeço ao Sr. Luiz (*in memorian*) e à Sra. Cirlei, que, já no início de minha infância, contribuíram, com seu carinho e amor de avós, significativamente para que eu me tornasse o que sou hoje.*

Agradeço a todos os meus colegas do Senado Federal, que sempre foram muito compreensivos e ajudaram em alguns debates jurídicos. Ademais, e em especial, agradeço ao Professor Leonardo, pelas oportunidades e confiança em meu trabalho. Embora, pelas restrições de horário, não tenhamos tido a oportunidade de nos conhecer ao longo do curso, acabamos nos conhecendo agora no final e o vínculo foi bastante bom. Autoridade em matéria de proteção de dados pessoais como é, não era esperado nada menos do que uma contribuição enorme ao melhoramento do texto. Também agradeço aos Professores Paulo Carmona e Amanda Flávio, que, ainda na banca de qualificação, deram valiosas sugestões para o necessário aprimoramento do trabalho. Agradeço, por fim, ao Professor e Desembargador Néviton Guedes, que me deu o impulso que faltava para iniciar a carreira jurídica e, naquele voto do julgamento da minha apelação, tornou o hoje possível.

"*A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais [na União] e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais*".

(Considerando nº 6, Regulamento Geral sobre a Proteção de Dados da Europa)

Assim como o exigir que automóveis sejam providos de freios, airbags e espelhos retrovisores não significa criar obstáculos para a indústria automobilística, o exigir que normas que envolvam direitos fundamentais e da personalidade observem requisitos mínimos de adequação constitucional tampouco pode ser lido como embaraço à atividade estatal.

(Voto da Ministra Rosa Weber no julgamento da ADI-MC 6.387/DF)

RESUMO

O presente trabalho tem o objetivo nuclear de avaliar as políticas de privacidade dos principais aplicativos utilizados em dispositivos móveis, ou seja, trata-se de uma pesquisa eminentemente empírica de leitura e aferição das principais cláusulas dispostas nas *políticas de privacidade*. Antes de se passar à prática, fez-se uma breve análise teórica dos institutos jurídicos envolvidos, passando pelo conceito do direito fundamental à privacidade e à proteção dos dados pessoais, grau de disponibilidade dos direitos da personalidade, aspectos atinentes ao direito contratual e ao próprio direito do consumidor, na medida em que as políticas de privacidade nada mais são do que verdadeiros contratos de adesão. Também se fez um breve panorama sobre a legislação específica aplicável ao direito na internet: LGPD, MCI, CDC e RGPD. Na sequência, foram selecionados 157 aplicativos, divididos em 12 categorias com alguma homogeneidade. Tendo isso como base, passou-se à análise efetiva das políticas de privacidade dos aplicativos móveis, que se deu em três etapas: (i) aferição de como se dá o consentimento e a possibilidade de sua revogação pelo usuário, bem como a expressão do legítimo interesse para o tratamento dos dados; (ii) análise crítica das permissões solicitadas por cada aplicativo móvel analisado e a sua real aderência à funcionalidade ordinária do *software*; e (iii) leitura efetiva e apontamento das cláusulas mais interessantes e curiosas de todas as políticas de privacidade dos 157 aplicativos. Os resultados encontrados demonstram que a maioria das empresas ainda não trocou o *mindset* para a política de *privacy by design*, inclusive os aplicativos governamentais. Ao final, desenvolveu-se brevemente o conceito de níveis de aplicativos, que pode ser uma possível solução apta a equacionar todos os legítimos interesses em jogo: o da privacidade dos usuários e a liberdade econômica das empresas, que prestam serviços essenciais no mundo hiperconectado atual.

Palavras-chave: Aplicativos móveis. Políticas de privacidade. Consentimento e revogação. Interesse legítimo. Permissões. Proteção de dados. Transparência.

ABSTRACT

The present work has the core objective of evaluating the privacy policies of the main applications used in mobile devices, that is, it is an eminently empirical research of reading and gauging the main clauses arranged in the privacy policies. Before being put into practice, a brief theoretical analysis was made of the legal institutes involved, going through the concept of the fundamental right to privacy and personal data protection, degree and level of availability of personality rights, aspects related to contractual law and to consumer law, since the privacy policies are no more than truly contracts of accession. A brief overview was also made of the specific legislation applicable to Internet law: LGPD, MCI, CDC and RGPD. In the sequence, 157 applications were selected, divided into 12 categories with some homogeneity. Based on this, I proceeded to the effective analysis of the privacy policies of the mobile applications, which took place in three stages: (i) gauging how consent is given and the possibility of its revocation by the user, as well as the expression of the legitimate interest for the data treatment; (ii) critical analysis of the permissions requested by each analyzed mobile application and its actual adherence to the ordinary functionality of the software; and (iii) effective reading and annotation of the most interesting and curious clauses of all 157 privacy policies. The results show that most companies have not yet switched from mindset to privacy by design policy, including government applications. In the end, the concept of application levels was briefly developed, which may be a possible solution for balancing all the legitimate interests at stake: the privacy of users and the economic freedom of companies, which provide essential services in today's hyperconnected world.

Keywords: Mobile applications. Privacy Policy. Consent and its withdrawing. Legitimate interest. Permissions. Data protection. Transparency.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
App	Aplicativo de celular
ART	Artigo
CC	Código Civil (Lei nº 10.406, de 10 de janeiro de 2002)
CPF	Cadastro de Pessoas Físicas
CRFB/88	Constituição da República Federativa do Brasil de 1988
IoT	Internet das Coisas (Internet of Things)
LAI	Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011)
LGPD	Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018)
MCI	Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014)
RGPD	Regulamento Geral de Proteção de Dados nº 679/2016 da União Europeia
STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal

1 INTRODUÇÃO

Há quem diga que a privacidade hoje é ilusória[1,2] ou ficta. Outros afirmam que os dados superaram o petróleo como o recurso mais valioso do mundo[3], o que pode ser bom[4]. A preocupação com a privacidade, em verdade, não é propriamente nova. Há muito se discutem as interferências do desenvolvimento tecnológico na vida privada das pessoas – câmeras, gravadores, televisores, computadores, celulares, dispositivos inteligentes e conectados à internet, dentre outros. Seriam as novas teletelas de Orwell? Há quem diga que são os "pequenos irmãos"[5] ou que se vive em uma nova religião: o dataísmo[6].

O medo do novo, desconhecido, sempre permeou os seios sociais. Em verdade, todos os principais inventos da história que, de modo amplo, *facilitaram* a realização de tarefas e estreitaram laços e comunicações – motores, aviões, barcos, prensa, papel – acabaram por estreitar o espectro de manifestação da privacidade dos indivíduos. Movimentos colonizadores do passado, em última análise, ao implicarem as restrições de manifestações sociais e culturais aos colonizados, também lhes diminuíram a amplitude da então vida privada, em sua manifestação de direito de ser deixado só. No ápice do regresso, é de se dizer que, quando o humano empreendeu sua primeira relação social com outrem, por necessidade de sua própria natureza[7], abriu mão de parte da sua privacidade em troca do convívio em sociedade. Sendo o humano um ser social por natureza, certamente tem convivido, em alguma medida, com restrições à sua privacidade há mais de 300 mil anos, que é de quando data o *homo sapiens*[8].

Elucubrações acerca de compressões da privacidade humana à parte, é fato que a atual sociedade, da informação, da hiperconexão e da comunicação em massa, vivencia um

---

[1] ESTADÃO. 'A privacidade na web é uma ilusão'. Disponível em: <https://link.estadao.com.br/noticias/geral,a-privacidade-na-web-e-uma-ilusao,10000032646>. Acesso em: 26 mar. 2021.

[2] US NEWS. The Illusion of Online Privacy. Disponível em: <https://www.usnews.com/news/articles/2015/08/25/the-illusion-of-online-privacy>. Acesso em: 26 mar. 2021.

[3] THE ECONOMIST. The world's most valuable resource is no longer oil, but data. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 26 mar. 2021.

[4] FORBES. Data Is The New Oil -- And That's A Good Thing. Disponível em: <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=614ec1817304>. Acesso em: 26 mar. 2021.

[5] RAMOS, André de Carvalho. O pequeno irmão que nos observa: os direitos dos consumidores e os bancos de dados no Brasil. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). *Coleção doutrinas essenciais*: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v.3, p.957-974.

[6] HARARI, Yuval Noah. Homo Deus: uma breve história do amanhã (edição eletrônica). São Paulo: Companhia das Letras, 2016.

[7] DALLARI, Dalmo de Abreu. Viver em Sociedade. Frutal-MG: Prospectiva. 2ª Edição, 2014, p. 13.

[8] FAPESP. Mais velho Homo sapiens, de 300 mil anos, é encontrado no Marrocos. Disponível em: <https://revistapesquisa.fapesp.br/mais-velho-homo-sapiens-de-300-mil-anos-e-encontrado-no-marrocos/>. Acesso em: 26 mar. 2021.

paradigma de tensão à privacidade sem precedentes. É inegável que as diversas ferramentas tecnológicas hoje à mão de bilhões de pessoas ao redor do mundo facilitam boa parte das atividades – o que é especialmente visível no cenário pandêmico vivido nos últimos meses –, mas o preço cobrado é compatível com, senão maior do que, o benefício.

Fala-se isso porque hoje se vive o paradigma da datificação[9] das vidas, o que nada mais é do que descrever a pessoa por meio de dados pessoais. Tal fato é possível dada a característica de ubiquidade[10] da internet: a conexão à internet é disponível em praticamente todos os lugares e a todo momento, sobretudo com os celulares, havendo uma verdadeira "onipresença do ambiente virtual"[11]. A tendência é que o nível de conectividade aumente ainda mais quando a IoT estiver efetivamente à disposição da maioria dos usuários, com suas geladeiras, despertadores, roupas, automóveis e afins inteligentes e conectados entre si por sistemas de radiofrequência[12].

Nessa esteira, é premente que se consiga regular os parâmetros para a privacidade e a proteção de dados no atual cenário de conexão massificada e ubíqua no presente, e de modo urgente, para que o universo da datificação não se aprofunde ainda mais sem que o Direito consiga estabelecer uma solução sólida, fática e juridicamente, capaz de também ser aplicável, com os ajustes contextuais necessários, ao porvir. Afinal, como aponta Ana Frazão, "a economia movida a dados e o capitalismo de vigilância são as duas faces da mesma moeda pois, quanto maior a importância dos dados, mais incentivos haverá para o aumento da vigilância e, por conseguinte, maior será a coleta de dados"[13].

O próprio STF, aliás, reconheceu, ainda na década de 1990, que "a convivência entre a proteção da privacidade e os chamados arquivos de consumo, mantidos pelo próprio fornecedor de crédito ou integrados em bancos de dados, tornou-se um imperativo da economia da sociedade de massas"[14]. Ou seja, não é de hoje a preocupação de como conciliar privacidade e proteção de dados pessoais com as necessidades econômicas hodiernas.

---

[9] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. Big Data: A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013, p. 91.

[10] ANDRADE, Norberto Nuno Gomes de Andrade. The right privacy and the right to identity in the Age of ubiquitous computing: Friends or foes? A proposal towards a legal articulation. In: AKRIVOPOLOUS, Christina; PSYGKAS, Athanasious (Org.). Personal data privacy and protection in a surveillance era: technologies and practices. New York: Information Science Reference, 2011. p. 20.

[11] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[12] WEBER, Rof H. Internet of Things – New security and privacy challenges, p.23.

[13] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[14] BRASIL. Supremo Tribunal Federal. ADI 1790-MC/DF. Rel. Min. Sepúlveda Pertence. Tribunal Pleno.

Sustenta-se tal posição na medida em que, se com o atual cenário de datificação – massiva, mas não tão profusa quanto pode vir a ser –, já se cogita de que dados pessoais coletados em funcionalidades do *Facebook*, e devidamente tratados por outra empresa, parceira comercial especializada no assunto, tenham influenciado fortemente os resultados de importantes participações democráticas ao redor do globo – o *sim* no Brexit, a eleição de Trump nos Estados Unidos[15] e inúmeras eleições de outros líderes nacionais em países em desenvolvimento[16] –, o futuro parece ainda mais preocupante. Afinal, a descrição do filme *The Great Hack*, produzido pela *Netflix* em 2019, parece aderente à atual realidade: "*they took your data, then they took control*" ("eles pegaram seus dados, então eles assumiram o controle")[17].

Tendo tudo isso em mente, a presente pesquisa tem como problema central a seguinte questão: os softwares (aplicativos) rotineiramente usados em dispositivos celulares, nos seus mais variados gêneros de funcionalidades, foram concebidos de modo adequado à tutela da privacidade legal e constitucionalmente estabelecida, principalmente no que toca ao requisito do consentimento válido e do legítimo interesse na perspectiva da boa-fé objetiva para a coleta e tratamento de dados?

Referido problema geral pode ter inúmeros desdobramentos naturais, que também são pontualmente analisados no presente trabalho: liberdade contratual nos termos de uso e políticas de privacidade à luz da dinâmica do direito do consumidor e da função social do contrato, dignidade da pessoa humana como o vetor último dos direitos fundamentais à privacidade e à proteção de dados pessoais, autorregulação e heterorregulação da internet, equacionamento entre a liberdade econômica e o resguardo à privacidade, eventual concepção de níveis de aplicativos como um acréscimo necessário ao consentimento granular (gradientes de funcionalidade ocupando o espaço do binarismo tradicional no mercado: ou funciona tudo, ou nada funciona), funcionamento de aplicativos governamentais ou oficiais.

Tudo isso para se chegar à finalidade de avaliar em que medida poderia ser aprimorada a transparência dos termos de privacidade das aplicações para fins de um maior conhecimento das finalidades à que utilizados os dados coletados dos usuários. Ou seja, busca-se aferir a real aderência das políticas de privacidade dos aplicativos mais comuns no Brasil às

---

Julgamento em 23/4/1998, publicação em 8/9/2000.

[15] BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 26 mar. 2021.

[16] THE GUARDIAN. Former Cambridge Analytica exec says she wants lies to stop. Disponível em: <https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies>. Acesso em: 26 mar. 2021.

[17] Para uma narrativa jornalística completa e fluida sobre o tema, recomenda-se o documentário *The Great Hack*, produzido pela Netflix em 2019.

balizas jurídicas sobre a tutela da proteção de dados, da privacidade e da autodeterminação informativa.

Dessa forma, a hipótese inicial que se coloca à prova na presente pesquisa é de que os aplicativos de celulares não protegem adequadamente os dados dos seus usuários, seja por meio do uso massivo de dados pessoais, sensíveis ou não, seja por meio da falta de transparência às pessoas, que não entendem o que está sendo coletado, para onde as informações vão, qual é a utilidade ou como impedir que aquilo se dê daquela forma.

A hipótese inicial de pesquisa também comporta uma série de testes subsidiários, devidamente colocados à prova. Pensa-se, por exemplo, que é aceitável conceber restrições à privacidade e à proteção de dados pessoais – aqui entendida como uma decorrência da própria dignidade da pessoa humana –, que têm na sua disponibilidade justamente uma de suas características principais. Contudo, para que a restrição seja aceitável sob a ótica da proporcionalidade, deve respeitar critérios de transparência, consentimento informado, real legítimo interesse e da boa-fé objetiva, o que não vem ocorrendo nos *terms and conditions* (termos e condições) e nas *privacy policies* (políticas de privacidade) atuais.

Paralelamente, é fato que os Estados não podem interferir indevidamente na liberdade econômica das empresas de tecnologia. Ou, ao menos, esse é o dogma hoje existente, em que se afirma que a heterorregulação poderia impedir o progresso tecnológico. Contudo, a partir do momento em que essas empresas acabam desvirtuando direitos eminentemente públicos e indisponíveis, pode surgir um interesse público – materializado por normas coercitivas estatais – de promover algum nível de controle dos *players*, ou se alcançará mais vezes o resultado do escândalo da Cambridge Analytica ou de quem faça as vezes. No Brasil, a heterorregulação começou a surgir com o MCI e com a LGPD, mas é o *enforcement*[18] das normas, eminentemente principiológicas, que colocará à prova o nível de interferência estatal.

Por fim, cogita-se ser possível que as empresas desenvolvedoras de aplicativos não concebam *softwares* apenas sob o paradigma do tudo ou nada, por meio de gradações de funcionalidades. E, noutro giro, concebe-se que nem mesmo os aplicativos governamentais oficiais tutelam adequadamente a privacidade dos cidadãos.

Tudo isso porque, como se viu, os direitos à privacidade e à proteção de dados pessoais estão fortemente tensionados pela conjuntura de evolução tecnológica atual. Como conciliar interesses empresariais de lucro com o tratamento dos dados, o novo petróleo do mundo, com interesses pessoais de resguardo de algum nível de privacidade, interesses difusos

[18] Termo aqui entendido como aplicação, execução e cumprimento efetivo das normas.

de não haver ameaças à segurança dos dados e de manutenção da ordem democrática? Não é um questionamento trivial, mas o presente trabalho pretende contribuir na evolução da discussão, numa mescla do ordenamento jurídico como *dever-ser* ou como mero retrato e validação dos fatos sociais consolidados[19].

Explicitando-se ligeiramente a metodologia a ser empregada, para a realização da pesquisa, faz-se, primeiramente, e para gerar algum nível de envolvimento do leitor com o trabalho, uma análise pormenorizada e leiga – pretensamente, sob a visão de um cidadão comum, sem olhar jurídico ou sem qualquer familiaridade com o tema – dos termos de privacidade do *Facebook*, que é o aplicativo mais comentado quando se fala em proteção de dados. Nessa leitura prefacial, são apontadas as questões que mais chamariam a atenção de um cidadão comum. Depois, no decorrer do trabalho, os *insights* ordinários são postos à prova sob a dinâmica jurídica.

Após, faz-se uma análise bibliográfica de autores nacionais e internacionais que se debruçaram sobre a temática do direito à proteção de dados pessoais. Identificada essa base teórica do assunto, passa-se à análise das leis brasileiras aplicáveis (Constituição Federal, CDC, Lei do *Habeas Data*, LAI, Lei do Cadastro Positivo, MCI e LGPD) em termos comparados com a legislação estrangeira, principalmente a europeia, mas com alguns pontos da californiana. O objetivo é buscar, sem pretensão de esgotar, quais avanços no arcabouço normativo estrangeiro poderiam ser úteis para uma regulação mais efetiva no cenário brasileiro de proteção de dados.

Por fim, busca-se a efetiva análise das políticas de privacidade dos principais aplicativos móveis no cenário brasileiro. A metodologia consistirá em acessar o site da *Google Play* (em que o *download* dos aplicativos é franqueado) e analisar todos os termos de privacidade mais relevantes, um a um. E a escolha pela plataforma da *Google* em detrimento da *Apple* se deu por uma simples razão: o *market share* (fração do mercado) indica que o sistema operacional *Android*, da *Google*, representa cerca de 90% dos usuários brasileiros[20,21]. Ou seja, parece mais relevante analisar as aplicações que *rodam* na plataforma *Google* do que na plataforma *Apple*.

---

[19] REALE, Miguel. Teoria Tridimensional do Direito - situação atual. São Paulo: Saraiva, 1994, 5.ª ed.

[20] STATCOUNTER. Mobile Operating System Market Share Brazil. Disponível em: <https://gs.statcounter.com/os-market-share/mobile/brazil>. Acesso em: 26 mar. 2021.

[21] TECHTUDO. 9 em cada 10 brasileiros usam celular Android, diz relatório do Google. Disponível em: <https://www.techtudo.com.br/noticias/2020/09/9-em-cada-10-brasileiros-usam-celular-android-diz-relatorio-do-google.ghtml>. Acesso em: 26 mar. 2021.

Seria possível, em outro estudo, proceder a uma análise comparativa das mesmas aplicações nos dois sistemas operacionais, para aferir se há diferenças relevantes. Sem qualquer teste, é possível que se comprove uma hipótese de que os produtos que rodam na plataforma da *Apple* respeitam melhor o bom uso dos dados dos usuários e sua privacidade, até pelo próprio fato de os dispositivos da *Apple* não serem *abertos*[22].

Os aplicativos são classificados por segmentos de mercado, também para aferir se há alguma diferença de tratamento. Pensa-se na seguinte divisão aproximada: comunicação e redes sociais, navegadores e e-mails, entretenimento, comer e beber, infantis e jogos, finanças e crédito, compras, notícias, turismo e mapas, educação, produtividade e aplicativos governamentais.

O estudo é analítico: baseado em tabelas comparativas, bem como na leitura de todos os termos de privacidade mais relevantes, para que se verifique qual a importância dada às informações pessoais dos usuários. Fazem-se análises numéricas simples para aferir quais segmentos e desenvolvedores de aplicativos se preocupam mais com a privacidade e a proteção dos dados de seus usuários. Em última análise, busca-se verificar, também, se há alguma diferença de tratamento entre os *terms and conditions* para os aplicativos no Brasil e no exterior. Se houver, são investigadas as causas.

Como análise complementar – e para checar se há alguma diferença no tratamento dos dados –, também são verificados os *terms and conditions* de aplicativos de plataformas públicas. O interesse aqui é verificar em que medida o Estado pode ter interesse em dados eminentemente pessoais. Sobretudo à luz de que o tratamento de dados pelo Estado é regulado em artigos específicos da LGPD.

Assim, demonstrado o método utilizado para a realização da pesquisa, passa-se à análise teórica dos institutos jurídicos envolvidos.

[22] UOL. Privacidade gera guerrinha de indiretas entre Apple, Facebook e Google. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/05/30/por-que-apple-facebook-e-google-estao-fazendo-barraco-por-privacidade.htm>. Acesso em: 26 mar. 2021.

2 O DIREITO À PRIVACIDADE E AO SIGILO DOS DADOS PESSOAIS

Essa realidade prefaciada na introdução é possível por um complexo e estruturado sistema de colocação de empresas em rede, em que se afirma que, com 150 interações, as rotinas de programação sabem mais sobre o usuário do que seu companheiro, e, com 250 *likes* (curtidas) ou interações em determinada plataforma, os algoritmos conseguem saber mais sobre o usuário do que ele próprio – isso na medida em que a memória computacional é muito maior do que a própria memória humana[23].

Luigi Zingales[24] afirma que, de posse desses dados pessoais, as plataformas digitais, diferentemente dos demais agentes econômicos clássicos – que *só* tinham a oferecer a candidatos políticos o seu poderio econômico-financeiro –, conseguem oferecer diretamente votos, na medida em que têm o condão de influenciar a ação coletiva política das sociedades.

Para além dessa realidade de eventual influência em eleições, é certo que os dados pessoais são coletados mormente para o fazimento de perfis digitais. Na maioria das vezes, como já se enunciou, o perfil digital é idêntico, ou muito similar, à realidade. Afinal, "*seus dados são você*"[25].

Esses perfis digitais geralmente se prestam à publicidade comportamental. Certamente a maioria das pessoas, quando da utilização da internet em suas diversas aplicações, já se deparou com anúncios patrocinados sobre bens ou serviços que vinham buscando recentemente ou recorrentemente buscavam. Para os profissionais de marketing e publicidade, nada mais efetivo do que apresentar uma propaganda[26] voltada direto ao alvo: oferecer carros a quem vem buscando automóveis, oferecer roupas de grife a quem é acostumado a usá-las, viagens aos viajantes e assim sucessivamente. É a otimização perfeita para a comunicação social em sua vertente de publicidade.

É certo que a publicidade comportamental, embora associada à sociedade de consumo em massa e aos seus inexoráveis problemas, não é propriamente deletéria ao usuário. Talvez, se esse fosse o único preço, o *trade-off* dos usuários comuns da internet devesse mesmo

---

[23] HILBERT, Martin; LÓPEZ, Priscila. The world's technological capacity to store, communicate, and compute information. Science, v. 332, n. 6025, p. 60-65, 2011.

[24] ZINGALES, Luigi. Digital platforms and concentration. In: STIGLER CENTER. 2018 antitrust and competition conference. Disponível em: <www.youtube.com/watch?v=O_pxLvKQBE8>. Acesso em: 4 jun. 2021.

[25] Expressão cunhada por organizações da sociedade civil no Brasil quando da discussão da LGPD: COALIZÃO DIREITOS NA REDE. Seus Dados São Você. Disponível em: <https://direitosnarede.org.br/campanha/seus-dados-sao-voce/>. Acesso em: 26 mar. 2021.

[26] Aqui todos os termos estão sendo utilizados em sentido amplo e como eventuais sinônimos, sem necessária preocupação com a real terminologia adequada no âmbito das ciências afetas à comunicação social.

pender para o lado de utilizar *gratuitamente* os diversos serviços e funcionalidades em troca de receber a publicidade pessoalmente projetada e direcionada. Poderia parecer, *a priori*, e partindo da premissa de Milton Friedman de que *there is no free lunch* (não existe almoço grátis), um sinalagma adequado.

Os dados também podem ser utilizados, contudo, para finalidades ligeiramente mais sofisticadas – isso sem contar a possibilidade de influenciarem os rumos de democracias, é claro. Com efeito, é viável pensar, por exemplo, que dados de padrão de consumo (cartão de crédito e afins) podem implicar, em alguma medida, discriminações para acesso a crédito. A pessoa que é acostumada a não poupar seus rendimentos poderia ter juros para empréstimo mais elevados do que outrem acostumado a poupar e investir grande fração de sua renda, ou sequer seria elegível ao empréstimo.

Outro exemplo caricato é o dos sensíveis dados relacionados à saúde. Muitos consumidores certamente já aceitaram fornecer o seu número no CPF a farmácias em troca de suposto desconto em medicamento. O que impede a farmácia de, por exemplo, fornecer os dados de seus clientes e a respectiva lista de medicamentos aos operadores de seguros de vida e de saúde?

Com isso, as seguradoras poderiam calcular com maior exatidão o exato nível de risco de determinado segurado, oferecendo-lhe um preço *sob a medida de seu estado de saúde*. Diabéticos, cardiopatas, asmáticos e outros doentes crônicos certamente pagariam mensalidades muito maiores do que pessoas saudáveis pelo mesmo plano de saúde, ou sequer seriam elegíveis às coberturas. O exemplo tem potencial sistêmico tão grave, que o próprio Ministério Público do Distrito Federal e Territórios começou uma investigação sobre eventual repasse de dados de farmácias a seguradores de saúde[27].

Apenas para responder à questão levantada no parágrafo anterior: no Brasil, parece que a interpretação adequada dos §§ 4º e 5º do art. 11 da LGPD[28] caminha no sentido de que os

---

[27] VEJA. MP investiga se farmácias repassam dados de clientes a planos de saúde. Disponível em: <https://veja.abril.com.br/economia/mp-investiga-se-farmacias-repassam-dados-de-clientes-a-planos-de-saude/>. Acesso em: 26 mar. 2021.

[28] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: (...)
§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
I - a portabilidade de dados quando solicitada pelo titular; ou
II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.
§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

operadores de plano de saúde não podem discriminar consumidores a partir de tratamento de dados de saúde para eventual contratação. Talvez a Lei tenha até dito mais do que deveria, pois, lido literalmente, o § 5º teria o potencial até mesmo de acabar com os tradicionais questionários aplicados pelas seguradoras quando da contratação da cobertura, o que não parece ser a real *mens legis*.

Mas, dito de outro modo: hoje, o que impede o tratamento de referidos dados no Brasil é tão somente um trecho de legislação ordinária, que, a depender dos ventos futuros das instâncias legisladoras, poderia ser alterado até mesmo por uma medida provisória. E, além disso, como garantir que as seguradoras efetivamente não tratarão os dados pessoais para a finalidade vedada em lei, se há uma opacidade[29,30] ampla nos seios no tema? Não se sabe.

O que se pretende demonstrar com isso é que o tratamento indiscriminado de dados pessoais, que parece ser a tônica atual no Brasil e no mundo de modo geral, tem um potencial sistêmico enorme. Os dois exemplos anteriores são caricatos de como o amplo acesso e tratamento competente de dados pessoais pode significar restrições ao exercício de direitos por cidadãos: no caso, o de contratar.

É verdade que os exemplos anteriores poderiam, para além de significar a revolta de alguns com os efeitos – provavelmente, os prejudicados pelo tratamento –, também implicar uma sensação de *justiça* para outros. Afinal, uma leitura possível é a de que, se os bancos e as seguradoras estão conseguindo, em tese, filtrar melhor quem lhes gera maior risco, o crédito e os prêmios dos seguros ficariam mais baratos e acessíveis para os poupadores e pessoas sem condições de agravamento de saúde. As contraprestações ficariam, assim, mais ajustadas à respectiva realidade de cada pessoa, quase em uma leitura do que se entende por igualdade material. Bem, essa leitura até seria possível, mas seria necessário um *salto de fé* para ignorar o basilar fato de que a informação reveladora dos riscos foi obtida com abuso de direito (art. 187 do Código Civil[31]).

Além da publicidade comportamental e dos exemplos retro, é preciso dizer que o tratamento massivo de dados também implica o agravamento do risco da própria segurança dos dados. Com efeito, apenas entre o final de 2020 e o início de 2021, houve ataque *hacker* ao sistema do STJ[32], com aparente *download* de inúmeros dados de processos – muitos dos quais

---

[29] DONEDA, Danilo. O IPv6 e a internet das coisas. Disponível em: <http://observatoriodainternet.br/o-ipv6-e-a-internet-das-coisas>. Acesso em 26 mar. 2021.

[30] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[31] Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

[32] UOL. Ataque hacker no STJ: peritos temem vazamento em massa de dados copiados. Disponível em:

são sigilosos –, além de vazamento de dados de mais de 220 milhões de brasileiros, inclusive com informações fiscais[33]. Os efeitos dos vazamentos e ataques, aparentemente, ainda não foram sentidos, mas é certo que não se tratou de atuações com boa-fé.

Carlos Affonso relata um duplo papel exercido por esses incidentes de segurança: que ainda há muito a ser feito pelos controladores dos dados pessoais em termos de segurança e sigilo de dados e que é necessária uma conscientização sobre a importância do tema, o que é importante para a criação de uma cultura da privacidade[34].

Ou seja: ou bem se consegue finalmente regular como as plataformas digitais tratam os dados pessoais de seus usuários e consumidores, ou se aceitam as consequências, inclusive pretensas e aparentes distorções democráticas, que o tratamento massivo e em aparente desalinhamento dos ditames legais e constitucionais pode ocasionar. Parece melhor optar pela primeira opção, lutando, em paralelo, pelo devido *enforcement* das normas já existentes.

É dentro desse cenário que se insere o presente trabalho, que tem a pretensão de conciliar as disposições normativas, jurisprudenciais e doutrinárias sobre os direitos à privacidade e à proteção de dados pessoais – que, aparentemente, se consolidou como um novo direito fundamental, autônomo, após recente decisão do STF[35], posição que já era defendida há bastante tempo pela doutrina nacional à luz da experiência internacional[36] – a um estudo empírico e prático: a análise efetiva e detalhada, uma a uma, das políticas de privacidade dos principais aplicativos utilizados pelos brasileiros, estratificados em categorias que geram agregação suficiente para promover uma análise comparativa necessária e útil.

Aliás, diz-se que as políticas de privacidade representam, em si mesmas, uma forma ineficiente para controlar o fluxo dos dados pessoais, consistindo, em verdade, em mais uma resposta de autorregulação do mercado para legitimar o tratamento dos dados pessoais de modo

---

<https://www.uol.com.br/tilt/noticias/redacao/2020/11/09/ataque-no-stj-hacker-continua-com-o-controle-de-documentos-sigilosos.htm>. Acesso em: 26 mar. 2021.

[33] EXAME. Vazamento de dados de "220 milhões de brasileiros" não aconteceu da noite para o dia. Disponível em: <https://exame.com/tecnologia/vazamento-de-dados-de-220-milhoes-de-brasileiros-nao-aconteceu-da-noite-para-o-dia/>. Acesso em: 26 mar. 2021.

[34] SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[35] MENDES, Laura Schertel; FONSECA, G. S.. STF Reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. REVISTA DE DIREITO DO CONSUMIDOR, v. 130, p. 471, 2020.

[36] MENDES, Laura Schertel. Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

amplo[37]. Dada a lógica de tudo ou nada, a manutenção da profunda assimetria informacional acaba comprimindo qualquer poder de barganha existente por parte do consumidor.

Essa foi a percepção de estudo empírico da *Global Privacy Enforcement Network/*GPEN realizado em 2014, que concluiu que: 85% das políticas de privacidade não prestam informação adequada sobre o tratamento dos dados pessoais; 59% são de difícil compreensão no tocante a informações básicas sobre privacidade; 33% coletam dados excessivos; e 43% não têm uma interface adequada[38]. A pretensão da presente análise é testar hipóteses similares.

Como se vê, o recorte inicial do estudo é avaliar aplicativos – provedores de aplicação, se se utilizar a nomenclatura do MCI – de celulares. E isso por um simples motivo. Dados da Pesquisa Nacional por Amostra de Domicílios Contínua - Tecnologia da Informação e Comunicação (PNAD Contínua TIC), feita em 2018 e divulgada há pouco menos de um ano, dão conta de que 98,1% dos brasileiros utilizavam ou utilizaram celular para acessar a internet naquele ano. Em comparação, os computadores foram usados por 50,7% dos brasileiros e os *tablets*, por 12,0%[39]. Dos brasileiros com mais de 10 anos, 79,3% tinham celulares próprios para uso pessoal, dos quais 88,8% tinham acesso à internet pelo aparelho.

Ou seja, o celular é efetivamente o principal meio de acesso à internet no país, sendo que a vantagem em relação aos *concorrentes* vem aumentando nos últimos anos. E, como os celulares costumam ter suas funcionalidades amplificadas, para quaisquer pretensões que sejam, pelos aplicativos móveis neles instaláveis, o foco da parte empírica do trabalho é efetivamente o de analisar, juridicamente, o funcionamento desses *softwares*.

Isso porque, em uma pretensão de busca por antecedentes causais, o pensamento que justifica o trabalho é, simplificadamente, o seguinte: (i) se celulares são os dispositivos mais utilizados para o acesso à internet e se sabe que o acesso à internet deixa inúmeros rastros

---

[37] SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC and the New Common Law of Privacy 114, Columbia Law Review 583 (2014), GWU Legal Studies Research Paper No. 2013-120: "Another of the most prominent FIPPs is the individual's right to consent to the collection and use of her personal data. These two FIPPs became the backbone of the U.S. self-regulatory approach, with privacy policies seeking to satisfy the right to notice, and with user choice seeking to satisfy the right to consent"

[38] Informational Commissioner's Office. Global survey finds 85% of mobile apps fail to provide basic privacy information. Disponível em: <https://www.wired-gov.net/wg/news.nsf/articles/Global+survey+finds+85+of+mobile+apps+fail+to+provide+basic+privacy+information+10092014151000?open>.

[39] BRASIL. Empresa Brasileira de Comunicação. Celular é o principal meio de acesso à internet no país. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/celular-e-o-principal-meio-de-acesso-internet-no-pais#:~:text=Acesso%20pelo%20celular%20aumentou%20para%2098%2C1%25%20de%202017%20para%202018&text=Os%20aparelhos%20s%C3%A3o%20o%20principal,por%20quase%20todos%20os%20brasileiros.&text=Os%20dados%20mostram%20que%2079,78%2C2%25%20em%202017.>. Acesso em: 26 mar. 2021.

de navegação com a coleta ampla de dados pessoais, então os celulares são responsáveis por boa parte dessas coletas e consequentes tratamentos; e (ii) se o uso dos celulares depende, ao que consta, da utilização de aplicativos móveis, então é justamente o uso desses aplicativos móveis, potencialmente, o principal responsável pelo tratamento massivo de dados dos usuários.

Como se viu, a premissa (i) parece correta pelos dados até agora apresentados e que também são mais bem descritos no decorrer do trabalho. Por sua vez, o antecedente da premissa (ii) também parece correto, na medida em que se desconhece como operar um celular sem usar aplicativos. Em alguma medida, a pessoa precisará se utilizar de algum provedor de aplicação, nem mesmo que seja o simples e-mail, navegador ou buscador.

Dessa forma, parece que toda a estrutura causal é coerente do ponto de vista fático, de modo que o trabalho demonstra a sua relevância. E, sustenta-se, mesmo que haja como infirmar as conclusões retro – certamente há, na medida em que a ciência da computação é muito mais complexa do que se pode imaginar –, é certo que os aplicativos móveis são, em alguma medida, responsáveis por fração relevante do tratamento de dados pessoais de seus usuários, já que as pessoas literalmente dormem e acordam ao lado do celular. Ou seja, se a pretensão é seguir os rastros e preferências da pessoa, na atual inexistência de *chips* cerebrais – que já estão em desenvolvimento[40]–, o celular parece ser a melhor opção[41].

Diante disso, o trabalho parece relevante por pretender estudar os mecanismos jurídicos utilizados pelos aplicativos móveis no tratamento de dados. O foco da análise é a observância, na visão do autor e com a correspondente legitimação a partir da revisão bibliográfica feita, dos fundamentos e princípios da proteção e tratamento de dados, da observância dos direitos do titular e, principalmente, do adequado procedimento quanto a dois dos requisitos legais para o tratamento de dados pessoais: o consentimento (art. 7º, I, da LGPD)

[40] CANALTECH. Neuralink | O que é e como funciona o projeto que conecta um chip ao cérebro. Disponível em: <https://canaltech.com.br/inteligencia-artificial/neuralink-o-que-e-como-funciona-170585/>. Acesso em: 26 mar. 2021.

[41] Antes de prosseguir, e nessa linha, uma nota é, desde já, válida: embora o autor tenha alguma familiaridade com cálculos e números – por também ser engenheiro, o que ajuda a justificar, de certo modo, a predileção pelos estudos jurídicos com caráter mais empírico –, não se tem qualquer pretensão de percorrer o tema dos aplicativos sob a ótica da ciência da computação. Embora não se ignore que os temas são inevitavelmente imbricados – fato observado até mesmo no MCI e na LGPD, que se utilizam de expressões como "nos limites técnicos do seu serviço" e "considerando a utilização de meios técnicos razoáveis" –, o autor não possui competência técnica para efetivamente avaliar os aplicativos sob a dinâmica computacional, até mesmo porque muitas funcionalidades são "segredos comercial e industrial", como a própria LGPD reconhece.

e o legítimo interesse (art. 7º, IX, da LGPD)[42], responsáveis por 5% e 70% dos casos de tratamentos de dados pessoais, respectivamente[43,44,45].

Ainda quanto a essa discrepância, cogita-se, desde logo, uma *aposta* sobre o porquê de as empresas optarem pelo tratamento de dados baseado no legítimo interesse em detrimento do consentimento do usuário: aquele é muito mais facilmente conseguido, dada a amplitude semântica e normativa do conceito, do que esse[46]. Tal fato indica, em alguma medida, que é muito mais difícil obter o consentimento válido do que alegar e comprovar o legítimo interesse, que pode ser, até mesmo, o lucro[47]. Afinal, a LGPD não veda tal pretensão, a liberdade ao particular lhe permite fazer tudo o que não for proibido em lei (art. 5º, II, da CRFB/88[48]).

A autoridade regulatória inglesa, a seu turno, sugere que se use o legítimo interesse como base legal se se desejar manter o controle sobre o processamento, assumindo a responsabilidade de demonstrar que está dentro das expectativas ordinárias e razoáveis das pessoas, sem impactos injustificados sobre elas. Por sua vez, o consentimento transfere toda a responsabilidade aos indivíduos, exonerando, de certa forma, o processador de dados de responsabilidades tamanhas *ex ante*. Ou seja, o legítimo interesse seria a base legal mais flexível[49].

É claro, contudo, que, como o próprio Deputado Federal Orlando Silva, Relator da LGPD na Câmara dos Deputados, mencionou, "o legítimo interesse não deve ser lido como um

---

[42] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular; (...)
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[43] TELE SÍNTESE. "Interesse legítimo" supera "consentimento" no tratamento de dados pessoais pelas empresas. Disponível em: <https://www.telesintese.com.br/interesse-legitimo-supera-consentimento-no-tratamento-de-dados-pelas-empresas/>. Acesso em: 26 mar. 2021.

[44] USTARAN, E. (Org.). (2018). European data protection: Law and practice. an IAPP Publication, International Association of Privacy Professionals.

[45] É bem verdade que o intento inicial do trabalho era o de analisar apenas os contornos do consentimento, mas, durante as leituras preambulares, encontrou-se a informação, dada por Marcel Leonardi, de que, na Europa, apenas 5% do tratamento de dados tem como base o consentimento, enquanto 70% são baseados no legítimo interesse. Havendo esse descompasso grande entre uma e outra hipótese autorizadora do tratamento de dados, não se pode ignorar a análise do legítimo interesse no presente trabalho.

[46] Um teste trivial é caricato: ao passo que a LGPD tem 37 referências ao termo "consentimento", há apenas 6 ao termo "legítimo interesse".

[47] BRASIL. Serviço Federal de Processamento de Dados. Consentimento e legítimo interesse: faca de dois gumes. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/consentimento-legitimo-interesse-faca-dois-gumes>. Acesso em: 26 mar. 2021.

[48] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei.

[49] REINO UNIDO. Information Comissioner's Office. Lawful basis for processing. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>. Acesso em: 3 jun. 2021.

cheque em branco"[50]. Nessa linha, sustenta-se que o legítimo interesse deve ser aferido à luz de um teste de adequação, respeitando a estrita necessidade dos dados (art. 10, §1º, da LGPD) para a realização de finalidades legítimas a partir de situações concretas (art. 10 da LGPD) e com resguardo das liberdades fundamentais do titular dos dados, desde que respeitadas suas legítimas expectativas (art. 10, II, da LGPD)[51]. Fala-se, assim, em um verdadeiro teste de proporcionalidade constitucional, para aferir legitimidade (finalidade lícita dentro de uma situação concreta), adequação, necessidade (minimização), balanceamento (legítima expectativa objetiva e direitos fundamentais)[52] e salvaguardas (transparência, direito de oposição, mitigação de riscos e legítima expectativa subjetiva)[53]. Ou seja, por mais que seja mais aberto, é claro que o legítimo interesse não abarca tudo.

À luz desses comentários introdutórios, pretende-se, ao longo deste primeiro capítulo, fazer uma revisão bibliográfica acerca da discussão sobre o direito à privacidade e sobre o direito à proteção de dados, especialmente quando considerada a sua tensão nos dias atuais, de hiperconexão.

De modo específico, são feitas análises acerca: (i) do panorama geral da discussão; (ii) do conteúdo jurídico do direito à privacidade, sobretudo sob o paradigma da internet, o conteúdo do direito à proteção de dados e o julgamento do STF e o grau de disponibilidade dos direitos de personalidade; (iii) dos aspectos de direito contratual envolvidos, sobretudo da subespécie *contratos eletrônicos*; (iv) dos aspectos de direito do consumidor envolvidos, na medida em que os termos de privacidade consistem em verdadeiros contratos de adesão; e (v) de aspectos gerais sobre o MCI, a LGPD e o RGPD. Aspectos mais específicos são

---

[50] BRASIL, Câmara dos Deputados. (2018). Parecer da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 4060, de 2016. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=SBT+1+PL406012+%3D%3E+PL+4060/2012>. Acesso em: 6 abr. 2021.

[51] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

[52] MATTIUZZO, Marcela; PONCE, Paula Pedigoni. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. Revista Internet & Sociedade, v. 1, n. 2, dez. de 2020, páginas 54 a 76. Disponível em: <https://revista.internetlab.org.br/o-legitimo-interesse-e-o-teste-da-proporcionalidade-uma-proposta-interpretativa/>.

[53] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

pontualmente discutidos durante a etapa de análise dos resultados. Antes de se iniciar a revisão bibliográfica, porém, levantam-se alguns pontos mais peculiares da política de privacidade do *Facebook*, sob a visão de um leigo.

2.1 Antes de começar: uma leitura exploratória da política de privacidade do *Facebook*

Como já se discorreu na introdução, o *Facebook* acabou ganhando notoriedade no bojo da discussão sobre privacidade e proteção de dados, na medida em que é a rede social mais utilizada no mundo[54] e esteve umbilicalmente ligado aos fatos da Cambridge Analytica. Além disso, das cinco redes sociais mais utilizadas no Brasil em 2020, o *Facebook* detém o controle de quatro delas. Ou seja, o *Facebook* é o aplicativo que mais se amolda para ser o representante dessa análise prefacial.

A política de privacidade ou de dados do *Facebook*[55] inicia com a informação de que os termos ali dispostos são aplicáveis ao *Facebook*, ao *Instagram*, ao *Messenger* e a outros produtos e recursos oferecidos pela empresa. Além disso, fala-se em processamento de informações necessárias para viabilizar a operação de referidos produtos[56].

Para o usuário comum[57], a primeira informação parece justificável, na medida em que, sendo os três aplicativos do mesmo grupo econômico e tendo eles operação similar, é aceitável que compartilhem da mesma política de funcionamento. A segunda afirmação, por sua vez, gera uma espécie de conforto, já que apenas seriam coletados os dados para viabilizar a operação da plataforma.

Na sequência, no grupo de "Quais tipos de informações coletamos?", informa que coleta dados sobre a câmera utilizada no aplicativo – supostamente para oferecer mais funcionalidades –, bem como sobre as comunicações pessoais. Também informa que o usuário tem a possibilidade de fornecer "dados com proteções especiais" (religião, política, saúde e outros) nas informações sobre seu perfil, o que pode estar sujeito a proteção especial a depender a lei do país do usuário.

---

[54] RESULTADOS DIGITAIS. Ranking das redes sociais 2020: as mais usadas no Brasil e no mundo. Disponível em: <https://resultadosdigitais.com.br/blog/redes-sociais-mais-usadas-no-brasil/>. Acesso em: 5 abr. 2021.

[55] FACEBOOK. Política de Dados. Disponível em: <https://www.facebook.com/about/privacy/>. Acesso em: 5 abr. 2021.

[56] "Esta política descreve as informações que processamos para viabilizar a operação do Facebook, do Instagram, do Messenger e de outros produtos e recursos oferecidos pelo Facebook (Produtos do Facebook ou Produtos)".

[57] Sem qualquer conotação pejorativa ou jocosa, mas de mera constatação de que o "usuário comum" é aquele que busca, na maioria das vezes, apenas o acesso facilitado ao produto ou serviço oferecido, sem se preocupar com cláusulas contratuais adesivas e obscuras.

Para o usuário comum, pode chamar um pouco a atenção a amplitude do acesso ativo à câmera, o que também pode parecer justificável pelo fato de os dados serem processados para o oferecimento de algumas funções dentro da própria câmera. Sobre o conteúdo das comunicações pessoais, o usuário comum poderia ficar apreensivo em manter diálogos importantes no âmbito da plataforma. Por fim, talvez o usuário ordinário também pudesse não entender o fato de sequer a política parecer se preocupar com o fato de ele estar no Brasil, na medida em que fala genericamente sobre as leis.

Também pode chamar a atenção a coleta de "informações sobre como você usa nossos Produtos, como o tipo de conteúdo que você visualiza ou com o qual se envolve; os recursos que você usa; as ações que você realiza; as pessoas ou contas com que você interage; e o tempo, frequência e duração das suas atividades", o que indicaria uma sensação de *perseguição* ou *monitoramento* no usuário.

Outro fato que pode despertar atenção é referente à possibilidade de serem coletadas informações do usuário a partir da interação de terceiros com a rede social, e vice-versa. Se o usuário optar por não disponibilizar seu número de telefone, mas um terceiro der tal informação relativa ao usuário original – por serem *amigos* na rede social, por exemplo –, o *Facebook* terá acesso à informação e vincula-la-á ao usuário original, que tinha optado por não fornecê-la. Talvez isso possa indicar ao usuário comum que sua privacidade não está apenas sob seu controle, mas depende da forma como diversos outros usuários lidam com a rede social.

Por sua vez, dentre as informações de dispositivo coletadas, estão os atributos, as operações, os identificadores, os sinais, os dados das configurações, as redes e conexões e os *cookies*. Dentre todas, as que provavelmente chamam mais atenção do usuário ordinário são o acesso ao GPS, à câmera ou às fotos, sendo isso atenuado pelo fato de tais informações só serem coletadas, em tese, se o usuário permitir.

Na sequência, surgem as explicações sobre a coleta de informações de parceiros comerciais do *Facebook*. De acordo com a política, "esses parceiros fornecem informações sobre suas atividades fora do *Facebook*, inclusive informações sobre seu dispositivo, os sites que você acessa, as compras que faz, os anúncios que visualiza e sobre o uso que faz dos serviços deles, independentemente de ter ou não uma conta ou de estar conectado ao *Facebook*", desde que os parceiros tenham autorização legal para fornecer ao *Facebook* tais informações.

O fato de ser exigida a autorização legal pode bastar para o usuário comum ficar mais tranquilo – juridicamente, sabe-se que essa autorização não é tão difícil de ser conseguida, seja via consentimento, seja via legítimo interesse. Mas, ainda assim, boa parte das pessoas – e aqui não se fala mais nem em usuário, na medida em que sequer precisa ser usuário para

eventualmente ter sua informação nas mãos do *Facebook* – pode ficar incomodada em ter suas informações, inclusive de compras fora da internet, compartilhadas com a empresa.

Por sua vez, o grupo "Como usamos essas informações?" inicia afirmando que as informações coletadas são utilizadas para o oferecimento do próprio produto da plataforma e para a personalização de recursos e conteúdos, inclusive anúncios e outros conteúdos patrocinados. Poderia chamar atenção o fato de serem usadas informações sobre interesses de "fora dos nossos Produtos" para a personalização da experiência, mas é provável que o usuário comum sequer se atentasse a isso. Para sua visão, aliás, essa personalização com vistas a gerar experiência unicamente pessoal é positiva, pois só será submetido a conteúdos com o qual tenha afinidade. Alguns usuários um pouco mais habilidosos podem não gostar da *bolha* formada[58].

Mais uma vez, pode chamar a atenção do usuário comum a possibilidade de o *Facebook* utilizar as informações pessoais coletadas, dentro e fora de suas plataformas para "ajudar os anunciantes e outros parceiros". Esse compartilhamento dos dados com terceiros pode parecer pernicioso, mesmo aos olhos do usuário não tão experiente.

Um fato que pode parecer positivo ao usuário comum – e mesmo ao operador jurídico – é a afirmação de que o processamento de dados pode ser utilizado para detectar quando alguém precisa de ajuda, notadamente para evitar qualquer conduta suicida. Como o *Facebook* detém uma enormidade de informações do usuário, nada mais natural do que seus algoritmos serem capazes de identificar eventuais pontos que indiquem níveis graves de depressão ou outras doenças psíquicas de seus usuários, usando o resultado desse processamento para evitar o pico da doença.

Pensa-se que, para além da prevenção ao suicídio, os algoritmos poderiam ser utilizados para auxiliar no combate a diversos tipos de violência, como aquelas às mulheres, às crianças, aos idosos, aos deficientes e outros. Como as informações que, em tese, indicam a existência de tais crimes já são ordinariamente coletadas pelo dispositivo móvel – isso é: se o celular já *ouve*[59] o que o usuário fala para fins de publicidade comportamental, também é capaz de *ouvir* uma mulher gritando algo como "para de me bater, fulano" –, poderia ser o caso de implementar o processamento dessas informações para a finalidade de repressão a essas formas de violência.

---

[58] FOLHA DE SÃO PAULO. Redes sociais criam bolhas ideológicas inacessíveis a quem pensa diferente. Disponível em: <https://www1.folha.uol.com.br/ilustrissima/2017/09/1920816-cada-macaco-no-seu-galho---zuckerman.shtml>. Acesso em: 5 abr. 2021.

[59] Cita-se o software Alphonso, utilizado em diversos aplicativos, que capta dados a partir do microfone do celular sobre hábitos de consumo televisivo ou outros áudios de fundo para fornecimento a anunciantes para que estes ofertem produtos e serviços personalizados ao indivíduo. Disponível em: <https://www.bbc.com/mundo/noticias-44724389>. Acesso em: 3 jun. 2021.

Ou seja, sempre que fosse atingida alguma rotina de programação que *ouvisse* a expressão "para de me bater, fulano" – com algum outro critério de verificação –, o aplicativo poderia chamar imediatamente o policiamento da região. Tal espécie de processamento geraria maior responsabilidade social por parte das empresas, o que eventualmente tornaria mais compreensível ao usuário o fornecimento dos consentimentos necessários. Até existem alguns aplicativos destinados à violência doméstica, mas nenhum parece ter esse tipo de ferramenta[60].

Nessa linha de responsabilidade social, o *Facebook* informa que usa as informações para "realizar e apoiar pesquisas e inovação sobre tópicos relacionados a bem-estar social geral, avanço tecnológico, interesse público, saúde e bem-estar. Por exemplo, analisamos as informações que temos sobre padrões de migração durante crises para auxiliar na ajuda humanitária". Para o usuário comum, isso pode parecer positivo, especialmente no que toca à crise humanitária de índole migratória. Alguém mais atento certamente lembraria que foi por meio de pesquisas como essas que a Cambridge Analytica começou a processar os dados dos usuários para pretensões menos nobres.

Na seção "Como essas informações são compartilhadas?", o usuário comum pode ver, no início, algum sentido de justiça, na medida em que ele escolhe o que e com quem compartilhar, inclusive ao disponibilizar informações públicas. Pode chamar mais atenção a possibilidade de o compartilhamento por terceiro de informação compartilhada mais restritamente pelo usuário poder ser mais amplo.

Possivelmente o usuário comum gostaria que sua opção inicial pela restrição fosse mantida, mas, do ponto de vista tecnológico, realmente é muito difícil impedir que o terceiro faça alguma captura do conteúdo da tela para posterior publicação na rede social. Então, o alerta é relevante: "Você deve ponderar com quem escolhe compartilhar, porque as pessoas que podem visualizar suas atividades em nossos Produtos podem decidir compartilhá-las com terceiros dentro e fora de nossos Produtos, inclusive com pessoas e empresas fora do público com o qual você compartilhou".

Sobre a integração e o compartilhamento de informações com parceiros, o usuário comum, provavelmente, ficaria confortável, na medida em que a narrativa usada se baseia no consentimento e na minoração dos dados[61], bem como na necessidade do tratamento para o

---

[60] GLOBO. Conheça canais e aplicativos que ajudam mulheres vítimas de violência doméstica. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2020/06/04/conheca-canais-e-aplicativos-que-ajudam-mulheres-vitimas-de-violencia-domestica.ghtml>. Acesso em: 5 abr. 2021.

[61] "Observação: estamos restringindo ainda mais o acesso de desenvolvedores a dados a fim de ajudar a evitar abusos. Por exemplo, removeremos o acesso dos desenvolvedores a seus dados do Facebook e do Instagram se você não usar o aplicativo deles por três meses. Além disso, estamos alterando o *login* de modo que, na próxima versão, reduziremos os dados que um aplicativo poderá solicitar, isento de análise, para incluir apenas nome,

fornecimento de serviços gratuitos. Ou seja, o *Facebook* compartilharia com terceiros aquilo a que o usuário desse aval. Juridicamente, no decorrer desse trabalho, problematiza-se essa questão do *aval*.

Também se informa o seguinte: "Não vendemos nenhuma de suas informações para ninguém e jamais o faremos". O usuário comum certamente fica aliviado com esse tipo de informação. Aquele um pouco mais experiente certamente sabe não se tratar de uma *venda* propriamente dita, mas de uma parceria comercial mais sofisticada, que, na essência, implica os mesmos resultados.

Por sua vez, informa-se que "o *Facebook* e o *Instagram* compartilham infraestrutura, sistemas e tecnologia com outras Empresas do *Facebook* (inclusive *WhatsApp* e *Oculus*) para fornecer uma experiência inovadora, relevante, consistente e segura", para o que há o processamento de informações. Para o usuário comum, sobretudo à luz do exemplo dado – evitar a perpetuidade de *spams* –, pode parecer compreensível, já que se trata de aplicativos do mesmo grupo econômico. O mais experiente pode eventualmente se sentir desconfortável por usar apenas o *WhatsApp*, mas ver suas informações compartilhadas com todas as empresas do *Facebook* de modo geral.

A política de privacidade também menciona ao usuário a possibilidade de acesso, retificação, portabilidade e apagamento dos dados, o que é positivo aos olhos do usuário comum e também do jurista. No tocante à transferência internacional de dados, o usuário comum pode se sentir ligeiramente carente de informações sobre o porquê de ser realmente necessária tal ação. Talvez tenha faltado a expressão de que isso "possibilita a operação de nossas empresas e o fornecimento de serviços gratuitos para pessoas do mundo inteiro".

Por fim, há uma última seção: "Aviso de privacidade do Brasil". Fala-se brevemente sobre os direitos básicos previstos na LGPD e sobre como exercê-los em relação ao *Facebook* e ao *Instagram*. Também há o contato do encarregado de proteção de dados do *Facebook*, que pode ser contatado pelo usuário em caso de dúvidas mais relevantes. Não há maior detalhamento, o que parece particularmente lacunoso dado o contexto de existirem mais de 130 milhões de usuários das ferramentas no Brasil (cerca de 5% dos usuários globais das ferramentas). Mas, de toda forma, certamente o usuário comum não gosta muito de *juridiquês*.

Esse é o panorama prático em que inserido o presente trabalho. Buscou-se, com uma breve leitura sobre a política de privacidade do *Facebook*, apontar alguns dos principais tópicos que são desenvolvidos na sequência, bem como dar algum senso de relevância empírica

---

biografia e nome de usuário do Instagram, foto do perfil e endereço de email. A solicitação de outros dados exigirá nossa aprovação".

à discussão. É a partir desse contexto que se faz a análise que se propõe, bibliográfica e, ao final, empírica de modo mais amplo, sob o enfoque jurídico. Tendo isso em mente, passa-se a discorrer sobre o panorama geral da privacidade e da proteção de dados.

2.2 Panorama geral

Inicialmente, importante contextualizar, de modo claro e efetivo, a problemática envolvida: muitos usuários não sabem, mas os aplicativos ditos *gratuitos* (*WhatsApp*, *Waze*, *Facebook*, etc.) possuem nítidos interesses comerciais nos dados de seus usuários. Em simples termos: esses aplicativos *ganham – bastante*[62] *– dinheiro* e *sobrevivem* no mercado porque, de uma ou outra forma, *comercializam* os dados dos usuários, principalmente com empresas especializadas no fazimento de propagandas voltadas ao público.

Nesse sentido, cunhou-se a expressão *zero-price advertisement business model* (modelo de negócios a preço zero via publicidade)[63] para fazer referência ao fato de que os usuários não pagam, em dinheiro, pelo produto ou serviço, mas o correspondente vem da coleta e tratamento de seus dados pessoais, que serão convertidos na facilitação à publicidade comportamental e gerará uma espécie de pagamento indireto. Diz-se que há um *trade-off* dos dados pessoais pelo serviço[64].

E, ao olhar para a maioria dos aplicativos que comportam uma versão paga – ou seja, que já teria a contraprestação pecuniária intrínseca à prestação do serviço ou ao produto –, vê-se que a dinâmica não é muito alterada. Trata-se do que se cunhou de modelos de negócio *freemium* (mistura entre gratuito e diferenciado, *free* e *premium*)[65]. As versões diferenciadas, *premium*, que já fizeram a monetização antecedente pela disponibilização do serviço, também apostam na utilização dos dados pessoais para rentabilizar ainda mais o serviço. A constatação

---

[62] Sem qualquer conotação pejorativa por haver ganhos patrimoniais relevantes por referidas empresas, na medida em que o lucro auferido dentro das balizas legais é justamente o foco de qualquer empreendimento. Trata-se de dado meramente objetivo de que as ditas *big techs* são as empresas mais valiosas ou ricas do mundo. Informações disponíveis em: <https://exame.com/tecnologia/apple-se-mantem-como-marca-mais-valiosa-do-mundo-veja-ranking/> e <https://segredosdomundo.r7.com/empresas-mais-ricas-do-mundo/>. Acesso em: 5 abr. 2021.

[63] STRANDBURG, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect. NYU School of Law, Public Law Research Paper n.13-62, p.96, Oct. 2013. Disponível em: <http://ssrn.com/abstract=232396>. Acesso em: 5 abr. 2021.

[64] IAB Europe. Consumers Driving the Digital Uptake: The economic value of online advertising-based services for consumers, p.7, Sept. 2010. Disponível em: <http://www.iabeurope.eu/files/7113/7000/0832/white_paper_consumers_driving_the_-digital_uptake.pdf>. Acesso em: 5 abr. 2021.

[65] NELSON, Brett. The "Freemium" Model: top flaws and potent fixes. Disponível em: <http://www.forbes.com/sites/brettnelson/2013/07/23/the-freemium-model-top-flaws-and-potent-fixes/>. Acesso em: 5 abr. 2021.

de Bruno Bioni parte da própria não diferenciação das políticas de privacidade das versões paga e gratuita[66].

Resta uma dúvida: qual a legitimidade desses aplicativos para fazerem essa *comercialização* de dados eminentemente pessoais? Um exemplo para deixar ainda mais claro o problema: o aplicativo de GPS *Waze*, por exemplo, tem acesso à galeria de imagens do celular do usuário. Isso porque, com acesso, ele consegue proceder a uma análise das imagens e exibir, em suas propagandas comerciais, aquilo que mais de adéqua ao padrão do usuário[67].

É inegável que a tecnologia – especialmente a internet como conceito de rede mundial – vem permeando quase todas as atividades rotineiras da vida, sejam elas eminentemente ligadas ao setor privado – *i.e.*, sites de comércio eletrônico – ou relacionadas à interação entre cidadão e setor público, como o necessário *accountability* da coisa pública[68].

Apesar de todos os benefícios da popularização da rede, sobretudo para a liberdade de expressão e informação e para as facilidades comunicativas, dela emerge um desafio muito relevante: como proteger a privacidade e os dados dos usuários? O atual modelo de negócios é concebido com base na coleta e no tratamento de dados pessoais, facilmente captados quando o usuário simplesmente *instala* um aplicativo ou *acessa* um site eletrônico.

Há quem recomende, por exemplo, utilizar navegador anônimo, desinstalar aplicativos desnecessários, limpar os perfis nas redes sociais, reconfigurar pontos específicos do celular e exercer o direito de consulta aos dados armazenados[69]. Certamente, opções muito interessantes e que contribuiriam para reduzir os rastros digitais. Mas é muito improvável que o usuário ordinário da internet se atente a tudo isso.

O interesse econômico nesses dados é muito simples: a publicidade comportamental. A constatação não é difícil: quantas vezes, *i.e.*, após procurar um aparelho celular para compra em sites especializados, o usuário já não se deparou com a publicidade desse mesmo celular nos mais diversos sites eletrônicos e em vários aplicativos móveis? Várias[70].

---

[66] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[67] Se for uma pessoa com muitas fotos de paisagens nos Estados Unidos, por exemplo, as propagandas serão de promoções de passagens aéreas para aquele país; por outro lado, se for uma pessoa com muitas fotos em restaurantes, as propagandas serão de promoções de locais de alimentação.

[68] ANTONIALLI, Dennys; CRUZ, Francisco Brito. *Privacidade e internet*: desafios para a democracia brasileira. *Ensaios democracia digital*, São Paulo, n. 1, mar. 2017.

[69] BBC. 5 formas rápidas e fáceis de reduzir seus rastros na internet. Disponível em: <https://www.bbc.com/portuguese/geral-43585945>. Acesso em: 5 abr. 2021.

[70] ANTONIALLI, Dennys; CRUZ, Francisco Brito. *Privacidade e internet*: desafios para a democracia brasileira. *Ensaios democracia digital*, São Paulo, n. 1, mar. 2017.

Mas a utilização de informações das pessoas não é nova. Remonta, no mínimo, à Idade Média, em que a Igreja Católica – mantenedora de diversos bancos de dados com informações eminentemente pessoais de seus fiéis – realizava verdadeiros cruzamentos de informações para decidir quem seria considerado realmente herege. Com a evolução histórica, esse controle sobre as informações pessoais dos cidadãos começou a interessar aos Estados, pelo movimento foucaultiano da *biopolítica*. A intenção era simples: manter a vigilância da população[71].

Contudo, hoje o problema da proteção de dados ganha escala, na medida em que "a estrutura globalizada da rede implica a transferência internacional de dados pessoais por parte de atores do setor privado e coloca em sobreposição modelos regulatórios diferentes, o que gera dificuldades de compatibilização"[72].

Isso gera – além do interesse eminentemente econômico das empresas para fins de publicidade comportamental – interesse nos Estados, que visam ao incremento de "suas capacidades de vigilância e eficiência na gestão pública"[73]. O problema aqui é de ordem constitucional: esse comportamento dos Estados acaba gerando um *chilling effect* (efeito inibidor) nas liberdades públicas dos cidadãos, sofridas conquistas históricas.

No Brasil, a LGPD e o Marco Civil da Internet estabelecem algumas balizas para impedir que eventual autoritarismo estatal avance indevidamente sobre a privacidade dos cidadãos. Um exemplo fácil é a necessidade de ordem judicial para o fornecimento de alguns tipos de registros (arts. 10, 13 e 15 do MCI). Mesmo assim, a regulamentação e aplicação da norma parecem não ser claras, o que gera insegurança para os usuários por (i) terem descrença na responsabilização dos *players* violadores e (ii) temerem que seus dados privados sejam *vazados* ao grande público.

De mais a mais, esse acesso quase irrestrito a informações eminentemente pessoais também afeta a experiência democrática dos cidadãos, pois se expõem ao poder de manipulação desses *players*. Exemplo disso são as chamadas *rondas virtuais* promovidas pelas áreas da segurança pública – foram bastante empregadas nas manifestações políticas brasileiras de 2013. O problema é fazer o filtro de até onde essas *rondas* são úteis para os fins de manutenção da

---

[71] ESTRADA, Manuel Martín Pino. *O comércio bilionário de dados pessoais na internet*. *Acadêmica Faculdade Progresso*, Guarulhos, n. 2, p. 3, 2017.
[72] ANTONIALLI, Dennys; CRUZ, Francisco Brito. *Privacidade e internet*: desafios para a democracia brasileira. *Ensaios democracia digital*, São Paulo, n. 1, p. 7, mar. 2017.
[73] Ibidem.

ordem pública – em casos em que seriam, *prima facie*, autorizadas, já que movidas pela proteção do maior interesse público[74].

A discussão que se deve ter é: qual o limite para que não haja invasão da privacidade dos usuários pela simples invasão? A partir de quando o Estado deixará de ser um mero mantenedor da ordem social para se tornar eminentemente policial e vigilante, resfriando manifestações políticas democráticas e republicanas?

Como se pode imaginar, o recorte não é fácil. E pior: transferi-lo ao Poder Judiciário, como é normalmente feito, pode implicar a existência de 18 mil[75] soluções diferentes, o que não é útil para a segurança jurídica e para a estabilização de expectativas dos cidadãos[76]. E a experiência democrática é posta ainda mais em xeque a partir do momento em que começam a surgir relatos acerca da capacidade de os *computadores* influenciarem a propaganda política e, ao cabo, o próprio resultado do sufrágio.

Exemplos recentíssimos disso são os escândalos envolvendo o vazamento de dados do *Facebook*, que teriam alegadamente auxiliado na eleição de Donald Trump nos Estados Unidos em 2016[77]. Ou seja, parece que as empresas e os Estados já perceberam que os dispositivos tecnológicos "permitem construir sistemas de bombardeio de informação e de manipulação de susceptibilidades" dos usuários/cidadãos[78].

E esse problema ganha especial relevo quando se considera o atual estado da arte: internet das coisas, em que automóveis, aviões, aparelhos, relógios e até bebidas alcoólicas interagem com os *smartphones*. Ou seja, a depender do tratamento do dado, as empresas e os Estados poderão até mesmo saber quando o cidadão abrir uma garrafa de bebida alcoólica. Três parecem ser as principais consequências possíveis dessa provável intermediação: (i) as empresas registrarem as preferências e o engajamento dos seus usuários e consumidores; (ii) as modificações no projeto das plataformas e dispositivos para haver influência nessa interação; e (iii) a abordagem proativa dos consumidores, e não a espera passiva pelo contato ou pela busca de ofertas[79]. Parece haver um pouco de tudo isso.

---

[74] Ibidem.
[75] Trata-se do número aproximado de membros do Poder Judiciário no Brasil. CNJ. *Justiça em números 2020*. P. 46. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf>. Acesso em: 5 abr. 2021.
[76] ANTONIALLI, Dennys; CRUZ, Francisco Brito. *Privacidade e internet*: desafios para a democracia brasileira. *Ensaios democracia digital*, São Paulo, n. 1, mar. 2017.
[77] BBC. *O escândalo que fez o Facebook perder US$ 35 bilhões em horas*. Inglaterra, 2018. Disponível em: <http://www.bbc.com/portuguese/internacional-43466255>. Acesso em: 20 mar. 2021.
[78] ANTONIALLI, Dennys; CRUZ, Francisco Brito. *Privacidade e internet*: desafios para a democracia brasileira. *Ensaios democracia digital*, São Paulo, n. 1, p. 8, mar. 2017.
[79] Ibidem, p. 14.

Ou seja, o consumidor acaba deixando de ser meramente passivo no ciclo econômico baseado no consumo, na medida em que seus dados são usados para a confecção, distribuição e segmentação dos bens de consumo[80]. Transforma-se na figura do *prosumer*, na medida em que consume e produz o bem de consumo, sendo mero expectador das suas informações pessoais[81].

Salienta-se que essa espécie de restrição criada pela publicidade comportamental – dar ao usuário mais daquilo por que ele já nutre interesse – acaba gerando uma bolha de interesses e de consumo. Ou seja, o cidadão/usuário acaba não sendo submetido ao experimentalismo e a qualquer grau de inovação do mercado, o que, em larga escala, acaba sendo ruim para o próprio desenvolvimento concorrencial do negócio[82].

Partindo-se mais especificamente para o problema estudado, sabe-se que a maioria dos modelos de negócios das plataformas e aplicativos ditos *gratuitos* são baseados na publicidade digital. E toda essa publicidade é baseada na coleta de dados dos usuários, para que seja mais *efetiva*. De acordo com a literatura, isso acontece porque, com a coleta e o tratamento dos dados pessoais, é tecnicamente viável empreender uma estratificação dos usuários de acordo com seus interesses macro e específicos, direcionando-lhes anúncios de forma mais efetiva[83]. E, sobretudo, de forma bastante mais barata, já que a comunicação é mais certeira e cirúrgica[84].

Com isso, mais usuários em determinada plataforma, com mais dados coletados, significam maior valorização daquele determinado site enquanto veículo utilizado para a promoção de anúncios, extremamente mais precisos. Afinal, é muito mais provável que você consiga vender um automóvel a quem demonstra algum interesse nessa temática do que a quem procura uma bicicleta e é engajado em temáticas contrárias ao uso de transporte privado.

E diversos são os mecanismos para a coleta e transmissão desses dados, normalmente enviados a empresas especializadas na sua análise – para posterior

---

[80] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[81] LISBOA, Roberto Senise. Prefácio. In: MATTOS, Karla Cristina da Costa e Silva. *O valor econômico da informação nas relações de consumo*. São Paulo: Almedina, 2012. p.16: "O acesso à informação, como direito fundamental e direito básico dos consumidores, transforma-os em *prosumers*, ou seja, participantes ativos na própria confecção, distribuição, aquisição e descarte de produtos e serviços colocados no mercado pelos fornecedores".

[82] Ibidem, p. 14.

[83] Ibidem, p. 15.

[84] EVANS, David D. The economics of the online advertising industry. Journal of Economic Perspectives, Apr. 2009, p.42. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>. Acesso em: 5 abr. 2021.

comercialização a outras empresas, interessadas, quando atuando com boa-fé, na publicidade efetiva.

Um exemplo conhecido são os *cookies*, verdadeiros identificadores de preferências – e a maioria dos usuários, por desconhecimento, acaba autorizando a atuação desses programas em sua navegação na internet. Aliás, alguns *websites* sequer funcionam corretamente quando se opta pelo modo de navegação anônimo, justamente porque sua única fonte de sobrevivência é a coleta e o processamento dos dados dos usuários[85].

Esses bancos de dados contêm informações muito reveladoras sobre a personalidade dos usuários, como os sites visitados, as notícias buscadas e efetivamente lidas, a lista de amigos com que mantêm contato efetivo, os lugares por que passaram, as palavras-chave buscadas: os exemplos são incontáveis, ainda mais quando se considera a recente tecnologia de armazenamento de arquivos na *nuvem*. Do ponto de vista da monetização, todos esses dados são muito relevantes para a exibição dos *posts* patrocinados nas mais diversas plataformas[86].

Todo esse processo de estratificação e identificação pontual dos interesses principais de cada usuário com base na coleta e tratamento dos dados dispostos no ambiente virtual tem tensionado o direito à privacidade e à proteção de dados, sobretudo por um conjunto de fatores: (i) dificuldade de informar, com clareza e inteligibilidade, ao usuário sobre a coleta e o tratamento de dados, bem como sobre os atores envolvidos nisso; (ii) a insuficiência do modelo baseado no consentimento dos usuários, sobretudo à luz da dinâmica binária do "*take it or leave it*" ("*pegar ou largar*"), "que reflete a ausência de uma vontade livre em razão da assimetria de poderes entre ele e o agente responsável pelo tratamento, bem como a sua dependência a muitos serviços da sociedade da informação"; (iii) as modernas técnicas de tratamento e análise de dados, com o cruzamento de informações existentes em diferentes plataformas (os *terceiros* ou *parceiros comerciais* já vistos na política de privacidade do *Facebook*, por exemplo), o que possibilita a montagem de um perfil virtual ainda mais fidedigno e completo[87]; e (iv) a adoção de práticas discriminatórias a partir dos dados – fala-se até em discriminação algorítmica[88] – e a possibilidade de manipulação do usuário com base nas informações coletadas.

---

[85] Ibidem.
[86] Ibidem.
[87] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. JOURNAL OF INSTITUTIONAL STUDIES, [S.l.], v. 6, n. 2, p. 507-533, set. 2020. Disponível em: <https://estudosinstitucionais.emnuvens.com.br/REI/article/view/521>. Acesso em: 5 abr. 2021.
[88] SCHERTEL MENDES, Laura; MATTIUZZO, Marcela. DISCRIMINAÇÃO ALGORÍTMICA: CONCEITO,

Nesse contexto, a evolução tecnológica não afastou esse interesse na detenção de informações pessoais de usuários e cidadãos, mas trouxe uma característica peculiar: agora, empresas descentralizadas e, em tese, desvinculadas da ingerência estatal procedem à coleta e à utilização dos dados pessoais de seus usuários.

Como não haveria nenhum interesse supostamente apto a legitimar essa compressão da esfera privada em prol dos interesses econômicos empresariais[89] – não mais existiria a preocupação com a manutenção da ordem social e com a evolução nacional, como antigamente –, a solução para a coleta dos dados da população foi jurídica: recolher as informações desde que o sujeito desses dados consentisse com isso[90].

Contudo, surgiu um problema para as empresas: com que interesse o usuário consentiria com a coleta dos seus dados pessoais? A solução foi elegante: as permissões seriam dadas como moeda de troca por serviços personalizados, brindes, direito de participar de sorteios, acesso gratuito à internet, produtos e financiamentos online, dentre outros[91]. Diz-se, assim, que o consentimento é muito mais um pilar da estratégia regulatória de legitimação dos modelos de negócio do que propriamente uma expectativa de eficiente proteção dos dados pessoais. O fardo normativo recai, hoje, unicamente sobre os titulares dos dados[92].

O convencimento, então, é praticamente imposto, na medida em que hoje não se cogita de que um adolescente não tenha instalados os aplicativos *WhatsApp*, *Instagram*, *Facebook* – segundo a visão dos próprios adolescentes, eles sofreriam *bullying* de seus amigos se não participassem dessas redes sociais. Então, por um imperativo, um determinismo, de índole social, é-se praticamente obrigado à submissão às *regras do jogo*. E, outras tantas vezes, essa publicização dos dados pessoais acontece *sponte propria*, com os usuários sendo, de certa forma, *seduzidos* pelas aplicações, que incentivam o extremo culto social, com exposição dos mais diversos momentos da vida[93].

FUNDAMENTO LEGAL E TIPOLOGIA. Direito Público, [S.l.], v. 16, n. 90, dez. 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Acesso em: 5 abr. 2021.

[89] Hoje, a coleta desses dados pessoais é baseada, sobretudo, em duas autorizações legais, que são convergentes na LGPD, no RGPD e na norma californiana: o consentimento qualificado e o legítimo interesse. A amplitude desse último conceito é grande, razão por que, como se enunciou na introdução, é responsável pela maior parte da autorização formal para o tratamento de dados na prática.

[90] ESTRADA, Manuel Martín Pino. *O comércio bilionário de dados pessoais na internet*. *Acadêmica Faculdade Progresso*, Guarulhos, n. 2, p. 4, 2017.

[91] Ibidem.

[92] BLUME, Peter. The inherent contradictions in data protection law. International Data Privacy Law, v. 2, n. 1, p. 27, 2012: "Seen from the perspective of the controllers, it is implied that data protection aims to make it legitimate to process personal data. (...) The fundamental observation is that data protection law is viewed as a societal necessity in order to make it possible for controllers to process personal data and to benefit from the information and knowledge processing entails".

[93] ABADE, André da Silva; ALVES, Josilene Dália. *Política de privacidade e dados pessoais*: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. *Facisa on-line*, Barra do Garças, n. 1, p. 125,

Fala-se, até mesmo, num pretenso direito à extimidade, que, sob o panorama psicanalítico, fundamenta-se na exteriorização voluntária da intimidade, em que o sujeito dá visibilidade ao "eu", no seu íntimo, nos seus segredos e nas suas singularidades[94]. Afinal, "considerando que o custo social da não exposição pode ser alto, os indivíduos acabam por expor a intimidade e o segredo, desejando fama, seguidores, interações, *likes*, scores e visualizações, numa autoafirmação constante, terminando por revelar dados pessoais, padrões sociais e informações de preferências"[95]. Dessa forma, não é viável "traçar um limite, como se o mundo da defesa da privacidade e o da ação pública fossem hostis ou não comunicantes; não existe uma separação, mas um *continuum*"[96], tornando-se a privacidade, então, fluida.

Sob a ótica institucional brasileira, por mais que a Constituição Federal coloque a proteção à privacidade como uma das pedras de toque do ordenamento jurídico e o STF tenha, ao que se indica, reconhecido a autonomia do direito fundamental à proteção de dados – ambos enquanto manifestações da dignidade da pessoa humana –, parece que o cidadão brasileiro não se atentou à necessidade de promover uma defesa integrada do direito.

Isso porque, embora a LGPD seja muito relevante e esteja na ordem do dia, dada sua recente vigência completa, ela ainda não parece ter ganhado efetivamente os círculos de diálogo social e, muito menos, a preocupação dos gestores de dados com o cumprimento de suas diretrizes. O *Facebook*, por exemplo, fez menções extremamente pontuais e superficiais à lei. O mesmo se pode dizer de legislações mais antigas e específicas – *habeas data*, CDC, Lei de Acesso à Informação, Marco Civil da Internet, entre outras –, que tutelam a proteção de dados em cada ambiente jurídico específico. Parece, então, que se vive em uma mata de invasão de privacidade com alguns esparsos clarões de tutela da vida privada e dos dados pessoais, sendo que o contrário deveria ser a verdade[97].

Os países europeus, em razão do aumento do fluxo dos dados pessoais como uma importante mercadoria, seguiram a mesma linha atualizaram suas legislações antes do que o Brasil: na Alemanha, o Ato Federal de Proteção de Dados (*Bundesdatenschutzgesetz* – BDSG); no Reino Unido, o Ato de Proteção de Dados de 1998, do Parlamento (*Act* 1998, de 16 de julho

---

jul. 2017.

[94] BOLESINA, Iuri. O direito à extimidade: as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017, p. 182.

[95] PESSOA. João Pedro Seefeldt. *O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI*. -- Porto Alegre, RS: Editora Fi, 2020.

[96] RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 47.

[97] ABADE, André da Silva; ALVES, Josilene Dália. *Política de privacidade e dados pessoais*: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. *Facisa on-line*, Barra do Garças, n. 1, jul. 2017.

de 1998); mais recentemente, os Estados Unidos e o Japão manifestaram preocupação com esse tratamento de dados, com a legislação *Safe Harbor* e o Ato de Proteção de Informações Pessoais, respectivamente[98].

De modo geral, o cerne de todas as legislações era o mesmo: estabelecer garantias mínimas para que os cidadãos tivessem algum controle – ainda que diminuto – sobre as informações pessoais que seriam tratadas e, de alguma forma, chegariam a conhecimento de terceiros. Nesse sentido, algumas regras dos *fair information principles* (princípios de informação justa)[99] eram:

> a) não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo; b) deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada; c) deve existir um meio para um indivíduo evitar que a informação a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento; d) deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito; e) toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados social[100].

Em uma análise ainda incipiente desses requisitos estabelecidos por todas as normas de proteção de dados, percebe-se que, em primeiro lugar e em tese, todos os sistemas de armazenamento de dados pessoais quando da utilização de aplicações da internet não estão em segredo, uma vez que o usuário expressamente consente com toda a utilização quando aceita a instalação ou utilização dos aplicativos – mesmo que não se atente exatamente para o que está assentindo. Ou, outra solução seria apostar no tratamento baseado no legítimo interesse.

Em segundo lugar, embora o RGPD tenha se atentado para o direito de acesso aos dados pessoais, o que foi posteriormente potencializado com o escândalo do *Facebook*[101], e o mesmo direito tenha sido previsto na LGPD, é certo que os usuários ainda não conseguem

---

[98] FERNANDES, David Augusto. *Dados pessoais*: uma nova *commodity*, ligados ao direito a intimidade e a dignidade da pessoa humana. *Revista Jurídica*, Curitiba, n. 49, p. 369, 2017.

[99] É importante contextualizar que esses princípios foram pensados no bojo da Organização para Cooperação e Desenvolvimento Econômico (OCDE), o que demonstra o caráter de relevância econômica da proteção de dados pessoais. Afinal, havendo um fluxo global de informações e dados, é necessário que haja um mínimo múltiplo comum em termos de normas de proteção de dados pessoais.

[100] Ibidem, p. 370.

[101] UOL. *Como descobrir o que o Facebook sabe sobre você*. São Paulo, 2018. Disponível em: <*https://tecnologia.uol.com.br/noticias/bbc/2018/03/27/como-descobrir-o-que-o-facebook-sabe-sobre-voce.htm?cmpid=copiaecola*>. Acesso em: 16 abr. 2021. Veja-se que essa ferramenta não é recente, mas certamente não era de conhecimento dos usuários: BBC Brasil. *Como descobrir o que o Facebook sabe sobre você*. São Paulo, 2018. Disponível em: <*http://www.bbc.com/portuguese/noticias/2015/11/151014_facebook_salasocial_informacoes_cc*>. Acesso em: 16 abr. 2021.

operar corretamente tal funcionalidade, sobretudo nas plataformas menores. E, noutro giro, também é difícil garantir que aqueles dados fornecidos são efetivamente os únicos que a empresa detém acerca do usuário, na medida em que se trata de uma declaração unilateral.

Em terceiro lugar, os usuários têm o conhecimento – ou deveriam ter – de que seus dados coletados podem ser usados para fins publicitários, pois anuem com essa condição ao instalar o aplicativo. A discussão central é saber até que ponto esse conhecimento realmente é suficiente para que a manifestação de vontade seja, ou não, consciente e informado.

Em quarto lugar, e novamente em tese, as companhias que detêm os dados possuem ferramentas de *compliance* para evitar o mau uso. Mas, como se viu pelo caso do *Facebook* – que certamente não é isolado, mas apenas o primeiro a ter o estopim midiático; nessa linha, houve tantos outros mais recentes no próprio Brasil –, as políticas de *compliance* não estão funcionando corretamente.

De modo mais geral, os *fair information principles* emanam seus preceitos para seis princípios basilares no tratamento dos dados: transparência, qualidade ou exatidão dos dados coletados, finalidade, livre acesso, segurança física e lógica e publicidade dos bancos de dados que tratem de informações pessoais.

Os dois que merecem maior destaque são a finalidade e o livre acesso: aquele seria a imposição de que os dados coletados efetivamente fossem utilizados apenas para os fins especificados quando da assinatura do consentimento[102]; este seria a possibilidade efetiva de os sujeitos dos dados coletados terem acesso às informações efetivamente possuídas e, em última análise, corrigi-las[103].

Por sua vez, sabe-se que o tratamento de dados é, de acordo com o conceito legal, "*toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*" (art. 5º, X, da LGPD).

No âmbito do tratamento – coleta, transmissão, processamento e posterior utilização da informação –, hoje se vive o paradigma do *profiling* (perfilamento), que se trata de "*qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar*

[102] LGPD, artigo 6º, I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
[103] LGPD, artigo 6º, IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (art. 4º do RGPD). Para a LGPD, tais dados utilizados para os fins de formação de perfil comportamental de pessoa natural identificada são dados pessoais (art. 12, § 2º).

Ou seja, constrói-se uma metainformação com hábitos, preferências pessoais e diversos registros da vida privada do usuário, com o objetivo de tentar prever, a partir dos dados pretéritos, tendências futuras e decisões de uma pessoa ou grupo, acerca dos mais variados gêneros de informação, desde publicidade comportamental até saber se o usuário tem algum potencial suicida ou terrorista[104].

Para além desses comentários de ordem institucional, estabelece-se que os usuários podem, sim, consentir com a utilização de seus dados pessoais – independentemente de sensíveis ou não sensíveis, com as exceções de dados que já sejam públicos ou aqueles casos em que a legislação dispense o consentimento – para determinadas finalidades legítimas. Dois critérios são necessários: (i) a manifestação do consentimento deve ser livre, expressa e inequívoca; e (ii) os provedores de aplicação devem explicitar a utilização dos dados coletados.

Nessa linha, um dos poucos estudos[105] com abordagem analítica de algumas aplicações *online* – mas mais voltado a sítios eletrônicos, ou seja, diferente do objetivo do presente trabalho – chegou ao resultado de que as plataformas de comércio eletrônico (*Mercado Livre* e *Americanas*) e os portais de serviços (*Google*) conseguem um desempenho adequado em termos de transparência sobre coleta e uso de dados. Ao revés, as redes sociais (*Facebook*, *WhatsApp* e *Twitter*) possuem um desempenho extremamente preocupante, especialmente no que tange à adequação dos termos de privacidade às exigências da legislação e ao não tratamento diferenciado de dados considerados sensíveis – que exigiriam, em tese, uma coleta muito mais restrita –, sendo que o *WhatsApp*, especialmente projetado para funcionar em celulares, teve o pior desempenho.

---

[104] Tal padrão de fazimento de perfis futuros com base no passado acaba limitando as liberdades individuais do sujeito, pois se espera que ele se comporte de acordo com os padrões interpretados de seus dados pessoais colhidos online. Ou seja, não se tenta buscar pessoas capazes de inovar em aspectos comportamentais, mas apenas na manutenção do status quo ante: trata-se de um discurso legitimador de governar o futuro pelos comportamentos passados. Não se nega a importância da análise histórica, mas a própria história mostra que padrões podem ser superados, tanto em âmbito coletivo quanto individual.

[105] ABADE, André da Silva; ALVES, Josilene Dália. *Política de privacidade e dados pessoais*: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. *Facisa on-line*, Barra do Garças, n. 1, jul. 2017.

Nesse âmbito específico das redes sociais, diz-se que "empresas de tecnologia vendem as informações pessoais para outras, tanto de âmbito nacional quanto internacional, mas para isso usam formas de chamar a atenção e fazem testes com as pessoas (está no contrato de adesão que as pessoas clicam ao se cadastrarem) sem que estas percebam (ex: o arco-íris e reconhecimento facial à distância)". São criados ícones de interação de acordo com o perfil de cada cliente, sendo que "as empresas de tecnologia não precisam que o usuário clique '*enter'* para ter a informação desejada, pois tudo que escrevemos fica gravado, mesmo não clicando nesta tecla"[106].

Como dito anteriormente, a defesa das empresas é não se tratar de uma violação à privacidade ou à proteção de dados: afirmam que esse acesso aos dados pessoais é devidamente consentido pelos usuários. O interesse econômico nas informações é nítido: com a mudança do panorama anterior – de que as empresas iriam até seus clientes por meio de panfletos – para o atual – de que os consumidores são induzidos às empresas por meio da publicidade digital específica e personalizada –, o *Facebook* tem uma receita 86% composta da publicidade comportamental; a *Google*, de modo ainda mais impressionante, tem sua receita composta em 96% da publicidade[107]. Como dados pessoais valem muito! E eles são entregues – muitas vezes sem sequer saber – mesmo sem se ganhar nada por isso.

Ou seja, o acesso às redes sociais deixa um rastro capaz de formar um perfil fidedigno do usuário e que, por tal razão, é cobiçado por quem deseja vender seus produtos ou serviços. A ideia de os dados pessoais serem vistos como a *commodity* do Século XXI é relacionada ao baixo valor agregado que essas informações em estado bruto, mas, quando devidamente tratadas por rotinas especializadas de programação, possuem um elevado valor agregado: sobretudo quando se considera o lucro que pode advir de uma publicidade comportamental pessoalmente projetada, o que é uma realidade no mercado mundial[108].

Na análise empírica do nível de consciência dos usuários sobre a política de privacidade, sobre a privacidade em si e sobre o valor dos dados pessoais, a maioria dos usuários questionados – larga maioria, aliás – informou conhecer a importância da privacidade e o que seria política de privacidade. Além disso, usuários mais idosos não dão tanta importância à

---

[106] ESTRADA, Manuel Martín Pino. *O comércio bilionário de dados pessoais na internet*. *Acadêmica Faculdade Progresso*, Guarulhos, n. 2, p. 15, 2017.
[107] Ibidem, p. 16.
[108] FERNANDES, David Augusto. *Dados pessoais*: uma nova *commodity*, ligados ao direito a intimidade e a dignidade da pessoa humana. *Revista Jurídica*, Curitiba, n. 49, p. 360, 2017.

preservação da privacidade digital – talvez por, pelos dados da pesquisa, não saberem o que é política de privacidade[109].

Infelizmente esse dado é sensível, pois certamente todos os *players* da internet sabem que as pessoas de mais idade não realizam um acompanhamento tão diligente de como seus dados podem ser utilizados – os mais jovens também não, diga-se. E, a depender da política de privacidade da plataforma, é justamente por meio desses usuários menos experientes digitalmente que as empresas interessadas na análise e *comercialização* dos dados pessoais dos usuários terão acesso àqueles dados que realmente interessam, de usuários normalmente mais resguardados.

Um exemplo disso é o recente escândalo de vazamento de informações – inclusive informações de *amigos digitais* dos usuários que expressaram a concordância, ou seja, em nítida violação ao limite do consentimento – do *Facebook*[110]. Esse é um nítido exemplo de quando a invasão da privacidade do usuário é ilegítima, sobretudo porque não houve manifestação do consentimento; mas há inúmeras *zonas cinzentas* em que o acesso aos dados, apesar de ser moralmente questionável, é juridicamente factível.

Embora os usuários de maior idade pareçam ser os mais vulneráveis em termos de assimetria informacional sobre o funcionamento das plataformas, segundo o estudo analisado, eles compõem o segmento que menos manifesta consentimento com o acesso aos dados pessoais pelas aplicações *online*[111].

Por outro lado, apesar de a maioria informar que não consente com o fornecimento dos dados ou que sabe o que são política de privacidade e importância dos dados pessoais, a falta de transparência parece ser uma regra nessa discussão: a larga maioria dos usuários (i) não tem qualquer ideia de como os dados pessoais são armazenados ou protegidos, (ii) não conhece os termos de privacidade dos serviços digitais utilizados, (iii) não sente segurança em saber que seus dados pessoais são armazenados na *nuvem* e (iv) não conhece a legislação que resguarda os usuários quanto aos seus dados pessoais[112].

---

[109] ABADE, André da Silva; ALVES, Josilene Dália. *Política de privacidade e dados pessoais*: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. *Facisa on-line*, Barra do Garças, n. 1, p. 138, jul. 2017.

[110] FOLHA DE SÃO PAULO. *Depois da Cambridge Analytica, especialistas em privacidade têm direito ao 'eu não disse?'*. São Paulo, 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/04/depois-da-cambridge-analytica-especialistas-em-privacidade-tem-direito-ao-eu-nao-disse.shtml>. Acesso em: 15 abr. 2021.

[111] ABADE, André da Silva; ALVES, Josilene Dália. *Política de privacidade e dados pessoais*: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. *Facisa on-line*, Barra do Garças, n. 1, p. 139, jul. 2017.

[112] Ibidem, p. 140.

A leitura, então, parece paradoxal: a maioria dos usuários informa saber a importância de resguardar seus dados pessoais, mas também informa não saber nada sobre como seus dados capturados são utilizados pelas empresas de tecnologia. E, do ponto de vista institucional, surge a assimetria legislativa: poucos informam saber a qual lei precisariam recorrer se se sentissem prejudicados pela atuação empresarial.

Então, em última análise, parece que se *trabalha de graça para empresas de tecnologia*, na medida em que alguns dados pessoais são exigidos para participar das redes sociais existentes: os "termos de uso" acabam exigindo que o usuário concorde com todos os termos de privacidade dos dados pessoais, senão ficarão excluídos da utilização da aplicação. Trata-se de uma decisão tudo ou nada. Como ressalta a literatura,

> as empresas de tecnologia oferecem um email "grátis" com muitos aplicativos, só que na verdade nada tem de grátis, e os aplicativos que oferecem gratuitamente, na verdade estão para vasculhar a privacidade, a intimidade, saber dos gostos, dos desejos de consumo, orientação política, orientação sexual, tendências criminosas, se é um mal pagador e assim por diante, nenhum aplicativo é de graça e muito menos para oferecer serviços ao usuário, pelo contrário, serve para vasculhá-la até o final, assim, o nosso perfil na nuvem vai sendo carregado todos os dias através do uso do e-mail, da redes sociais virtuais (não necessariamente o *Facebook*), chegando um nível que, de tanto tempo de usá-los poderá ser possível as condutas futuras e desta forma direcionar propagandas específicas e individuais através da internet[113].

Então, vê-se que a delimitação aqui pretendida é polêmica. Parece haver um consenso de ordem prática: o Brasil vem regulando e fiscalizando mal como as empresas de tecnologia utilizam os dados pessoais de seus usuários, com principal crítica à falta de transparência na utilização: não seria um problema utilizar, afinal haveria interesse econômico legítimo, apesar de moralmente questionável; o problema é utilizar e não explicar onde e por que estão sendo utilizados.

Nesse contexto, a solução parece caminhar no sentido de termos maior respeito à legislação posta. Contudo, esse cenário regulatório não é simples, uma vez que a indústria da tecnologia é extremamente volátil. Para fazer o cotejo de como compatibilizar privacidade, proteção de dados e tecnologia, é necessário saber, antes, o que se entende por privacidade e proteção de dados. É o que se passa a fazer.

2.3 Conteúdo jurídico do direito à privacidade

[113] ESTRADA, Manuel Martín Pino. *O comércio bilionário de dados pessoais na internet*. *Acadêmica Faculdade Progresso*, Guarulhos, n. 2, p. 19, 2017.

Na Antiguidade Clássica – cultura grega posteriormente passada à romana –, falava-se na distinção entre o espaço público, comum aos cidadãos livres (*pólis*), e o privado, particular dos indivíduos (*oikos*). O privado consistia no material, âmbito em que a pessoa se submetia às necessidades da própria natureza humana, ou seja, trata-se de uma preocupação concreta com a própria sobrevivência em pequenas comunidades, e não em qualquer espécie de atividade meramente contemplativa com vistas apenas à promoção de um sentimento de liberdade[114].

Nesse particular, a concepção era de que, ao adentrar na esfera pública da *polis*, o cidadão recebia uma segunda vida (*bio politikos*), relacionando-se com o que lhe é comum (*konion*), e não mais com o que lhe é próprio (*idion*). A convivência pública significava, aqui, *status* social[115]. A diferença, então, era de que o privado se relacionava ao âmbito familiar, ao passo que o público, ao político[116].

Na Idade Média, começou-se a conceber a privacidade como isolamento, na medida em que a vida privada tornou-se costume entre as famílias nobres e, portanto, também começou a denotar *status*. As práticas corriqueiras – *e.g.*, necessidades fisiológicas ou atos sexuais – começaram a ser encobertas, mas o isolamento ainda era uma realidade de poucos[117].

O lar passa a significar uma verdadeira separação com o ambiente comum e público. A casa não é mais vista como espaço de discussões menores, mas como verdadeiro centro de representação do poder político. Desse contexto, algumas casas começam a ser identificadas como símbolos das grandes dinastias, sobrenomes, ou como novos centros do poder político[118].

Posteriormente, a burguesia emergente tem ainda maior apreço pela individualidade, na sua busca por tentar levantar barreiras para proteger um lugar apenas seu, ampliando a distância entre locais de habitação e de trabalho. Fortaleceu-se a noção do que era privado, o que também guardou estrita relação com o próprio direito à propriedade[119].

A mudança é interna, uma emancipação psicológica: a privacidade passa a significar uma verdadeira expressão da personalidade, que permite a singularização do

---

[114] ARENDT, Hannah. *A condição humana*. 10 ed. Rio de Janeiro: Forense Universitária, 2005, p. 33.
[115] CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.
[116] PESSOA. João Pedro Seefeldt. *O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI*. -- Porto Alegre, RS: Editora Fi, 2020.
[117] CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.
[118] DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 125.
[119] RODOTÀ, Stefano. *A vida na sociedade de vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 26.

indivíduo perante a sociedade. Essa novidade passou a ser tão importante que, no século XIX, começaram a surgir os contornos próprios do direito à privacidade[120].

A discussão ganhou contornos especiais no marco filosófico do liberalismo, dentro do qual John Locke defendeu "a existência de uma esfera de liberdade natural a cada sujeito, um espaço que deve ser impenetrável à coerção que o direito civil impõe", com o fito de que "a privacidade seja considerada o bem mais sagrado da pessoa humana, pois todo homem tem um bem em sua própria pessoa"[121].

John Stuart Mill, de modo similar, afirmou que as condutas humanas que seriam analisáveis em cotejo com um *standard* social ou jurídico seriam apenas aquelas que produziam obrigações e deveres sociais que afetassem terceiros. Ou seja, há aspectos da vida e de suas diversas facetas que dizem respeito somente ao indivíduo, notadamente as características privadas, independentes de qualquer espécie de crivo pela esfera pública. Trata-se do aspecto em que o indivíduo é efetivamente soberano sobre si[122].

Hannah Arendt descreve que, na esfera social, as pessoas interagem umas com as outras a partir da necessidade de trabalhar, negociar e afins. Ou seja, a manifestação da pessoa dentro da esfera social é, de certo modo, limitada pelos próprios padrões de comportamento. Na vida íntima, por sua vez, dado o princípio da exclusividade, como as pessoas conseguem escolher precisamente com quem conviver e partilhar momentos e fatos, há nítida manifestação da pessoa em sua singularidade. Ou seja, a privacidade contemplaria três atributos: o direito de estar só (solidão), o direito de exigir sigilo (segredo) e o direito de decidir sobre si mesmo (autonomia)[123].

Ou seja, a privacidade é interna ao homem, uma manifestação de sua personalidade em aspecto íntimo, que contribui para sua formação como humano. Não se trata, portanto, de mera segmentação entre público e privado, mas de verdadeira defesa da autodeterminação psicossocial, o núcleo essencial da pessoa[124].

---

[120] Ibidem.
[121] TARODO, Salvador Tarodo. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: Derecho y Salud, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006, p. 136. Tradução livre.
[122] MILL, John Stuart. *A liberdade*. São Paulo: Martins Fontes, 2000.
[123] ARENDT, Hannah. *Reflections on Little-Rock*. Dissent Magazine, v. 6, n. 1, inverno, 1959, p. 52-53.
[124] MACHADO, Joana de Moraes Souza. Caminhos para a tutela da privacidade a sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil. 2014. 186 p. Tese (Doutorado) - Fundação Edson Queiroz, Universidade de Fortaleza, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito Constitucional, 2014. Disponível em: <http://uolp.unifor.br/oul/ObraSiteLivroTrazer.do?method=trazerLivro>. Acesso em: 21 mar. 2021.

A conduta protegida aqui é o recorte de quais aspectos da vida pessoal – justamente por se referirem apenas ao pessoal – podem ser conhecidos ou acessados por terceiros. A privacidade é a faculdade de fazer concessões no terreno mais reservado de sua existência[125].

No que toca à diferenciação entre tutela da intimidade e da vida privada, há os que seguem a linha de se tratar de mero preciosismo – na medida em que o constituinte teria usado os dois termos apenas para fins de tutelar qualquer aspecto íntimo da pessoa[126] –, mas também há aquelas que propõe a divisão conceitual, com base na teoria alemã das esferas.

Trata-se de desenvolvimento de Heinrich Hubmann, que se utiliza da figura as esferas concêntricas para a representação dos diversos graus de manifestação do sentimento de privacidade. Fala-se em: esfera da vida privada (*Privatsphäre*), onde se encontram as informações que a pessoa deseja não serem de domínio público; esfera da intimidade (*Vertrauensphäre*), onde se localizam as informações que a pessoa confidencia, em reserva, somente a determinados sujeitos; esfera do segredo (*Geheimnsphäre*), onde se encontram as informações que a pessoa não compartilha com ninguém ou apenas com pouquíssimas pessoas; e, maior do que todas, fala-se na própria esfera pessoal, que abrangeria também a própria vida pública (*Öffentlichkeit*) e não sujeita a uma proteção mais estreita pela privacidade[127].

A esfera da privacidade trataria das relações de maior proximidade emocional e dos nosso dados pessoais mais públicos, tais como endereço, telefone, inscrição no CPF. No âmbito da esfera da intimidade, a mais densa das três, fala-se em informações confidenciais sobre segredos familiares, domésticos e profissionais, de modo que se fala em inviolabilidade de domicílio e sigilo de comunicações privadas, telemáticas, telefônicas, informáticas.

Tal esfera, portanto, abarcaria o mundo intrapsíquico do indivíduo. Pode-se dizer que a intimidade protege a manifestação pessoal do indivíduo, ao passo que a vida privada protege o contexto, um dado bruto. Por sua vez, o núcleo do segredo é, como se espera, o mais fechado, sendo revelado a poucas pessoas ou a ninguém. Pode-se falar, hoje, em alguns dados pessoais sensíveis, por exemplo[128].

---

[125] ARDENGHI, Régis Schneider. Direito à vida privada e direito à informação: colisão de direitos fundamentais. Revista da ESMESC. [S.l.], v. 19, n. 25, p. 227-251, 2012. Disponível em: <http://revista.esmesc.org.br/re/article/view/57>. Acesso em: 21 mar. 2021.

[126] JABUR, Gilberto Haddad. A dignidade e o rompimento de privacidade. In: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (coordenadores). Direito à privacidade. São Paulo: Ideias e Letras , 2005. p. 85-106.

[127] HUBMANN, Heinrich. *Das persönlichkeitsrecht*. Münster: Böhlau-Verlag, 1953 apud COSTA JR. Paulo José da. O direito de estar só: tutela penal da intimidade. 2. ed. São Paulo: RT, 1995, p. 30-36.

[128] ESTRADA, Manuel Martín Pino. *O comércio bilionário de dados pessoais na internet*. *Acadêmica Faculdade Progresso*, Guarulhos, n. 2, p. 7, 2017.

A teoria alemã, contudo, acabou caindo em desuso, por sua insuficiência técnica e excesso de subjetivismo face à relação entre as esferas e a evolução tecnológica, além de considerar o indivíduo como uma verdadeira cebola passiva. Em seu lugar, é mais bem aplicável a teoria do mosaico, que sustenta a privacidade em contexto: a união de informações eventualmente irrelevantes em contextos específicos pode, em nova conjuntura, implicar a formação de pleno significado. Ou seja, não se fala mais em proteção segmentada da privacidade, mas macroscópica e contextual[129]. Aliás, o apelo era proteção à privacidade contextual provém até mesmo dos ensinamentos de *law and economics*[130].

Pouco antes do desenvolvimento da teoria alemã das esferas, porém, foi possível verificar o marco jurídico do que se alcunhou *right to privacy* (direito à privacidade): o trabalho de Warren e Brandeis, profícuo ex-juiz da Suprema Corte dos Estados Unidos. O contexto da discussão teria sido o suposto vazamento não autorizado de fatos íntimos a respeito do casamento da filha de Warren, ou seja, tratava-se de verdadeira preocupação com a tutela da personalidade humana[131].

Contemporaneamente, o também ex-Juiz Thomas Cooley cunhou a expressão *right to be let alone* (direito de ser deixado só) – claro que isso não tutelava apenas o sentido literal de solidão, na medida em que também se fala em privacidade exercida coletivamente –, em clara preocupação com o fato de que fotografias instantâneas e empresas de comunicação teriam devassado a privacidade do lar[132].

Já àquela época, falava-se na ameaça de numerosos dispositivos tecnológicos: "aquilo que é sussurrado na alcova deve ser berrado no telhado", na medida em que a fofoca – anteriormente, mero vício ocioso – teria se tornado um verdadeiro instrumento de barganha,

---

[129] CONESA, Fulgencio Madrid. Derecho a la intimidad, informática y Estado de Derecho. Valencia: Universidad de Valencia, 1984, p. 45.

[130] "As noted, extracting economic value from data and protecting privacy do not need to be antithetical goals. The economic literature we have examined clearly suggests that the extent to which personal information should be protected or shared to maximize individual or societal welfare is not a one-size-fits-all problem: the optimal balancing of privacy and disclosure is very much context dependent, and it changes from scenario to scenario. In fact, privacy guarantees may be most needed precisely when the goal is to extract benefits from the data. In the healthcare realm, for instance, if privacy risks are not addressed, public concern might end up outweighing public support for initiatives that rely on extensive collection of patients' medical records (Kohane, 2015). Thus, it stands to reason that, case by case, diverse combinations of regulatory interventions, technological solutions, and economic incentives, could ensure the balancing of protection and sharing that increases individual and societal welfare". *In*: ACQUISTI, Alessandro; TAYLOR, Curtis; WAGMAN, Liad. *The Economics of Privacy*. Disponível em: <https://www.ftc.gov/system/files/documents/public_comments/2017/10/00006-141501.pdf>. Acesso em: 4 jun. 2021.

[131] WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. Harvard Law Review, v. IV, n. 5, December, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 21 mar. 2021.

[132] CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.

um produto comercializável[133]. Passados quase 150 anos, a preocupação parece não ser muito diferente da externada na presente análise.

Como o objeto da preocupação era a própria fofoca, por mera decorrência conceitual, os amparados pela proteção à privacidade seriam apenas os abastados: afinal, ninguém teria interesse econômico na vida ordinária. Esse cenário começou a mudar de rumo a partir da década de 1960, com o desenvolvimento da tecnologia de coleta e sensoriamento, o que implicou exponencial crescimento do recolhimento, processamento, utilização e circulação das informações.

O contexto, portanto, é de verdadeira democratização da tutela da privacidade[134]. Um dos maiores exemplos de que a tutela da privacidade teria deixado de ser mero privilégio de abastados preocupados com fofocas indevidas foi a Declaração Universal dos Direitos Humanos, de 1948, que afirma, em seu art. 12, que "*ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataque, toda a pessoa tem direito a proteção da lei*"[135].

Em verdade, a ideia embrionária de proteção legal à privacidade foi gestada no bojo da Declaração dos Direitos do Homem e do Cidadão de 1789, que afirmava que "ninguém deve ser incomodado por suas opiniões, inclusive religiosas, sempre e quando sua manifestação não perturba a ordem pública estabelecida pela Lei"[136].

No Brasil, a onda democrática trazida pela Constituição Federal de 1988 optou por não utilizar o termo *privacidade*: a opção do legislador constituinte foi pelos termos *vida privada* e *intimidade*. De uma ou outra forma, o cerne ainda é o mesmo: trata-se da tutela de uma liberdade da pessoa, uma verdadeira necessidade do homem.

Trata-se, além disso, de uma decorrência da escola americana da privacidade, cujos dois elementos centrais – privacidade e intimidade – asseguravam ao indivíduo o direito de determinar a extensão de sua vida privada que poderia ser conhecida ou divulgada. Contudo,

---

[133] CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.

[134] DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. 2000. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>. Acesso em: 21 mar. 2021.

[135] UNICEF. Declaração Universal dos Direitos Humanos. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 5 abr. 2021.

[136] FRANÇA. Déclaration des Droits de l'Homme et du Citoyen de 1789. Disponível em: <https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789>. Acesso em: 3 jun. 2021.

como o *right to privacy* permitiria a não divulgação de informações verdadeiras, afastou-se a sua incidência nos casos de interesse público geral, autorização legal e, claro, consentimento.

Não necessariamente uma devassa à privacidade significará uma quebra indevida da intimidade. Ao se invadir uma casa, por exemplo, certamente você estará violando a vida privada; a depender das circunstâncias internas, também a intimidade. Embora haja inegável fluidez entre os conceitos, é certo que tal teoria contribui sobremaneira para a diferenciação entre público e privado[137].

De modo geral, contudo, há certo consenso no que se tutela pela vida privada: convívio pessoal e familiar do indivíduo, círculo próximo da pessoa e importante forma de desenvolvimento de relações sociais e valores essenciais. O elemento central da vida privada seria a intimidade. Essa é a proteção da Constituição Federal e da própria legislação infraconstitucional, alçando o direito à privacidade ao patamar de um direito da personalidade e verdadeiro direito fundamental. Aliás, essa vem sendo a regra em outros países[138].

Com efeito, o direito à privacidade começou a existir enquanto decorrência dos direitos da personalidade na legislação civil ordinária, sendo posteriormente reconhecido como direito constitucional fundamental. Seguindo a tendência, "dentre as constituições atuais, observa-se que algumas Cartas preveem a privacidade apenas de forma genérica; em outras, a privacidade nos meios de comunicação e, por fim, há aquelas que protegem a privacidade sob esses dois aspectos e também a privacidade informacional, como as de Portugal, Hungria, Eslovênia e Rússia"[139].

Servindo quase como um paradigma da inovação normativa no ponto, a Constituição espanhola, "além de garantir o direito à intimidade e à vida privada, à privacidade do domicílio, à privacidade das comunicações, ainda limita o uso da informática para garantir a intimidade pessoal e familiar (artigo 18)". Então, hoje, a "maior parte dos países democráticos tutela a privacidade na própria Constituição, exceto alguns países da raiz *common law*, como o Reino Unido, que reconhece o direito à privacidade mediante jurisprudência"[140].

Dentro desse panorama, é inarredável a conclusão de que a tutela da privacidade implica verdadeira proteção e promoção da dignidade da pessoa humana (art. 1º, III, da

---

[137] CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.

[138] VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 p. Dissertação (Mestrado) - Universidade de Brasília, Faculdade de Direito, Programa de Pós-Graduação em Direito, Estado e Sociedade, 2007. Disponível em: <http://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf>. Acesso em: 21 mar. 2021.

[139] Idem.

[140] Ibidem.

Constituição[141]). Como direito fundamental que é, a tutela da privacidade deveria ser encarada pelas óticas de liberdade negativa, limitadora, e positiva, prestacional.

Contudo, a legislação brasileira parece enxergá-la apenas sob o viés de freio ao Estado ou aos demais particulares sob o paradigma de eficácia horizontal dos direitos fundamentais, limitando-se a tutelá-la com a responsabilidade civil. Ou seja, via de regra, o máximo que uma violação à privacidade implicará é uma indenização. Sob a ótica prestacional, deveria haver maiores incentivos à mudança de mentalidade dos *players*, para que realmente fosse factível se cogitar de uma privacidade por projeto, desde a concepção.

Posta em contexto, a Constituição Federal é quase contemporânea ao próprio *boom* tecnológico e à era da supervalorização da informação. A partir do início da década de 1990, a internet surgiu como um novo espaço social de coletivização dos dados: agora, as informações privadas não ficavam mais restritas à comunidade micro em que a pessoa vivia, mas potencialmente podiam atingir toda a coletividade. Na internet, tudo passa a ser armazenado e lá é desenvolvida e expressada a personalidade e a individualidade de cada um[142].

Não obstante todos os inegáveis benefícios trazidos pela nova tecnologia, no que tange à privacidade, ela também trouxe duas dificuldades intrínsecas: (i) diferentemente do plano físico e material, no ambiente digital, não se sabe quem está notando quais de suas pegadas; e, pela própria abrangência da rede, (ii) não se tem a real dimensão do alcance do ato, na medida em que a disseminação daquele conteúdo pode até mesmo chegar a ser viral.

Quem não se lembra do vídeo feito para celebração religiosa de adolescente, que deveria ter sido exibido apenas no modo privado, mas ganhou intensa repercussão indevida[143]? Apesar de, nesse caso, o conteúdo ter sido uma aparente brincadeira – não se descarta que tenha causado sofrimento ao adolescente e aos seus familiares, tanto é que o caso foi levado ao Poder Judiciário –, a discussão pode ficar muito mais séria, havendo inclusive manifestação de preconceitos de toda ordem[144].

---

[141] Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) III - a dignidade da pessoa humana.

[142] GREENWALD, Gleen. Sem lugar para se esconder. Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

[143] EXAME. Justiça determina que YouTube remova vídeo de Nissim Ourfali. Disponível em: <https://exame.abril.com.br/tecnologia/justica-determina-que-youtube-remova-video-de-nissim-ourfali/>. Acesso em: 22 mar. 2021.

[144] A título exemplificativo: CORREIO BRAZILIENSE. Mãe luta para banir memes na internet com foto do filho deficiente. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/mundo/2016/02/01/interna_mundo,516149/mae-luta-para-banir-memes-na-internet-com-foto-do-filho-deficiente.shtml>. Acesso em: 22 mar. 2021.

O que é peculiar é que a internet, além de conceber um pernicioso modelo de *invasão* de privacidade – que é o cerne da discussão do presente trabalho –, também passou a abarcar um notável movimento de *evasão* da privacidade, ou seja, uma publicização deliberada de fatos da vida privada.

Nas palavras de Bauman, "o medo da exposição foi abafado pela alegria de ser notado", na medida em que a existência só é válida e efetiva quando exposta[145]. Esse conceito ajuda a entender o porquê de tanto sucesso de redes de compartilhamento de fotos, por exemplo. Outro ponto é que talvez os usuários ignorem – nos dois sentidos possíveis da expressão – que os conteúdos colocados na rede dificilmente podem dela ser removidos, especialmente quando se trata de exposição voluntária.

Discute-se muito, nessa esteira, a questão de um pretenso direito ao esquecimento em todo o cenário mundial. Embora a Europa já tenha chancelado a sua existência, por decisões judiciais[146] e pelo texto do próprio RGPD (embora mais com uma conotação no sentido do direito ao apagamento de dados[147]), os contornos ainda estão em discussão no Brasil. É claro que, recentemente, o STF concluiu ser incompatível com a Constituição a ideia do direito ao esquecimento no Brasil, mas deixou em aberto a análise de particularidades de casos concretos[148].

Para além disso, também não devem ser ignorados os requisitos previstos no art. 19 do Marco Civil da Internet, que estabelece a necessidade de ordem judicial com identificação específica do conteúdo a ser removido[149] (por meio de identificador consistente na URL

---

[145] BAUMAN, Zygmunt. Vigilância líquida: diálogos com David Lyon. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editor, 2014.

[146] UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção), 13 de maio de 2014. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>. Acesso em: 5 abr. 2021.

[147] "Artigo 17.º Direito ao apagamento dos dados («direito a ser esquecido») 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos: (...)".

[148] Foi fixada a seguinte tese: "É incompatível com a Constituição Federal a ideia de um direito ao esquecimento, assim entendido como o poder de obstar, em razão da passagem do tempo, a divulgação de fatos ou dados verídicos e licitamente obtidos e publicados em meios de comunicação social – analógicos ou digitais. Eventuais excessos ou abusos no exercício da liberdade de expressão e de informação devem ser analisados caso a caso, a partir dos parâmetros constitucionais, especialmente os relativos à proteção da honra, da imagem, da privacidade e da personalidade em geral, e as expressas e específicas previsões legais nos âmbitos penal e cível". Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1>. Acesso em: 5 abr. 2021.

[149] Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

específica – localizador uniforme de recursos, o *link* de cada sítio da internet[150]). Ou seja, os requisitos a serem cumpridos para se ter a tutela de remoção de conteúdo online são apertados.

Tudo isso é colocado em ainda mais holofote quando se considera que o dispositivo pelo qual mais se acessa a internet é o celular, que, por conceito, acompanha a trajetória do cotidiano humano em todos os seus diferentes cenários: desde instrumento de trabalho, até dispositivo para navegação, utilização de redes sociais, compartilhamento de imagens. Ou seja, o celular está em *todos* os lugares. Partindo-se dessa premissa, é de se cogitar que os dados privados das mais variadas situações vivenciadas estejam também em todos os lugares.

Nesse contexto, é de suma relevância pontuar que o simples compartilhamento de informações em rede não implica uma chancela para que aquela informação se torne integralmente pública. Afinal, por conceito, os direitos da personalidade são indisponíveis, se olhados em absoluto, e os direitos fundamentais são irrenunciáveis e inalienáveis. É claro que pode haver disposição parcial de aspectos dos direitos da personalidade[151], mas referida limitação ao espectro dos direitos da personalidade deve ser pontual e contextual. Isso é, não pode uma informação publicada nas redes sociais do usuário reclamando de dores de cabeça constantes ser usada *contra* si para negar um emprego ou majorar seu seguro de saúde.

Nesse sentido, "a exposição em público não pode ser o critério determinante para decidir se uma situação deve ser ou não considerada privada"[152] e o "simples fato de um local ter acesso aberto ao público não significa que tudo que seja dito ou praticado por uma pessoa em tal espaço possa ser legitimamente divulgado em cadeia nacional", afinal, "o que deve ser analisado não é o caráter público ou privado do local, mas a expectativa de privacidade em torno do ato captado naquelas circunstâncias concretas"[153].

Dessa forma, "ressaltar a importância do direito à privacidade, manifestado da maneira que for, é valorizar a liberdade, combater a discriminação e proteger as escolhas pessoais de cada um. Respeitar a privacidade é exercício de cidadania indispensável"[154]. Hoje se está tão preocupado com a tutela de direitos sociais e difusos de segunda e terceira dimensões, que quase se esquece da basilar tutela das próprias liberdades civis. A privacidade deve, sim,

---

[150] CONJUR. Indicação de URL é imprescindível para remoção de conteúdo da internet. Disponível em: <https://www.conjur.com.br/2020-jan-29/indicacao-url-imprescindivel-remover-conteudo-internet>. Acesso em: 5 abr. 2021.
[151] Não fosse possível, programas de *reality show* seriam inviáveis.
[152] LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2011, p. 366.
[153] SCHREIBER, Anderson. Direitos da personalidade. 2. ed. São Paulo: Atlas , 2013.
[154] CANCELIER, Mikhail Vieira de Lorenzi. *O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.

ser um tema de destaque, afinal, não é menos importante do que a luta pela valorização e pelo *enforcement* de qualquer outro direito fundamental[155].

Por fim – e como já se falou –, o atual paradigma da convivência online exige uma adaptação do conceito tradicional de Warren: hoje, a privacidade não deve ser mais vista como mera oposição à publicidade. Essa dicotomia absoluta chancelaria a ideia de que qualquer ato que transbordasse os limites claros da esfera do privado permite que se coletem e disseminem informações de modo descontrolado. Isso negligencia amplo espectro do âmbito de proteção do direito fundamental à privacidade[156].

O conceito, contudo, não é novo: Habermas já afirmava que o antônimo de privacidade é a indiscrição, e não a publicidade[157]. Essa mudança de prisma interpretativo possibilita que se harmonize o exercício público da privacidade, mais compatível com a contemporaneidade.

Ou seja, mesmo em público, a privacidade estará presente. Isso não desvirtua a clara percepção de que, ao legitimamente escolher pela publicidade de determinado ato, a pessoa tem pleno conhecimento de que o alcance da informação será ainda maior. Afinal, "proteger a privacidade em público não significa uma tutela absoluta, mas apenas representa a limitação de certas maneiras de usar e de revelar algumas informações, pois nem sempre o que foi feito em público" é, efetivamente, *público*[158].

Tendo tudo isso em mente, e voltando-se brevemente ao panorama brasileiro, vê-se que a tutela para casos de invasão de privacidade é apenas repressiva, seja civil (pagamento de indenização por danos morais e materiais) ou penalmente (Lei nº 12.737/2012 – conhecida como "Lei Carolina Dieckmann" –, que dispõe sobre a tipificação criminal de delitos informáticos, como um dos maiores exemplos). A lógica está invertida: deixa-se o dano acontecer para, se for o caso, tutelar a sua reparação, ao passo que a ideia geral deveria ser a de privacidade por conceito (*privacy by design*).

Esse arcabouço normativo nacional é mais bem investigado na sequência do trabalho. Antes, porém, é conveniente fazer uma aproximação possível ao problema de pesquisa. Isso porque, ao pretender investigar os termos de privacidade dos aplicativos, é inegável que, sob uma visão liberal mais clássica, referidos documentos sejam efetivamente

---

[155] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar , 2008.
[156] NISSENBAUM, Helen. Priavacy in context: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.
[157] HABERMAS, Jürgen. Mudança estrutural da esfera pública: investigações sobre uma categoria da sociedade burguesa. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014.
[158] LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2011, p. 367.

encarados como contratos massificados, feitos em ambiente eletrônico, e sob a técnica de adesão.

Mesmo numa visão mais moderna, não é fácil superar a constatação de se tratar de um ajuste de vontades, sobretudo pelo próprio paradigma do tratamento de dados baseado no consentimento. Contudo, ainda assim, hoje não mais se enxerga a política de privacidade como um contrato propriamente dito, no sentido de ser ajuste de vontades que serviria e legitimar a proteção mais alongada ou mais estreita do direito à privacidade e da proteção de dados.

Isso porque referidos direitos fundamentais têm eficácia imediata e são autoaplicáveis, por serem normas de eficácia plena. Então, não precisariam do instrumento contratual, ou do mero ajuste de vontade, para serem protegidos e tutelados no caso concreto. Contudo, como as políticas de privacidade são os instrumentos que, hoje, dispõem sobre os aspectos de proteção de dados e de privacidade no âmbito dos aplicativos de celulares, é necessário enfrentar, brevemente, alguns aspectos contratuais aplicáveis.

Essa discussão é relevante, pois, como se verá, mesmo sob o paradigma mais clássico de liberdades civis (autonomia contratual dita plena), ou, mais recentemente, sob a proteção dos mantos do arcabouço consumerista insculpido no CDC, também seria possível tutelar a privacidade dos usuários de aplicativos. Isso mesmo que inexistisse a regulamentação específica do MCI e da LGPD, ou seja, utilizando-se só de normas, precipuamente princípios, mais gerais e clássicos da dinâmica contratual.

Nessa esteira de argumentação, Marco Aurélio Bellizze afirma, por exemplo, que, embora a LGPD tenha entrado em vigor recentemente, "a privacidade do cidadão não esteve desamparada pelo ordenamento jurídico brasileiro, tal como é possível verificar não apenas do arcabouço legal anterior à LGPD, mas pela atuação dos tribunais superiores, de agências reguladoras (ANATEL) e por disposições da própria Constituição Federal"[159]. Nessa linha, há julgados do STF e do STJ da década de 1990 que repisam a importância da privacidade e da proteção de dados pessoais[160], inclusive em bancos de dados para o *scoring* (atribuição de nota)

[159] BELLIZZE, Marco Aurélio; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[160] Veja-se: "Não obstante, as medidas de proteção de dados não ficaram adstritas às previsões constitucionais – e nem poderiam. O avanço tecnológico fez-se sentir nos tribunais superiores, ainda na década de 1990. Menciona-se, aqui, o julgamento do RHD 22/DF, quando os Ministros Celso de Mello e Sepúlveda Pertence reforçaram a importância do habeas data na concretização do direito material, em especial, à personalidade, intimidade e proteção de dados pessoais. Outro julgado paradigmático para o tema é o Recurso Especial 22.337/RS, de relatoria do Ministro Ruy Rosado de Aguiar Júnior. A discussão acerca do tempo de prescrição da inscrição no cadastro do Sistema de Proteção ao Crédito (SPC) deu a oportunidade para que o relator registrasse sua preocupação com a crescente utilização de bancos de dados sem controle de finalidade, e advertisse que tais registros devem ser feitos

do consumidor, demonstrando que, já àquela época, o Poder Judiciário preocupava-se com a "coleta geral e indiscriminada dos dados pessoais"[161] dos brasileiros.

Bruno Bioni, no mesmo sentido, organizou coletânea de casos importantes que versaram sobre a temática da proteção de dados pessoais mesmo antes da LGPD, sobretudo com foco na análise do consentimento – informado, livre, expresso e inequívoco – e nos deveres de informação e transparência. Ou seja, mesmo antes de se conceber uma proteção mais completa aos dados pessoais no Brasil, havia relevante debate jurídico sobre o tema[162].

Assim, com base em uma interpretação sistemática das normas existentes, sobretudo aquelas principiológicas, já era "possível" promover uma proteção aos dados pessoais minimamente razoável no Brasil antes mesmo da LGPD, "particularmente para as relações de consumo estabelecidas na internet"[163].

É claro que a proteção de dados pessoais não esteve totalmente desamparada antes da vigência da LGPD, mormente devido, para além das normas mais específicas (fala-se na lei da política nacional de arquivos públicos e privados, na lei do *habeas data*, na LAI, no CDC, no Código Civil, na lei do cadastro positivo, no MCI), ao próprio panorama geral contratual e constitucional.

A posição aqui defendida é convergente com a de Ricardo Villas Bôas Cueva, para quem "a edição de lei nacional de proteção dos dados pessoais é essencial para suprir as omissões hoje existentes e garantir um nível adequado de proteção" (posição manifestada antes da aprovação da LGPD). Isso porque, como defende Cueva, a limitada aplicabilidade da lei consumerista no âmbito da proteção de dados, "a jurisprudência restritiva do Supremo Tribunal Federal acerca do *habeas data* e do sigilo de dados, bem como a ausência de princípios claros

---

depois de ciência prévia do consumidor. Em termos de proteção de dados, o Superior Tribunal de Justiça continua a dar sua contribuição à sociedade, a partir do aparato legal que foi se desenvolvendo. Apenas como exemplo, registre-se o julgamento do Recurso Especial 1.168.547/RJ, no qual o Ministro Luis Felipe Salomão reconheceu no direito de privacidade o "dispor com exclusividade sobre as próprias informações"; o Recurso Especial 306.570/SP, reforçando a independência da proteção dos dados pessoais com relação ao sigilo bancário e, mais recente, o Recurso Especial 1.419.698/RS representativo de controvérsia, quando a Segunda Seção apreciou a licitude do cadastro no modelo credit scoring, Código Civil que confere uma nota ao consumidor a partir da análise de dados referentes à operações de crédito contratadas por ele anteriormente. A metodologia do cadastro foi considerada legal pela Corte que, oportunamente, reforçou os limites da tutela do consumidor e de sua privacidade, consagrados no Código de Defesa do Consumidor e na Lei do Cadastro Positivo, ao determinar que o consumidor tem direito de ser informado sobre as fontes utilizadas para coleta de seus dados e a natureza das informações levadas em consideração. Além disso, ressaltou-se que a utilização de informações sensíveis, incorretas ou desatualizadas configura abuso de direito, e que a responsabilidade civil dos envolvidos é objetiva e solidária".

[161] BESSA, Leonardo Roscoe. O consumidor e os limites dos bancos de dados de proteção ao crédito. São Paulo: Revista dos Tribunais: 2003, p. 99.

[162] BIONI, Bruno. O consentimento como processo: em busca do consentimento válido. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz. Tratado de proteção de dados pessoais. São Paulo: Forense: 2021.

[163] SARTORI, Ellen Carina Mattias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet. Revista de Direito Civil Contemporâneo, São Paulo, v. 9, ano 3, p. 49-104, out.-dez. 2016.

a nortear a proteção de dados pessoais" indicam o longo caminho jurídico para que "a proteção de dados pessoais se torne efetiva no Brasil"[164].

De toda forma, mesmo que se considere a visão de enquadrar as políticas de privacidade como uma espécie de contrato como ultrapassada ou retrógrada, é fato que essa tende a ser a base da construção da LGPD no que toca ao consentimento como requisito para o tratamento de dados. Invariavelmente, também permeia o próprio conceito do legítimo interesse, de modo que estudar brevemente o panorama contratual geral não é despiciendo.

2.4 O julgamento da ADI-MC nº 6.387/DF

Outro fato que marca a evolução da discussão sobre a privacidade no Brasil foi o julgamento recente da ADI-MC nº 6.387/DF pelo STF. Referida ADI questionava a Medida Provisória nº 954, que permitia o compartilhamento de dados por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de suporte à produção estatística oficial durante a pandemia do coronavírus.

Laura Schertel e Otávio Luiz apontam que o julgamento é semelhante ao realizado pelo Tribunal Constitucional Alemão no ano de 1983, em que também se discutiu o compartilhamento de informações pessoais para produção de estatísticas oficiais, sendo que a Corte também deu relevância à necessidade de medidas garantidoras da proteção dos direitos fundamentais[165].

A autora reconhece três aspectos centrais no julgamento: (i) a superação do pensamento de existência de dados neutros ou insignificantes, que não demandariam proteção constitucional; (ii) a afirmação da existência de um direito fundamental à proteção de dados pessoais, autônomo a quaisquer outros, o que naturalmente carrega a eficácia positiva e negativa inerente ao instituto; e (iii) os preceitos constitucionais demandam que se promova uma estrutura institucional de proteção de dados pessoais à altura das balizas da Carta maior[166].

Para além disso, a Corte se balizou pelo teste da proporcionalidade para a aferição do legítimo interesse público no compartilhamento dos dados: afirmou que, num escrutínio

---

[164] CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo, São Paulo, v. 13, ano 4, p. 59-67, out.-dez. 2017.

[165] SCHERTEL, Laura; RODRIGUES JÚNIOR, Otávio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz. Tratado de proteção de dados pessoais. São Paulo: Forense: 2021.

[166] MENDES, Laura Schertel. Decisão histórica do STF reconhece o direito fundamental à proteção de dados pessoais. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em 24/5/2021.

detalhado, não haveria necessidade, adequação e proporcionalidade em estrito sentido na medida. E essa constatação mormente se deu pela falta de transparência argumentativa na edição da Medida Provisória, o que contraria o devido processo legal substantivo: se o legislador – no caso, o Presidente da República – não declinou as condições suficientes para a aferição da adequação e necessidade, não há como validar constitucionalmente a medida.

Foi dado foco especial ao princípio da necessidade, pelo qual o tratamento dos dados – o compartilhamento – deveria respeitar a "limitação ao mínimo necessário para alcançar suas finalidades"[167], além de não haver preservação dos dados por "tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada"[168]. Trata-se do retrato da lógica do menor privilégio, que é uma das principais balizas para a aferição da validade do tratamento dos dados pessoais, notadamente em um contexto de aparentes acessos excessivos.

Outra preocupação especial da Corte foi quanto à necessidade de assegurar mecanismos de proteção e segurança dos dados pessoais porventura compartilhados. Assim, "ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros".

O Tribunal reconheceu que, quanto à segurança dos dados e ao seu tratamento adequado, é certo que, naquela circunstância, como a LGPD ainda não vigorava, ainda não havia definição eficaz de critérios para responsabilização dos agentes por danos ocorridos no tratamento, de modo que a análise da Medida Provisória deveria se dar em um escrutínio mais cuidadoso. Em tese, tal argumento levaria a crer que, vigendo a LGPD, a análise poderia ser menos rigorosa sob a dinâmica constitucional, na medida em que a própria lei já daria critérios mais objetivos para a aferição da validade do tratamento dos dados. Pensa-se, contudo, que seguiria existindo um problema de *enforcement* da norma legal.

Por fim, ainda dentre as conclusões principais extraídas da própria ementa do julgado, é também possível elencar que o Tribunal sequer aceitou o *fundamento de crise*. Com efeito, afirmou que sequer a pandemia e sua necessidade intrínseca de formulação de políticas

[167] A Ministra Rosa Weber criticou em seu voto o compartilhamento de dados de 200 milhões de pessoas, sendo que o alvo da pesquisa a ser empreendida pelo IBGE tinha cerca de 200 mil pessoas. Ou seja, a multiplicação do privilégio por 1000 vezes além do necessário pareceu à Ministra, corretamente, excessivo.
[168] BRASIL. Supremo Tribunal Federal. ADI-MC nº 6.387/DF, Rel. Min. Rosa Weber, julgamento em 7/5/2020.

públicas urgentes e com atuação imediata poderia ser invocada como pretexto para justificar o enfraquecimento de direitos fundamentais e o atropelo de garantias constitucionais.

Aliás, já até se debate na literatura internacional o fato de a pandemia ser "uma oportunidade sem precedentes para os governos justificarem a expansão pós-pandêmica de políticas de vigilância e de coleta de dados tanto de cidadãos quanto de não-cidadãos"[169]. Certamente é, mas o tratamento de dados pessoais é, em alguma medida, necessário na medida em que a finalidade pública de controlar a pandemia parece, *prima facie*, preponderar sobre o direito individual de proteção dos dados pessoais – desde que o tratamento seja balizado pelos ditames constitucionais e legais.

Clarissa Long ainda afirma que é improvável que aconteça o movimento voluntário de retração do uso dos dados e que isso se restrinja apenas às finalidades inicialmente elencadas. Isso, como a professora coloca, é chancelado pela história, além de também representar um grave risco no bojo dos aplicativos analisados.

Além disso, esse argumento é interessante sobretudo quando se considera a análise do legítimo interesse: em situações de crise, é quase esperado que o Estado pretenda malversar os dados pessoais para alguma espécie de enfrentamento imediato. Em alguma medida, esse argumento da *crise* é utilizado para justificar a necessidade de uso dos aplicativos de rastreamento de contatos – discussão que tomou o mundo inteiro. De toda forma, fato é que a baliza colocada pelo Tribunal ratifica a posição de que o legítimo interesse deve ser efetivamente justificado à luz da proporcionalidade.

Então, aplicando as linhas gerais do julgamento da Corte ao caso em análise – os aplicativos móveis –, é possível apontar dois principais problemas: (i) a mesma falta de transparência quanto aos motivos para o tratamento dos dados – o que impossibilita a correta aferição do teste de proporcionalidade para investigar o legítimo interesse – existe nos aplicativos em geral, como se vê na parte empírica do trabalho; e (ii) também não há como averiguar as garantias relevantes sob a perspectiva da segurança no tratamento dos dados pessoais, na medida em que os aplicativos se limitam a informar generalidades sobre uma espécie de compartilhamento seguro dos dados coletados.

Ou seja, levando a último efeito a decisão da Corte, é provável que o funcionamento de praticamente todos os aplicativos tivesse que ser revisto no Brasil, ante a incompatibilidade tanto com a LGPD quanto com os fundamentos constitucionais protetivos do usuário, consumidor e titular dos dados e privacidade. Mas, como disse a Ministra Rosa Weber em seu

[169] LONG, Clarissa; Privacy and Pandemics In PISTOR, Katharina. Law in the time of COVID-19. Columbia Law School Books, 2020.

voto, as condições de manipulação dos dados pessoais digitalizados são um dos maiores desafios contemporâneos do direito à privacidade.

Adentrando nas minúcias de cada voto, é possível perceber que a Ministra Rosa Weber teve especial preocupação com a falta de clareza da finalidade do tratamento[170]. A transparência defendida pela Ministra em seu voto é justamente uma das pedras angulares da argumentação contida no presente trabalho, em que se pretende objetivar, com clareza, os porquês de determinados acessos requeridos e a sucessão de tratamentos posteriores à coleta.

Se o usuário entender com a clareza legal e constitucionalmente imposta a *cadeia de custódia* dos seus dados pessoais, certamente fará um *trade-off* mais consciente no momento do seu consentimento ou de *concordar*, ainda que tacitamente, com o legítimo interesse do operador. E, como a Ministra apontou o dever de transparência ao Poder Executivo – editor da Medida Provisória –, no caso deste trabalho, o dever cabe aos provedores de aplicação.

No que concerne à preocupação com a segurança dos dados, a Ministra Rosa Weber aponta que a Medida Provisória até continha previsão de vedação ao compartilhamento dos dados ali coletados pelo IBGE com outros entes, públicos ou privados. Contudo, na correta avaliação da Ministra, a mera enunciação, quase retórica, dessa vedação não é suficiente dentro da dinâmica constitucional de proteção aos dados pessoais, na medida em que não se "apresenta mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida". Além disso, a Ministra demonstrou preocupação com a aparente ausência de aplicação dos instrumentos de anonimização ou pseudonomização dos dados, o que seria compatível com o caso concreto ante a desnecessidade de manutenção de critérios de identificação pessoal nos dados coletados.

In casu, a crítica da Ministra é também aplicável aos termos de privacidade dos aplicativos móveis, na medida em que, frequentemente, se opta simplesmente por recorrer à fluidez de construções semânticas que, de prático e concreto, nada dizem. É o que já se falou – e que é comprovado na parte específica de análise empírica – de termos que se limitam a dizer que cuidam dos dados pessoais com zelo, que só compartilham com terceiros confiáveis, dentre outros exemplos. Quase nenhum declina com cuidado quais são os terceiros que receberão os dados e quais os mecanismos de segurança concretos para evitar eventuais problemas.

[170] "(…) limita-se a enunciar que os dados em questão serão utilizados exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados".

Em seu voto, o Ministro Luiz Fux, retomando o voto da própria Ministra Rosa Weber e do Ministro Alexandre de Moraes – que se baseou no "sigilo de dados" constitucional –, assentou que "a proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, extraídos da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), previstos na Constituição Federal de 1988".

Tal constatação vem ratificar um conceito alcançado pelo Tribunal Constitucional Alemão ainda em 1983, que concluiu pela necessidade de proteção apartada da proteção dos dados pessoais e da autodeterminação informativa como forma de possibilitar à pessoa o livre desenvolvimento de sua personalidade[171].

O Ministro elenca quatro critérios para que o processamento de dados seja válido: atendimento a propósitos legítimos, específicos, explícitos e informados; limitação da coleta ao mínimo necessário para a realização das finalidades normativas; prescrição de medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados; e prevenção da ocorrência de danos, conforme assentado no direito comparado e na LGPD. É a partir da aferição desses quatro critérios, e não do compartilhamento de dados *per se*, que o Ministro concluiu pela inconstitucionalidade da Medida Provisória.

O Ministro Ricardo Lewandowski, por sua vez, afirmou não se tratar de "informações insignificantes, mas da chave de acesso a dados de milhões de pessoas", refutando a tese de pretensa neutralidade dos dados, o que afastaria a necessidade de uma proteção mais apertada sob a dinâmica constitucional.

O Ministro Gilmar Mendes, por sua vez, fez profusa discussão sobre a autonomia do direito fundamental à proteção dos dados pessoais[172]. O Ministro afirma que, no decorrer do século passado e ao longo do atual, vê-se uma transformação do alcance e sentido da privacidade, deixando de ser mera tutela da esfera privada individual. Essa abordagem de direito negativo de não intervenção balizou o primórdio da discussão com Warren e Brandeis e influenciou até mesmo Tércio Sampaio no Brasil[173].

---

[171] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[172] "A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa".

[173] FERRAZ JÚNIOR, Tércio. Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 430-459, 1993.

Nesse mesmo sentido, advoga Laura Schertel, para a qual, hoje, com a proteção mais abrangente dos dados pessoais, não se está preocupado tão somente com o conteúdo dos dados divulgados, mas com as possibilidades e finalidades do tratamento[174]. E é justamente esse aspecto mais procedimental que faz parte do âmbito de proteção do direito fundamental à proteção dos dados pessoais, com preocupações quanto à governança, à transparência e à sindicabilidade do tratamento de dados. Trata-se da tutela da dignidade e da personalidade dos cidadãos no bojo de uma sociedade da informação[175].

Assim, o reconhecimento de uma categoria autônoma de direito fundamental para a proteção dos dados pessoais é medida necessária para que se faça frente ao cenário de incessante evolução tecnológica – mormente baseado nos dados pessoais –, com uma hipervulnerabilidade informacional, técnica e econômica do usuário, consumidor e titular dos dados[176]. Se até mesmo juristas têm dificuldades compreensíveis para o adequado entendimento de políticas de privacidade, por exemplo, é natural que se espere que a maioria da população também nada entenda sobre as cláusulas de disposição de seus dados pessoais. É, pois, uma necessidade para dar a adequada proteção à dignidade da pessoa humana.

Partindo dessa necessidade, Laura Schertel propõe que se analise o direito fundamental à proteção dos dados pessoais sob uma dupla dimensão. Subjetivamente, protege-se o titular dos dados contra os riscos que ameaçam a personalidade em face da coleta, processamento, utilização e circulação dos dados. Trata-se do binômio identificação de finalidades e estabelecimento de limites, sempre sob a ótica da proibição (ao tratamento sem justificativa) e da transparência, ou seja, o devido processo informacional[177]. Há semelhança notável com o processo legal substantivo declinado pela Ministra Rosa Weber como requisito para normas legais sobre tratamento (compartilhamento) de dados pessoais.

Objetivamente, atribui-se ao indivíduo a possibilidade de controlar o fluxo de seus dados pessoais, com uma deferência real ao direito à autodeterminação informacional[178]. Por

---

[174] MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. *In*: Revista Pensar, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

[175] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. JOURNAL OF INSTITUTIONAL STUDIES, [S.l.], v. 6, n. 2, p. 507-533, set. 2020. Disponível em: <https://estudosinstitucionais.emnuvens.com.br/REI/article/view/521>. Acesso em: 5 abr. 2021.

[176] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[177] Como destacado por Julie E. Cohen: "o caráter autônomo da privacidade sugere uma necessidade de repensar a concepção do devido processo como uma tomada de decisão individualizada. (...) O devido processo na era de computação abrangente deve pressupor limites à personalização nos processos administrativos públicos" (COHEN, Julie E. What Privacy is For. Harvard Law Review, Vol. 126, 2013, p. 1931).

[178] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140, p. 176-177

dificuldades inerentes a cada indivíduo – vulnerabilidade –, geralmente se atribui esse aspecto objetivo da proteção dos dados pessoais a autoridades independentes, como a ANPD.

À luz desses conceitos, o Ministro Gilmar Mendes assenta que "a autodeterminação só pode ser afastada por um dever de justificação minudente e exaustivo das finalidades atribuídas ao tratamento de dados", sendo que "o princípio da transparência impõe que a norma garanta ao titular dos dados um nível de controle suficiente para a verificação prospectiva da licitude do tratamento de dados".

Ou seja, o operador dos dados, seja ele público ou privado, deve dar condições para que o titular dos dados efetivamente faça uma gestão dos seus dados pessoais, controlando se concorda com o tratamento em maior ou menor escala. E é justamente essa uma das maiores falhas em quase todos os aplicativos aqui analisados, na medida em que não há transparência de nenhuma espécie; quando muito, recorre-se à fluidez semântica de determinadas construções linguísticas.

Quanto ao teste de proporcionalidade, o Ministro pontua que a redação genérica da Medida Provisória então combatida quanto aos objetivos do compartilhamento dos dados não esclarece "em que medida e sob quais parâmetros os dados objeto do compartilhamento serão utilizados para fins da estatística oficial na época da pandemia".

Sustenta-se que, se o Ministro tivesse a oportunidade de ler os termos e privacidade dos aplicativos móveis, ficaria ainda mais consternado com o grau de generalidade das afirmações ali efetuadas. E, à luz da eficácia horizontal dos direitos fundamentais, os mesmos requisitos de especificidade são aplicáveis aos termos de privacidade dos aplicativos móveis, para que seja viável o teste do parâmetro da adequação.

O que se vê, assim, é que o Tribunal chancela a percepção de que o direito fundamental à proteção de dados pessoais se preocupa mais com as questões adjetivas do tratamento de dados – mormente balizado pelo próprio direito à autodeterminação informativa – do que com a proteção substantiva do sigilo em si[179]. Ou seja, modifica-se o paradigma de pessoa-informação-sigilo, do clássico direito à privacidade, para pessoa-informação-circulação-controle, à luz do desenvolvimento tecnológico atual[180].

Doneda, ao lembrar que a Convenção de Strasbourg é o principal marco da abordagem da proteção de dados pessoais como um direito fundamental, concorda com essa

[179] MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. Revista Pensar, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.
[180] RODATÀ, Stefano. *A vida na sociedade da vigilância*. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 93.

abordagem[181]. É possível concluir de sua análise que tal julgamento marcou uma espécie de efetiva comunhão entre o direito à privacidade e a visão clássica do direito à proteção do sigilo das comunicações, inclusive chancelada outrora pela Corte[182]. Essa posição mais clássica era defendida por Tércio Sampaio, para o qual a Constituição chancelaria apenas a proteção à comunicação, e não ao dado comunicado em si[183].

Dentro de uma análise mais consequencialista, Bioni indica que é importante tutelar o direito fundamental à proteção dos dados pessoais de forma autônoma para "um alcance normativo maior, que é capaz de abraçar toda e qualquer atividade de processamento de dados (ainda que não pessoal), mas que impacta a vida de um indivíduo". Isso porque "a proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade"[184].

Além disso, Bioni afirma que "a tutela jurídica dos dados pessoais é um imperativo que impõe uma nova fronteira aos direitos da personalidade, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana e, por tabela, ao livre desenvolvimento de sua personalidade", diferente de uma mera "evolução"[185] do direito à privacidade, à luz da capacidade de autodeterminação[186].

Concorda-se que defender a autonomia normativa do direito fundamental à proteção dos dados pessoais é incompatível com a compreensão de se tratar de uma evolução do conceito de privacidade – para, de algum modo, seguir enquadrando as normas de proteção de dados como proteção à privacidade *lato sensu*. Contudo, parece fora de dúvidas que entender que tal direito surgiu no contexto de uma *evolução* tecnológica é adequado, na medida em que os dados pessoais só passaram a estar no centro do debate internacional efetivamente nos últimos 30 ou 40 anos.

---

[181] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 13 dez. 2011.

[182] BRASIL. Supremo Tribunal Federal. RE 418416, Relator: Sepúlveda Pertence, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006.

[183] FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo. 1993. v. 88.

[184] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[185] MORAES, Maria Celina Bodin de. Apresentação do autor e da obra. In: RODATÀ, Stefano. *A vida na sociedade da vigilância*. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p.7: "O notório conceito do 'direito a ficar só', o direito à vida privada atribuído à elaboração de Warren e Brandeis (mas na verdade, adverte o autor, concebido por Robert Kerr quarenta anos antes), é qualitativamente diferente da privacidade como 'direito à autodeterminação informativa', o qual concede a cada um de nós um real poder sobre nossas próprias informações, nossos próprios dados. Percebe-se aqui, segundo Rodotà, um ponto de chegada na longa evolução do conceito de privacidade, da originária definição – *the right to be let alone* – ao direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada".

[186] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

O apontamento da autonomia normativa no Brasil demorou a ser efetivamente reconhecido, mas, agora que chegou, servirá para dar mais densidade e holofote à discussão sobre proteção de dados pessoais. Proteger dados significa proteger a liberdade e a autodeterminação informativa, dois aspectos centrais da dignidade humana.

2.5 Aspectos da legislação específica sobre proteção de dados

Feito o panorama geral a respeito de normas contratuais e consumeristas, importante passar a colocá-las em prisma mais específico. Nesse sentido, passa-se à análise breve dos conceitos mais importantes das legislações específicas sobre direito das relações na internet.

2.5.1 Aspectos gerais e o Marco Civil da Internet

Atenta à evolução e à popularização da internet na década de 1990, a Organização das Nações Unidas (ONU), por meio de uma Comissão específica, elaborou uma Lei Modelo para tratar sobre comércio eletrônico. Foi a primeira norma a nível internacional, que acabou influenciando as legislações nacionais, inclusive a brasileira[187].

Com efeito, embora tenham existido diversos projetos de lei em tramitação no Congresso Nacional, apenas em 2013, foi editado Decreto que regulamenta o Código de Defesa do Consumidor no que tange às contratações por comércio eletrônico (o de nº 7.962).

De modo específico – e dentre as previsões mais relevantes para o presente trabalho –, o art. 4º do referido Decreto[188] estabelece que o fornecedor deve apresentar, antes da

[187] UNITED NATIONS COMISSION ON INTERNATIONAL TRADE LAW. Model Law on Electronic Commerce with Guide to Enactment 1996. New York: United Nations. 1999. Disponível em: <http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf>. Acesso em: 24 mar. 2021.

[188] Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:
I - apresentar sumário do contrato antes da contratação, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizadas as cláusulas que limitem direitos;
II - fornecer ferramentas eficazes ao consumidor para identificação e correção imediata de erros ocorridos nas etapas anteriores à finalização da contratação;
III - confirmar imediatamente o recebimento da aceitação da oferta;
IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação;
V - manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato;
VI - confirmar imediatamente o recebimento d as demandas do consumidor referidas no inciso, pelo mesmo meio empregado pelo consumidor; e
VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.
Parágrafo único. A manifestação do fornecedor às demandas previstas no inciso V do caput será encaminhada em até cinco dias ao consumidor.

contratação, sumário do contrato, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizando as cláusulas que impliquem limitações de direitos consumeristas; a cópia fiel do contrato integral deve ser disponibilizada imediatamente após a contratação. Além disso, o Decreto impõe a obrigatoriedade de os fornecedores utilizarem mecanismos eficazes de segurança com vista ao tratamento de dados do consumidor.

Frise-se, desde já, que se entende que tal Decreto é perfeitamente aplicável ao contexto de utilização de aplicativos móveis, inclusive os *gratuitos*. Isso porque, embora o comércio seja, conceitualmente, apenas uma das espécies possíveis de relação de consumo (art. 3º do CDC), entende-se que a autoridade normativa acabou falando menos do que deveria, talvez ignorando a realidade que estaria por vir (de *boom* de aplicativos "gratuitos" na internet).

Ou seja, e como já se enunciou quando da construção do argumento por analogia com os contratos de incorporação imobiliária, o que se sustenta é que as políticas de privacidade e os termos de uso dos aplicativos móveis deveriam, sim, ser acompanhados de um sumário do *contrato* ou termo. Esse sumário pode ser no formato de quadro-resumo ou de qualquer outro meio igualmente ou mais interativo e explicativo, tendo como o norte da bússola dar mais transparência ao usuário. Afinal, não parece mais aceitável o paradigma de apostar nessas contratações mais obscuras[189].

Embora tenha significado importante avanço, o Decreto nº 7.962/2013 ainda era insuficiente para tutelar as nuances das relações consumeristas. Com efeito, era necessária uma legislação mais específica para regular as relações na internet, inclusive as de consumo eletrônico. Especificamente quanto a esse último ponto, é também fato que a vulnerabilidade técnica e informacional do consumidor é mais acentuada no comércio eletrônico – na medida em que não consegue experimentar o produto e é bombardeado por campanhas publicitárias online –, o que demanda um reforço no princípio da boa-fé objetiva, sobretudo com seus deveres laterais de conduta (informação, proteção contra fraudes, correção de erros, proibição de publicidade enganosa ou abusiva, proibição de *spam*, etc.)[190].

De certa forma, o Marco Civil da Internet (Lei nº 12.965/2014) supriu algumas lacunas da legislação então existente. Com efeito, referida Lei foi baseada em três pilares fundantes: liberdade de expressão, neutralidade da rede e privacidade[191]. Em específico, o que se busca discutir no presente trabalho é justamente este último.

---

[189] Fossem as políticas de privacidade uma decisão judicial, certamente caberia contra elas o recurso de embargos de declaração.
[190] MARTINS, Guilherme Magalhães. Contratos Eletrônicos de Consumo. 3 ed. São Paulo: Atlas. 2016.
[191] Ibidem.

A jurisprudência do STJ vem se tornando profícua nos temas tangíveis ao direito e à internet, mesmo antes do próprio MCI. Com efeito, já em 2012, o Tribunal ratificava conceitos tradicionais do direito de internet, conceituando os diversos tipos de provedores, com suas respectivas responsabilidades e funcionalidades específicas para a adequada operação em rede. Àquela época, de acordo com os conceitos do momento, os aplicativos seriam uma mistura dos provedores de informação e de conteúdo, na medida em que produzem as informações que são divulgadas na rede, geralmente por eles próprios[192].

Com a evolução temporal, o Marco Civil da Internet acabou adaptando o conceito e criando uma nova categoria: a dos provedores de aplicação. Assim, estabelece, em seu art. 5º, VII[193], que uma aplicação de internet é o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet. Por esse conceito legal, é fora de dúvidas, portanto, que os aplicativos a serem analisados são verdadeiros provedores de aplicações, na medida em que consistem em um conjunto de funcionalidades – o *software* em funcionamento – que pode ser acessado na loja específica de cada modelo de celular.

O art. 2º do MCI prevê que a livre iniciativa e a defesa do consumidor são verdadeiros fundamentos do uso da internet no Brasil. Essa é justamente a celeuma em discussão no presente trabalho, em que se pensa na ponderação entre o respeito à privacidade do consumidor e usuário da aplicação e o legítimo interesse da provedora da aplicação para a obtenção dos dados para fins econômicos.

Além disso, fala-se em respeito aos direitos humanos, à pluralidade, à diversidade e à finalidade social da rede, conceitos já desenvolvidos anteriormente e que remetem à ideia de que a utilização da internet é de verdadeira importância coletiva. Especificamente quanto ao respeito à diversidade, embora as redes tenham facilitado a manifestação de individualidades, é também certo que o próprio efeito *bolha* tende a dificultar o completo desenvolvimento de

---

[192] Veja-se: "a world wide web (www) é uma rede mundial composta pelo somatório de todos os servidores a ela conectados. Esses servidores são bancos de dados que concentram toda a informação disponível na internet, divulgadas por intermédio das incontáveis páginas de acesso (webpages). Os provedores de serviços de internet são aqueles que fornecem serviços ligados ao funcionamento dessa rede mundial de computadores, ou por meio dela. Trata-se de gênero do qual são espécies as demais categorias, como: (i) provedores de backbone (espinha dorsal), que detêm estrutura de rede capaz de processar grandes volumes de informação. São os responsáveis pela conectividade da internet, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores backbone e revendem aos usuários finais, possibilitando a esses conexão com a internet; (iii) provedores de hospedagem, que armazenam dados de terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na internet; e (v) provedores de conteúdo, que disponibilizam na rede as informações criadas ou desenvolvidas pelos provedores de informação". BRASIL. Superior Tribunal de Justiça, REsp nº 1.308.830/RS, Rel. Min. Nancy Andrighi, DJe 19/06/2012.

[193] Art. 5º Para os efeitos desta Lei, considera-se: (...) VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

uma personalidade com respeito real à pluralidade e à diversidade, na medida em que a clausura do usuário em seu círculo de supostas preferências pessoais acirra os ânimos democráticos, pois cada indivíduo ou grupo se sente isolado em si, na mentalidade *nós e eles*[194].

De modo mais específico, o art. 3º do Marco Civil[195] estabelece a proteção da privacidade e a liberdade dos modelos de negócios como princípios básicos do uso da internet no Brasil. Nesse ponto, contudo, a própria legislação estabelece a restrição de que a liberdade negocial encontre freio nos demais princípios estabelecidos no ordenamento jurídico e na própria Lei. No caso, seria possível inferir que a liberdade de iniciativa encontra verdadeiros contornos na máxima de proteção ao consumidor e à sua privacidade.

Outro ponto relevante do artigo é a previsão do respeito aos princípios da "proteção da privacidade" e da "proteção dos dados pessoais" em incisos distintos, de forma autônoma. Parece que próprio MCI já tentava, desde 2014, introduzir a ideia – mais bem descrita na sequência do trabalho – segundo a qual a proteção dos dados pessoais é um direito fundamental autônomo em relação à privacidade, na medida em que tutelam questões diversas e em profundidade diferente. A mesma distinção foi feita posteriormente na LGPD, mas com uma atualização do conceito de proteção dos dados pessoais para a autodeterminação informativa. Ou seja, o MCI começa a representar uma superação da doutrina da privacidade na internet, atualizando conceitos e respectivas proteções.

Na sequência, o art. 6º do Marco Civil[196] estabelece que a interpretação da Lei também considerará a natureza, os usos e os costumes particulares da internet, bem como sua importância para a promoção do desenvolvimento humano, econômico, social e cultural. Tal disposição poderia, *prima facie*, chancelar que os aplicativos móveis continuem procedendo da forma como vêm operando, ou seja, esgarçando o requisito do consentimento dos usuários ou do legítimo interesse ao utilizarem os seus dados com interesses econômicos[197].

Nesse ponto, contudo, é imperativo rememorar que meros costumes e práticas comuns no ambiente digital não são suficientes para afastar disposições legais claras. Com

---

[194] EL PAÍS. "Temos de rechaçar a mentalidade do 'nós contra eles' que os cínicos tentam nos vender". Disponível em: <https://brasil.elpais.com/brasil/2016/07/09/internacional/1468096197_045190.html>. Acesso em: 6 abr. 2021.

[195] Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...)
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei; (...)
VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

[196] Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

[197] Afinal, trata-se da máxima popular se todos fazem, por que eu não poderia fazer?

efeito, a tutela da privacidade e da proteção dos dados pessoais é um mandamento legal expresso. E, ainda que assim não fosse, seria relevante tomar como base os usos e costumes da internet a nível global, ou seja, observar as práticas dos países em que a legislação protetiva aos usuários da rede está mais avançada em seu *enforcement*.

O art. 7º da Lei[198] estabelece que a internet é essencial ao exercício da cidadania. Para tanto, são estabelecidos alguns direitos básicos dos usuários, dentre os quais se destacam para a presente análise: (i) a inviolabilidade da intimidade e da vida privada (art. 7º, I a III); (ii) o recebimento de informações claras e completas em contratos de prestação de serviços (art. 7º, VI); (iii) o não fornecimento a terceiro dos dados pessoais do próprio usuário, a menos que tenha existido consentimento livre, expresso e informado para tanto (art. 7º, VII).

Além disso, é de se mencionar (iv) o recebimento de informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais do usuário, que somente poderão ser utilizados para fins que se justifiquem, não sejam vedados pela legislação e estejam especificados nos termos de privacidade das aplicações (art. 7º, VIII); (v) por pressuposto, o consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (art. 7º, IX); (vi) a publicidade e a clareza de políticas de uso dos provedores de aplicações (art. 7º, XI); e (vii) a aplicabilidade do sistema protetivo previsto no CDC às relações de consumo realizadas na internet (art. 7º, XIII).

---

[198] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (...)
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet.

No bojo desse artigo, é muito relevante observar que os incisos VII e IX remetem à necessidade do consentimento para o fornecimento de dados pessoais a terceiros (nesse caso, o consentimento deve ser livre, expresso e informado), salvo outras hipóteses legais, e para a coleta, uso, armazenamento e tratamento dos dados pessoais (nesse caso, o consentimento deve ser expresso e destacado das demais cláusulas contratuais). Como inexistia qualquer outra lei que tratasse sobre o fornecimento de dados pessoais no âmbito da internet, é de se concluir que o consentimento expresso do usuário era, no bojo do Marco Civil da Internet, a única possibilidade para o tratamento dos dados pessoais.

Como já se enunciou, hoje, a hipótese de tratamento de dados pessoais mais usada é a do legítimo interesse, provavelmente por sua maior facilidade aos provedores de aplicações. Fato é que, legalmente, tal hipótese não existia no Brasil até a vigência da LGPD, que, no ponto, certamente foi influenciada pelo RGPD europeu, o qual também acentuou a importância do legítimo interesse como hipótese para o tratamento de dados pessoais.

Nesse aspecto, parece que, para a tutela dos dados pessoais e da privacidade, a LGPD acabou representando um retrocesso ao prever a hipótese de tratamento baseado no legítimo interesse, na medida em que parecia melhor investir nas características de um bom consentimento pelo usuário, além, é claro, dos mecanismos de planejamento da privacidade desde a concepção da aplicação até a eliminação do dado. Tutela integral.

No mesmo art. 7º do MCI, em relação ao direito à exclusão definitiva dos dados pessoais, a LGPD parece ter representado um avanço legislativo, pois, antes, a exclusão dos dados só podia ocorrer a partir do término da relação usuário-provedor (inciso X). Hoje, a LGPD permite a eliminação dos dados pessoais tratados com base no consentimento do titular a qualquer momento (art. 18, VI), ou seja, não é necessário o término da relação.

Contudo, a LGPD poderia ter avançado ainda mais, permitindo o apagamento dos dados mesmo nas outras hipóteses autorizadoras do tratamento, e não só quando for caso de consentimento do usuário. Se apenas 5% dos tratamentos forem mesmo baseados no consentimento, isso significa que o titular só poderá ter seus dados esquecidos (usando a nomenclatura europeia da RGPD) uma vez a cada vinte hipóteses, o que parece insuficiente.

Por sua vez, o art. 8º do Marco Civil[199] estabelece que a garantia do direito à privacidade nas comunicações é condição essencial ao pleno exercício do direito de acesso à

[199] Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

internet. Por essa razão, são nulas as cláusulas contratuais – porque abusivas – que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas pela internet.

Nesse ponto, importante salientar que o legislador ordinário parece ter dito menos do que o necessário, na medida em que não faz sentido que apenas as comunicações em tempo real sejam protegidas por sigilo. Isso porque, hoje, com o avanço tecnológico, os dados armazenados no dispositivo informático (no presente caso, aparelho celular) também deveriam receber a referida tutela, na medida em que são perfeitamente suficientes para o refazimento de todo o fluxo de comunicações.

Não se vive mais sob o paradigma de comunicações telefônicas, em que o fluxo só existia no exato momento da conversa, sem posteriores registros sobre o conteúdo do diálogo, mas somente de que o diálogo existiu. Em se tendo acesso ao e-mail ou ao *WhatsApp* de um usuário, por exemplo, qualquer pessoa consegue restabelecer, em tese, o fluxo integral das comunicações – salvo se mensagens forem apagadas dos registros, o que, ainda assim, não parece garantir total sigilo. Então, hoje, não parece haver qualquer explicação para se tutelar a comunicação e não o próprio dado em si.

Contudo, a jurisprudência do STF parece divergir do entendimento de que os dados em si mesmos merecem a proteção constitucional, tendo como base precedente de meados da década de 90 ainda nas decisões mais atuais. Para a Corte, "descabe invocar a garantia constitucional do sigilo das comunicações de dados quando o acesso não alcança a troca de dados, restringindo-se apenas às informações armazenadas nos dispositivos eletrônicos", na medida em que "a proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador"[200]. É possível que, dado o atual cenário de fácil conversão do dado em fluxo, a Corte precise rever seu posicionamento de quase três décadas.

Por sua vez, o art. 10 da Lei[201] também protege a preservação da intimidade, da vida privada, da honra e da imagem das partes envolvidas, direta ou indiretamente, na

---

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

[200] SUPREMO TRIBUNAL FEDERAL. RHC 132062 / RS - RIO GRANDE DO SUL, Redator do Acórdão Min. Edson Fachin, Julgamento em 22/11/2016, publicação em 24/10/2017, Primeira Turma. No mesmo sentido: HC 91867 / PA – PARÁ, Rel. Min. Gilmar Mendes; e RHC 169682 AgR / RS - RIO GRANDE DO SUL, Rel. Min. Luiz Fux.

[201] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo,

comunicação privada estabelecida, ao prescrever o atendimento de todos esses requisitos como condição para a guarda e disponibilização de registros de acesso a aplicações de internet, dos dados pessoais e do conteúdo da comunicação.

De modo específico, o § 1º do referido artigo estabelece que o provedor de aplicações responsável pela guarda somente será obrigado a disponibilizar tais registros desde que (i) exista ordem judicial específica e respeitados os direitos básicos previstos no art. 7º retro e (ii) tais dados possam contribuir para a identificação do usuário que se pretende descobrir.

Ainda mais preocupado com o conteúdo das comunicações privadas, o § 2º dispõe que referido material somente poderá ser disponibilizado mediante ordem judicial específica. Ou seja, a construção verbal passou de um teor autorizativo para um verdadeiramente impositivo. Certamente, nesse aspecto, o MCI não conseguiu o adequado *enforcement*, na medida em que, na sua literalidade, transportaria o ônus da disponibilização do conteúdo das comunicações privadas apenas ao Poder Judiciário; e, como se sabe, os dados dispostos nas comunicações privadas são há muito tratados pelos provedores de aplicações.

Contudo, entende-se, pelas mesmas razões expostas anteriormente, que não faria sentido dar tutela mais alargada ao conteúdo das comunicações privadas e não aos próprios dados armazenados no dispositivo informático do usuário. Por essa razão, entende-se que mesmo a disponibilização de outras informações que não o mero conteúdo das comunicações somente seria possível mediante ordem judicial específica e fundamentada. Assim, seria inviável, *a priori*, que os próprios provedores de aplicações empreendessem referida guarda e disponibilização *sponte propria*.

Na sequência, o § 4º do referido dispositivo estabelece que as medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. Esse requisito conversa diretamente com o princípio geral de transparência e informação ao consumidor/usuário, que não é exatamente bem respeitado nos dias atuais.

Sobre a questão dos segredos empresariais, aliás, Ana Frazão afirma que "a opacidade e a falta de transparência, longe de serem características intrínsecas aos mercados

---

respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. (...)

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

digitais, são na realidade o resultado da ação deliberada dos agentes econômicos ou estatais a quem a ausência de controle aproveita. Por meio de uma série de estratégias jurídicas (como a proteção do segredo de negócios) e não jurídicas, é criado um ambiente de ofuscação que permite aos atores poderosos ordenar, ranquear e avaliar as pessoas, mantendo suas técnicas em segredo, inclusive para o fim de proteger sua valorosa propriedade intelectual"[202]. Ou seja, há uma aparente utilização indevida de escusas empresariais para vedar o amplo acesso à informação pelos consumidores e usuários, razão por que é urgente a ampliação dos mecanismos de transparência e *accountability*.

O art. 11 do Marco Civil[203] estabelece que a legislação brasileira – com todas as suas peculiaridades referentes ao direito à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e de seus registros – é aplicável aos casos de usuários nacionais de aplicativos móveis (art. 11, § 1º). Isso porque, nesses casos, ao menos a coleta dos dados pessoais e o uso da própria aplicação se dão no Brasil. Além disso, o *caput* do dispositivo também se utiliza de termos distintos para se referir à privacidade e à proteção dos dados pessoais, o que indica, novamente, o caminho rumo à autonomia conceitual da proteção de dados.

Tal apontamento é relevante se considerado o contexto de que a maioria dos aplicativos móveis foi desenvolvida por provedores de aplicações estrangeiros, ou seja, por empresas sediadas no exterior (art. 11, § 2°). Ademais, a Lei também estabelece o requisito de que os provedores de aplicações prestem informações que permitam a verificação do cumprimento da legislação nacional no que tange à observância do dever de privacidade (art. 11, § 3º). O mínimo que se esperaria, nesse sentido, é que as políticas de privacidade fizessem alguma menção específica à legislação brasileira de proteção de dados, o que não é exatamente

---

[202] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[203] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

a realidade em muitas das aqui analisadas. A própria política do *Facebook*, já enunciada anteriormente, não é profícua nas menções de adequação à legislação nacional. E isso porque a rede conta com mais de 130 milhões de usuários no Brasil, um mercado relevante o suficiente para que, ao menos, a política de privacidade fosse adaptada ao país.

O ponto, contudo, é que a Lei estabelece uma norma de eficácia limitada, na medida em que estabelece a obrigatoriedade de um regulamento para explicitar como se daria esse dever de transparência. Pensa-se, entretanto, que não é o caso de se promover a execução desse dever apenas quando da existência de um regulamento, na medida em que se trata de verdadeira norma de ordem pública, por aplicação dos próprios dispositivos do CDC.

Por sua vez, a reprimenda aos provedores que descumpram as normas insertas nos arts. 10 e 11 do MCI é variável a depender da gravidade do fato, podendo chegar, no máximo, à proibição do exercício da atividade de provedoria de aplicações no Brasil[204]. É improvável, contudo, que se chegue a tal ponto, na medida em que multas e advertências talvez sejam suficientes e, invariavelmente essas discussões seriam levadas ao Poder Judiciário, que faria alguma ponderação entre excluir o serviço do Brasil, com algum prejuízo aos usuários, ou mantê-lo mesmo sem o fiel cumprimento das normas. Para provedores menores, é factível conjecturar punições mais graves; mas, para provedores já consolidados e com milhões de usuários – *WhatsApp*, por exemplo –, parece inimaginável que alguma sanção de exclusão do serviço do Brasil pudesse ser aplicada.

Na sequência, percebe-se que o art. 15 do MCI[205] prescreve o prazo de seis meses para a guarda dos registros de acesso a aplicações de internet. De acordo com o próprio conceito do MCI, os registros de acesso são o conjunto de informações referentes à identificação do IP (*internet protocol*) de acesso, com data e hora. Ou seja, trata-se de um panorama ligeiramente distinto do tratamento dos dados pessoais em si, mas se sustenta que tal prazo deveria ao menos orientar o tempo máximo de guarda dos dados pessoais dos usuários para quaisquer finalidades, inclusive pelo próprio princípio da *finalidade* insculpido na LGPD.

---

[204] Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

[205] Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Isso seria útil para evitar que o usuário pudesse ser surpreendido com o uso, contra si, de dado coletado há muito no passado, já que não se pode perder de vista que, no atual estado da arte, o consumidor perde totalmente a rastreabilidade de seus dados. Aliás, o próprio CDC, em sua seção sobre bancos de dados e cadastros de consumidores, afirma que eventuais informações negativas não podem ficar registradas por mais de cinco anos[206].

A lei do cadastro positivo acabou aumentando, dentro de tal escopo, o prazo para quinze anos[207]. Ou seja, parece que apenas a LGPD não optou por utilizar um prazo taxativo, o que acaba permitindo que o tratamento seja, literalmente, infinito, visto que se depende tão somente da argumentação via princípios para dizer que o tratamento não é mais legítimo pelo lapso temporal.

Na sequência, de acordo com o art. 16 do Marco Civil[208] é vedada a guarda, por provedores de aplicações, de (i) registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente e (ii) de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular. Mais uma vez, fala-se de guarda dos dados – uma das modalidades de tratamento – autorizada tão somente pelo consentimento do usuário, sem outras hipóteses. Como já se disse, o MCI pareceu apostar somente no consentimento como hipótese de tratamento de dados, paradigma que foi sendo deixado de lado mais recentemente, tanto pela nova lei do cadastro positivo – que inverteu a lógica, de *opt-in* para *opt-out* (ou seja, de optar por entrar e dar o *check* para optar por sair e retirar o *check*) –, quanto pela própria LGPD, que apostou no legítimo interesse.

Por fim, o art. 29 do Marco Civil[209] impõe a necessidade de o poder público, a sociedade civil e os provedores de aplicação desenvolverem mecanismos de controle parental de conteúdo porventura impróprio aos filhos menores. Essa disposição é particularmente

---

[206] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

[207] Art. 14. As informações de adimplemento não poderão constar de bancos de dados por período superior a 15 (quinze) anos.

[208] Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou
II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

[209] Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.
Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

relevante quando se considera a coleta de dados de usuários menores de idade. Outros dispositivos mais diretamente relacionados a cada objeto de análise do presente trabalho são avaliados nas subseções específicas.

Em termos de regulamentação, o Decreto nº 8.771/2016 estabelece que dado pessoal é aquele relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando relacionados a uma pessoa (art. 14, I[210]). Também conceitua, no inciso II do mesmo artigo, o tratamento de dados pessoais a partir da conjunção de todos os núcleos de atividade: coleta, produção, recepção, etc.

Viu-se, com isso, que o MCI representou importante paradigma para a proteção de dados e a privacidade no Brasil. Talvez tenha pecado por colocar muitas expectativas no requisito do consentimento, falando apenas que deveria ser livre, expresso, informado e destacado, sem dar maiores detalhes concretos de como isso se daria. Como a discussão global sobre a matéria evoluiu e se percebeu que talvez o consentimento não fosse mais tão suficiente assim, as normas mais novas passaram a se valer de outras tantas hipóteses autorizativas do tratamento de dados, sendo que o *carro-chefe* da LGPD é o legítimo interesse, importado do RGPD europeu.

Para entender melhor as características dessa nova proposta para a regulação dos dados pessoais no Brasil, é salutar que se estudem, muito brevemente, o RGPD (a grande fonte inspiradora da legislação brasileira) e a LGPD, como se passa a fazer.

2.5.2 Panorama Europeu para a Proteção de Dados

É importante salientar que a norma brasileira foi francamente inspirada pelo – e *pressionada* a ser criada pela tutela do – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Fala-se em inspiração e *pressão* porque, se o Brasil não criasse uma legislação de dados compatível com o panorama internacional, provavelmente deixaria de ser rota do tráfego internacional de dados, o que certamente teria inúmeras consequências aos consumidores e usuários brasileiros da rede. Então, partindo do

[210] Art. 14. Para os fins do disposto neste Decreto, considera-se:
I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

pressuposto de que era preciso criar algo robusto, nada melhor do que buscar inspiração na legislação europeia, que ficou conhecida como o *standard* a ser seguido.

Com efeito, a Carta de Direitos Fundamentais da União Europeia estabelece que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito, o que é um verdadeiro direito fundamental. O paradigma europeu[211] é de que o tratamento dos dados pessoais deverá ser concebido para servir as pessoas, mas o direito à proteção de dados pessoais não é absoluto, devendo ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

Os direitos básicos que balizam a aferição da proporcionalidade são o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística[212].

De modo similar à legislação brasileira, o Regulamento Europeu dispõe que os princípios da proteção de dados não deverão aplicar-se às informações anônimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anônimos que o seu titular não seja ou já não possa ser identificado. E o requisito para aferir se o usuário é identificável é a real expectativa de que a empresa, investindo tecnologia ordinária, possa se interessar pela identificação[213].

Ocorre, contudo, que nenhum dos dados coletados em aplicativos móveis são efetivamente anônimos, na medida em que a identificação do usuário é um pressuposto fundamental da própria publicidade comportamental. É claro que se afirma que o tratamento dos dados pessoas não identifica de modo individualizado o usuário, mas apenas o insere em um grupo de interesses agregados. O ponto é que, ao se fazer a agregação de diversos gêneros de interesse, parece possível criar fielmente o perfil digital específico para cada usuário.

Afinal, como previsto no próprio regulamento, as pessoas singulares podem ser associadas a identificadores por via eletrônica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet), *cookie*s ou outros identificadores, como as etiquetas de identificação por radiofrequência. Esses

---

[211] PARLAMENTO EUROPEU. Regulamento Geral sobre a Proteção de Dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt>. Acesso em: 25 mar. 2021.
[212] É o teor do Considerando 4 do RGPD.
[213] É o teor do Considerando 26 do RGPD.

identificadores, associados a outros tantos recebidos de fontes diversas, podem identificar precisamente pessoas singulares[214].

Nos termos do Regulamento Europeu, o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca no sentido de que o titular de dados consente com o tratamento dos dados que lhe digam respeito, com declarações escritas, orais ou recebidas na interface eletrônica, mediante conduta que indique claramente a aceitação do tratamento dos dados. Concebe-se que o silêncio do titular, sua omissão ou a existência de opções pré-validadas (*opt-out*) desconstituem o consentimento. Além disso, é sabido que o consentimento deve abarcar todas as finalidades do tratamento de dados, de modo específico para cada finalidade. Se durante o uso da ferramenta eletrônica, o pedido de consentimento deve ser bastante claro e conciso, sem atrapalhar a utilização do serviço[215].

Semelhantemente à legislação nacional, a regulação europeia estabelece que as crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Assim, há proteção mais específica e estreita quando da utilização de dados de crianças para o tratamento, a comercialização ou criação de perfis de crianças[216].

Por sua vez, o Regulamento Europeu estabelece que o princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento dos dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Ou seja, devem ser fornecidas aos titulares dos dados informações sobre a identidade do responsável pelo tratamento, as finalidades e as garantias de segurança de que o tratamento seja efetuado com equidade e transparência[217].

---

[214] É o teor do Considerando 30 do RGPD.

[215] É o teor do Considerando 32 do RGPD: "(32) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido".

[216] É o teor do Considerando 38 do RGPD.

[217] É o teor do Considerando 39 do RGPD.

Além disso, garante-se que as pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. As finalidades do tratamento deverão ser específicas, explícitas e legítimas, especialmente quando se fala da fase de coleta dos dados durante o tratamento. Ademais, os dados devem ser adequados, pertinentes e limitados ao estritamente necessário à realização da finalidade pretendida, subsistindo a guarda durante o menor tempo possível, o que se coaduna com a preocupação já manifestada de tratamento infinito de dados pessoas colhidos no passado[218].

De todo modo, para que o consentimento seja considerado informado ("dado com conhecimento de causa"), o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado[219].

No caso, por exemplo, parece temerário vincular o funcionamento de determinado aplicativo ao consentimento (*take it or leave it*), que é a realidade em muitos dos aplicativos analisados. Aliás, presume-se que o consentimento não é dado em livre manifestação vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico[220].

---

[218] É o teor do Considerando 39 do RGPD.

[219] É o teor do Considerando 42 do RGPD: "(42) Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho (10), uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado".

[220] É o teor do Considerando 43 do RGPD: "(43) A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução".

Por sua vez, estabelece-se que os legítimos interesses podem justificar o tratamento de dados, "desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável". Além disso, associa-se o legítimo interesse à ideia de previsibilidade de boa-fé do tratamento no momento da relação em que se daria a coleta dos dados. Outro ponto relevante é que o RGPD também considera como legítimo interesse a "comercialização direta" dos dados pessoais. Colocar tal expressão na norma retrata maior transparência do legislador europeu do que do brasileiro, pois, à luz da existência desse tipo de relação comercial, é melhor para o usuário destinatário da norma saber que essa é a realidade[221].

Além disso, também é interessante a perspectiva de que, por regra, os direitos dos titulares dos dados parecem não prevalecer sobre a expectativa de tratamento por parte do operador daquele dado (o provedor de aplicação), desde que respeitado o critério da previsibilidade inicial. Isso faz sentido, na medida em que caminhar em sentido contrário poderia implicar a chancela ao comportamento contraditório: o usuário que sabia que seu dado poderia ser tratado (com algumas especificidades: como, quando, onde, etc.) e, sabendo isso, concordou em utilizar o serviço *gratuito* depois não pode pretender vedar o tratamento. Contudo, a norma também é bem clara no sentido de que, superada a expectativa legítima inicial de tratamento pelo titular do dado, essa operação deve ser cessada em razão da prevalência dos interesses, no caso concreto, do titular.

O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm. Sempre que os dados pessoais forem coletados, o titular deve ser também informado da eventual obrigatoriedade do fornecimento dos dados e de eventuais consequências. Ademais, sempre que os dados pessoais forem objeto de tratamento para efeitos

---

[221] É o teor do Considerando 47 do RGPD: "(47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta".

de comercialização direta, o titular poderá se opor, inclusive à definição de perfis. Tal direito deve ficar explícito ao titular, de modo claro e distinto das demais informações[222].

Trata-se de previsão análoga à nacional, em que se discutiu a viabilidade da criação de *níveis de aplicativo*. Nesse ponto, contudo, o Regulamento Europeu refuta a ideia de que se institua uma espécie de cobrança individualizada a cada cláusula que o usuário não quer dar o seu consentimento, já que apregoa ser um direito de exercício gratuito, o que parece até mesmo um pouco contraditório com a pretensão do RGPD de criar um ambiente regulado de negócios de dados pessoais, pois, se todos se opuserem à comercialização direta, é provável que os provedores ficassem sem uma das principais rendas, o que poderia implicar uma cessação no desenvolvimento tecnológico. Nessa linha, o regulamento parece induzir a uma cobrança do tipo *tudo ou nada* – embora tenha indicado, em diversas outras seções, que o consentimento deveria ser granular.

O Regulamento Europeu ainda afirma, corretamente e para que a população fique atenta, que, se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controle sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa das pessoas singulares[223].

Saindo do ambiente dos *consideranda*, é de se afirmar que a sua existência é uma das mais importantes diferenças em relação à legislação brasileira. Isso porque, como a legislação aqui produzida não costuma conter textos não normativos[224], a LGPD perdeu a oportunidade de conter essa ampla gama de 173 vetores interpretativos, que é o número dos *consideranda* no RGPD. De toda forma, é inegável que, de um ou outra forma, os textos descritos no regulamento europeu, principalmente nessa parte mais interpretativa, servirão como uma espécie de guia para o *enforcement* da legislação brasileira.

Passando mais especificamente ao texto, o Regulamento Europeu (art. 4º) traz algumas definições relevantes e semelhantes às da legislação nacional. Com efeito, a lei

[222] É o teor do Considerando 60 e do Considerando 70 do RGPD.
[223] É o teor do Considerando 85 do RGPD.
[224] A exemplo da controvérsia existente outrora sobre a natureza jurídica do preâmbulo da CRFB/88, quando o STF, no âmbito da ADI nº 2.076/AC, chegou à conclusão de se tratar de texto sem valor jurídico-normativo, por não se situar no âmbito do Direito, mas da Política, refletindo mera posição ideológica do constituinte, sem relevância jurídica. Ou seja, teria natureza política, e não jurídica.

europeia, para além de definir tradicionalmente um dado pessoal e o seu tratamento, afirma também que um dado pessoal é violado quando ocorre uma violação da segurança que provoque a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, aos próprios dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Pare que fique claro, são exemplos de dados pessoais: o nome e apelido; o endereço de uma residência; um endereço de correio eletrônico como nome.apelido@empresa.com; o número de um cartão de identificação; dados de localização (por exemplo, a função de dados de localização em um celular – nesses casos, há legislação ainda mais específica do que a RGPD); um endereço IP (protocolo de internet); os rastros de navegação (cookies); o identificador de publicidade do seu telefone; os dados detidos por um hospital ou médico, que permitam identificar uma pessoa de forma inequívoca[225].

Como se viu, uma das hipóteses de permissão para o tratamento é o consentimento do titular dos dados, ou seja, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Em geral, o tratamento mais empreendido por aplicativos móveis é a própria definição de perfis, ou seja, qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspectos relacionados com o seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocamentos.

De acordo com o art. 5º do Regulamento[226], são princípios gerais relativos ao tratamento dos dados pessoais: licitude, lealdade, transparência, limitação das finalidades,

---

[225] COMISSÃO EUROPEIA. O que são dados pessoais? Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt>. Acesso em: 26 mar. 2021.

[226] Artigo 5.º Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para

minimização dos dados, exatidão, limitação da conservação, integridade, confidencialidade e responsabilidade. De modo geral, todos os princípios também são abarcados pela legislação brasileira e já existem desde os *fair information principles*.

De modo similar, o Regulamento dispõe que o consentimento e os legítimos interesses são hipóteses que autorizam o tratamento lícito dos dados pessoais, devendo aquele ser para finalidade específica e estes não podem se dar em situações em que prevaleçam os interesses ou direitos do titular que exijam a proteção dos dados, especialmente se for uma criança (art. 6º, 1).

Além disso, há importante disposição de que, se houver mudança da finalidade do tratamento dos dados, e isso não se der com base no consentimento do usuário, o responsável pelo tratamento deve checar o grau de compatibilidade da nova finalidade com a original, levando em conta cinco critérios: (i) quaisquer vínculos entre as finalidades inicial e atual; (ii) o contexto de coleta dos dados, notadamente quanto à relação entre titular-responsável pelo tratamento; (iii) a natureza dos dados pessoais (preocupação maior com dados penais e dados sensíveis); (iv) as consequências do tratamento pretendido para o titular do dado; e (v) a existência de salvaguardas adequadas do ponto de vista da segurança da informação (art. 6º, 4).

Para o Regulamento, ao avaliar se o consentimento é dado livremente, há que verificar se a execução de um contrato está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução do ajuste. Além disso, o pedido de consentimento deve ser escrito de forma bastante clara, a ponto de distingui-lo de quaisquer outros aspectos da relação provedor-usuário (art. 7º).

No que toca aos aplicativos móveis, é particularmente sensível que o usuário só poderá fazer o *download* e usar a ferramenta em sua inteireza se manifestar concordância integral com o tratamento de dados, em qualquer de suas modalidades. Na ótica da legislação europeia, portanto, esse tipo de consentimento seria inválido. E, trazendo-se esse conceito ao Brasil, seria quase uma espécie de *venda casada* – prática abusiva (art. 39, I, CDC) –, na medida em que o usuário só tem acesso à aplicação se concordar com o tratamento de seus dados pessoais. Talvez seja o momento de se dar mais atenção ao consentimento granular no Brasil.

---

fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»).

No tocante aos dados pessoais sensíveis (categorias especiais de dados), o RGPD tem a previsão de que podem ser tratados caso tenham sido tornados manifestamente públicos pelos titulares dos dados, o que parece menos protetivo do que a LGPD, pois a norma brasileira não apresenta essa exceção à regra do não tratamento, talvez por algum grau de *inocência* regulatória. Contudo, o RGPD também parece desconsiderar o critério do tratamento contextual dos dados, a que tanto se refere em outras passagens da norma.

Ora, se um usuário posta em sua rede social que é homossexual, por exemplo, dificilmente está antevendo que essa informação chegará ao conhecimento de planos de saúde, que poderia fazer alguma forma de discriminação econômica por maior propensão ao vírus HIV (numa antiquada e incorreta visão, já que aparentemente sem respaldo científico, de que a orientação sexual pudesse implicar maiores chances de contágio pela grave doença).

Na sequência, o Regulamento Europeu estabelece alguns direitos básicos dos titulares dos dados, como a transparência e existência de regras empresariais claras para o exercício dos direitos previstos no Regulamento (art. 12). O que mais chama atenção nesse ponto é a boa qualificação de o que se entende por uma transparência mais ativa: informações concisas, transparentes, inteligíveis, de fácil acesso, com linguagem clara e simples (especialmente para crianças), com informações escritas ou mesmo orais.

Por sua vez, no bojo do direito à informação e ao acesso aos próprios dados pessoais (arts. 13 a 15), prevê-se que, quando da coleta dos dados, o responsável pelo tratamento deve deixar claro qual é o legítimo interesse que justifica o tratamento (se esse for o caso autorizativo) e também esclarecer quais as finalidades para o tratamento, com o respectivo fundamento jurídico. Isso é particularmente relevante e interessante, ainda mais se for levado, na prática, à sua literalidade, que parece indicar uma espécie de diagrama de relações causais: "eu, responsável, coleto esse dado aqui para essa finalidade e com base nesse fundamento, sendo que meu legítimo interesse (se aplicável) é esse". Razoável e transparente.

Além disso, fala-se nos direitos à retificação, apagamento (direito ao esquecimento), limitação do tratamento e portabilidade (arts. 16 a 20) e à oposição ao tratamento, inclusive em termos de decisões individuais automatizadas e definições de perfis (arts. 21 e 22). Prevê-se que o titular não precisa se submeter a uma tomada de decisões baseada exclusivamente no tratamento automatizado, inclusive via *profiling*, mas pode dar o consentimento para que assim seja. Dentro do direito de oposição, particularmente relevante num contexto em que se discute a discriminação algorítmica, prevê-se também o direito à

interação com alguma pessoa física para discutir a tomada de decisões. Trata-se de uma preocupação que Mayer-Schoneberger denomina de "ditadura dos dados"[227].

Por sua vez, os arts. 25 e 26 do Regulamento estabelecem a necessidade de que a proteção de dados se dê desde a concepção (*privacy by design*) e por padrão (*privacy by default*)[228], sem se esquecer, no entanto, de ferramentas repressoras eficientes (privacidade em caso de falha). Em síntese, pensar a privacidade desde o projeto do sistema significa colocá-la em holofote quando do momento da própria definição dos meios de tratamento de dados, prevendo as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento.

Noutro giro, o art. 30 do RGPD estabelece uma espécie de custódia do dado, na medida em que cada responsável pelo tratamento deve guardar registro de todas as suas atividades de tratamento, com informações dos responsáveis, das finalidades, das categorias de titulares ou de dados pessoais (à luz da ideia de não individualização, mas de inserção em grupos), as categorias de destinatários daqueles dados, inclusive países estrangeiros, os prazos para a exclusão dos dados e as medidas de segurança lógica da informação.

O art. 35 do Regulamento prevê a necessidade de avaliação prévia do impacto sobre a proteção de dados nos casos em que o tratamento for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. Essa avaliação criteriosa contempla, no mínimo, uma descrição sistemática das operações a serem efetuadas e de suas respectivas finalidades legítimas, uma explanação acerca da necessidade e proporcionalidade envolvidas, uma avaliação sobre os riscos para os direitos e liberdades dos titulares e as medidas para fazê-los diminuir. Nos casos em que a análise resultar uma percepção de elevado risco, o responsável

---

[227] MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. Big Data: A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013. p.90.

[228] Artigo 25.o
Proteção de dados desde a conceção e por defeito
1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.
3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.os 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.o.

pelo tratamento deve proceder a uma consulta prévia à autoridade de controle, que avaliará a possibilidade do fazimento do tratamento.

Além disso, os arts. 40 a 43 do Regulamento estabelecem a possiblidade de se criar uma espécie de *selo de qualidade* para a identificação de pessoas que promovem o tratamento de dados de modo adequado. Em geral, são estabelecidos alguns critérios mínimos[229], que acabam resumindo todo o arcabouço protetivo da regulação europeia.

O art. 47 do RGPD determina que as empresas responsáveis pelo tratamento de dados pessoais – em qualquer de suas facetas – devem assegurar a aplicação dos princípios gerais de proteção de dados, tais como a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, a qualidade dos dados, a proteção dos dados desde a concepção e por padrão, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores.

Por fim, o RGPD estabelece uma multa de até 20 milhões de euros ou 4% do volume anual mundial de negócios, o que for mais elevado, para os responsáveis por tratamento abusivo dos princípios básicos estabelecidos na norma, inclusive acerca dos limites e condições do consentimento. Tal multa, a mais grave da norma, explicita como é importante que se tutele adequadamente o consentimento dos usuários, na medida em que o contrário – desprestigiar o consentimento – poderia dar azo a uma sucessão de abusos de direito.

Feito o panorama geral europeu sobre a proteção de dados, também é de se frisar a existência do *California Consumer Privacy Act of 2018* (CCPA)[230], que regula a proteção de informações pessoais na Califórnia, o berço de boa parte das empresas de tecnologia. O paradigma americano é substancialmente diverso do brasileiro e europeu, principalmente pela própria cultura jurídica de *common law*, além de que é certo que a LGPD se baseou, quase que

---

[229] Dentre eles, vale frisar a preocupação com: a) o tratamento equitativo e transparente; b) os legítimos interesses dos responsáveis pelo tratamento em contextos específicos; c) o recolhimento de dados pessoais; d) a pseudonimização dos dados pessoais; e) a informação prestada ao público e aos titulares dos dados; f) o exercício dos direitos dos titulares dos dados; g) as informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido. Além disso, são também relevantes: h) as medidas e procedimentos destinados à proteção de dados desde a concepção e por defeito e as medidas destinadas a garantir a segurança do tratamento, por meio do registro das atividades de tratamento; i) a notificação de violações de dados pessoais às autoridades de controle e a comunicação dessas violações de dados pessoais aos titulares dos dados; j) a transferência de dados pessoais para países terceiros ou organizações internacionais; e k) as ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento e os titulares dos dados em relação ao tratamento.

[230] CALIFÓRNIA, ESTADOS UNIDOS DA AMÉRICA. California Consumer Privacy Act of 2018. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>. Acesso em 6 abr. 2021.

integralmente, no RGPD, de modo que a norma californiana não é tão relevante para a análise exploratória ora empreendida, que não tem pretensões de esgotar o tema. O CCPA prevê, por exemplo, a proteção de informações pessoais, o que é mais abrangente do que o conceito de dados pessoais, por incluir, por exemplo, informações sobre propriedades e residência do consumidor.

No que é pertinente ao trabalho, cumpre ressaltar que a norma também se baseia no consentimento para o tratamento de dados, que significa qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do consumidor, por meio da qual o consumidor, ou o responsável legal do consumidor, uma pessoa com procuração, ou uma pessoa que atua como tutora do consumidor, inclusive por meio de uma declaração ou de uma ação afirmativa clara, significa concordar com o processamento de informações pessoais relacionadas ao consumidor para uma finalidade específica estritamente definida.

Esclarece-se que a aceitação de termos de uso gerais ou amplos, ou documento semelhante, que contenha descrições de processamento de informações pessoais junto com outras informações não relacionadas, não constitui consentimento. Passar o mouse sobre, silenciar, pausar ou fechar um determinado conteúdo não constitui consentimento. Da mesma forma, a concordância obtida pelo uso de padrões obscuros não constitui consentimento. A tendência é de que isso represente o fim da era *opt-out* na Califórnia, passando-se a um tempo do *opt-in*, que é mais ajustado à adequada tutela da proteção dos dados e da privacidade.

Feita a longa análise do RGPD e a brevíssima análise do CCPA, passa-se à exposição mais detalhada da LGPD, sobretudo nos pontos mais pertinentes ao presente trabalho.

2.5.3 Lei Geral de Proteção de Dados (LGPD)

De modo mais específico, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) dispõe sobre o tratamento de dados pessoais, inclusive em meios digitais (foco do trabalho), com o especial objetivo de promover os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ou seja, há foco em liberdade e privacidade para que se chegue ao contexto de maior autodeterminação informativa.

De acordo com Laura Schertel, "a grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo *ex ante* de proteção dedados, baseado no conceito de que não existem mais dados irrelevantes diante do

processamento eletrônico e ubíquo de dados na sociedade da informação"[231]. Isso porque os dados pessoais passam a ser encarados como projeções diretas da personalidade.

O art. 2º da Lei estabelece que alguns fundamentos da proteção de dados: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Por força do art. 3º da Lei[232], a legislação é aplicável a todos os aplicativos ora analisados, na medida em que os dados pessoais são coletados no território nacional, já que, por pressuposto, os usuários são situados no Brasil, independentemente de sua nacionalidade (art. 3º, § 1º). Em verdade, a própria coleta é uma das fases do tratamento de dados. Além disso, o tratamento de dados existente nos aplicativos móveis é, sim, para fins estritamente econômicos – a menos, em tese, nos aplicativos governamentais que são analisados; mas, mesmo para esses, a legislação é aplicável, por conter normas específicas –, de modo que não incide nenhuma das exceções do art. 4º.

A Lei também traz um rol dos mais importantes conceitos. Para ela, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Ou seja, não se limita "a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros"[233].

No que tange à terminologia *dado* e *informação*, é interessante notar que há certa sobreposição conceitual, na medida em que significam um fato ou determinado aspecto da realidade. De modo mais técnico, o *dado* tem uma conotação um pouco mais fragmentada, uma espécie de pré-informação, anterior ao procedimento interpretativo que daria maior sentido à

---

[231] MENDES, Laura Schertel Ferreira. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. REVISTA DOS TRIBUNAIS (SÃO PAULO. IMPRESSO), v. 1, p. 35, 2019.

[232] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

[233] PINHEIRO, Patrícia Peck. Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018, p. 25.

parcela de realidade. A *informação*, a seu turno, pressupõe uma espécie de depuração do conteúdo, tendo um sentido mais instrumental de redução das incertezas[234].

Ou seja, o *dado* é algo mais bruto, abstrato, sem efetiva repercussão prática na dinâmica social. A *informação* é uma espécie de resultado obtido após o tratamento correto do *dado*, para que ele tenha uma real conotação prática de poder mudar a realidade. "Mestrado" e "direito à proteção de dados" são dados brutos se encontrados isoladamente; "mestrado com foco no direito à proteção de dados" é uma informação. Como dizia Rodotà, ainda na década de 1970, transformar informação dispersa (dados) em informação organizada (informações) é uma novidade introduzida pelos dispositivos informáticos[235].

Bioni indica que prevalece o conceito expansionista pelo qual dado pessoal equivale a uma informação que, dentro de um esforço razoável – o que serviria para diferenciar o dado pessoal de dado anônimo –, identifica um sujeito, direta ou indiretamente[236].

Por sua vez, os dados pessoais sensíveis, à semelhança dos dados especiais do RGPD, são aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Salvo algumas hipóteses mais restritivas e que fazem sentido dentro do contexto específico, a diferença é que, pelo nível informacional desses dados sensíveis, eles só podem ser tratados quando houver consentimento específico e destacado pelo titular.

Outro conceito relevante diz respeito ao dado anonimizado, que é aquele cujo titular não pode ser identificado se se considerar a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento. De modo geral, e como já se enunciou, muitos provedores no âmbito digital alegam que os dados pessoais de que dispõem não são capazes de identificar o seu titular, justamente por terem sofrido o processo de anonimização, geralmente associado à rotulação do dado em grupos genéricos: sabe-se que a pessoa que mora no apartamento X gosta de livros, carros e joias, mas supostamente não se sabe que essa pessoa gosta do livro A, do carro B e da joia C, tampouco se identifica que a pessoa é o fulano Y.

Contudo, em um contexto de tratamento massivo de dados pessoais, em que o titular dessas frações de sua personalidade não consegue rastrear a cadeia percorrida pelo seu dado –

---

[234] DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.
[235] RODOTÀ, Stefano. Elaboratori elettronici e controllo sociale. Bologna: Il Mulino, 1973, p. 14.
[236] BIONI, Bruno Ricardo. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação/GPoPAI da Universidade de São Paulo. 2016, p. 34-35.

quando e onde foi coletado, para onde foi enviado, por quem foi tratado e para que está sendo usado hoje –, não parece razoável crer que esses dados, supostamente genéricos, abstratos e anonimizados, não são capazes de, quando agrupados, identificar com precisão um indivíduo.

Justamente à luz dessa realidade, o RGPD utiliza-se do termo *pseudonimização*, que parte de uma realidade em que a anonimização de fato é impossível. Tal procedimento consiste no tratamento de dados de modo que deixem de ser atribuíveis a um titular específico sem que se recorra a informações suplementares. Para tanto, essas suplementações devem ser mantidas separadamente, inclusive com medidas técnicas e organizativas do ponto de vista da tecnologia da informação, para que não seja possível atribuir a agregação a uma pessoa singular identificada ou identificável.

Ou seja, o RGPD já parte do pressuposto de que a agregação de dados dispersos pode identificar com absoluta precisão uma pessoa e tenta, com isso, ser um pouco mais transparente ao indicar que a anonimização de fato inexiste. O que se pode pretender é tentar evitar as vinculações entre os diversos dados coletados do usuário, que é exatamente o que os algoritmos mais sofisticados fazem, sendo que a exatidão no apontamento do indivíduo é, certamente, uma vantagem competitiva no atual mercado.

Enquanto isso, a LGPD aposta no conceito de anonimização, que é a forma pela qual se transforma um dado em dado anonimizado. A única questão mais aberta na Lei diz respeito ao fato de se mencionar a utilização de *meios técnicos razoáveis e disponíveis* no momento dessa anonimização. Ou seja, com esse critério de razoabilidade, a norma acaba deixando uma lacuna aberta, pois o que pode ser razoável para uns não é para outros. Pode ser, na prática, até mais abrangente do que o *choque* de realidade do RGPD com sua pseudonimização ao invés de anonimização.

O *Facebook*, por exemplo, certamente tem meios de anonimização muito mais sofisticados e eficientes do que a pequena farmácia do bairro, mas esta lida com informações relevantes e, legalmente, sensíveis. Sabendo disso, eventualmente as empresas maiores podem pretender *avocar* os dados pessoais para si por meio de outras menores antecedentes, que foram as efetivas responsáveis pela coleta, na medida em que o critério da razoabilidade para a anonimização poderia seguir padrões mais baixos.

Por dever de transparência, é necessário dizer que o contrário também pode ocorrer: o *Facebook*, justamente apostando que nenhuma instância fiscalizatória será capaz de entender seus sofisticados algoritmos – e é realmente complexo, pois se trata dos segredos comerciais das empresas e de suas vantagens competitivas –, pode fazer uma anonimização mais simples do que suas capacidades técnicas seriam capazes dentro da razoabilidade. Ao revés, a pequena

farmácia da esquina, em tese, terá um algoritmo mais simples de ser auditado para a aferição da anonimização.

Na prática, portanto, não há como garantir que os critérios de razoabilidade serão efetivamente seguidos na ponta do lápis. Quem vai fiscalizar? O titular tem o direito de requisitar a anonimização dos dados (art. 18, IV), a ANPD poderá dispor sobre padrões e técnicas utilizados nos processos de anonimização e verificar sua segurança (art. 12, § 3º). Mas cada pequena farmácia será fiscalizada? Alguém conseguirá entender o algoritmo das grandes empresas cujo negócio é tão somente o tratamento de dados pessoais? Questões meramente provocativas, mas que indicam que se deve esperar a realidade, sem muita expectativa positiva, fornecer as respostas.

Fato é que a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios (art. 12, § 1º). E, além disso, os dados anonimizados não são considerados dados pessoais, salvo se o processo de anonimização for revertido ou puder sê-lo com esforços razoáveis (art. 12, *caput*).

Na sequência, a LGPD, seguindo a linha das normas estrangeiras, define o consentimento como a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Sobre isso, Rodotà afirma que "raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados"[237], ou seja, o usuário perde de perspectiva a real utilidade de seus dados pessoais no bojo de organizações complexas e estruturadas, de modo que não consegue refletir sobre a real periculosidade daquilo com o que está consentindo.

O consentimento ser *livre* significa que o titular pode escolher entre aceitar ou recusar a utilização de seu dado sem intervenções que viciem sua concordância. Para a aferição, é essencial que se investigue a assimetria entre as partes, para verificar o real poder de barganha do cidadão no bojo do tratamento dos dados[238].

Também fortalecendo a centralidade do titular dos dados no ordenamento jurídico, a LGPD acaba enfrentando, nesse ponto, o funcionamento binário do *take it or leave it*, ao afirmar que, se o tratamento for condição para o oferecimento do produto ou serviço, o titular

---

[237] RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

[238] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

deve ser informado com destaque sobre o fato e sobre como poderá exercer seus direitos legais (art. 9º, § 3º). Essa parece a realidade de quase todos os aplicativos móveis, na medida em que as aplicações requerem o tratamento de dados para disponibilizarem o *download* da ferramenta – é justamente onde ganharão a remuneração pelo produto.

Fala-se que, com referido dispositivo, "visa-se oxigenar processos de tomada de decisão, além de incentivar configurações de privacidade personalizáveis e a possibilidade da manifestação do consentimento de forma granular, podendo o cidadão emitir autorizações fragmentadas no tocante ao fluxo de seus dados"[239]. Tal disposição é perfeitamente concorde com o funcionamento dos aplicativos em níveis, como se desenvolverá mais à frente.

Por sua vez, a qualificação *informado* significa que o titular deve dispor de informações necessárias e suficientes para avaliar corretamente a situação do tratamento dos dados e a forma como isso será operacionalizado. A informação é crucial para que o consentimento seja efetivamente consciente e livre, além de específico a determinadas situações. Deve haver transparência, adequação, clareza e suficiência nas informações prestadas sobre riscos e implicações do tratamento.

Para regular a qualidade dessas informações, a LGPD também dispõe que, na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (art. 9º, § 1º). Além disso, mudanças na finalidade original do tratamento, que não sejam compatíveis com o consentimento original, devem ser previamente informadas ao titular dos dados, que poderá revogar o seu consentimento caso não concorde com as alterações (§ 2º).

Por sua vez, a manifestação deve ser *inequívoca*, ou seja, não ambígua, clara, evidente, sem manipulação. Uma das melhores formas de garantir essa característica do consentimento é mudando o paradigma atual, de *opt-out* para *opt-in*. Se, respeitadas todas as demais balizas de informação e liberdade – além dos princípios atinentes à proteção de dados –, o usuário deliberadamente deu o *check* na caixinha não pré-selecionada para concordar com o tratamento, é razoável inferir que tenha, sim, sido inequívoco.

Ademais, também é de se falar que o tratamento dos dados deve respeitar a *finalidade* para a qual o usuário consentiu. Por ela, entende-se que o tratamento deve seguir propósitos legítimos, específicos, explícitos e informados, sem possibilidade de tratamento

[239] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

posterior de forma incompatível com essas finalidades, mesmo nos casos em que a base legal não for o consentimento do titular (art. 6º, I). Ou seja, o consentimento deve se referir a finalidades determinadas, sendo que autorizações genéricas para o tratamento são nulas (art. 8º, § 4º). O consentimento, assim, vale para determinado tratamento, agente e condição. Uma vez mais, avança-se na direção da granularidade das concordâncias para o tratamento.

Há ainda que se falar da necessidade de o consentimento ser *específico* e *expresso*, isso é, com carga participativa máxima do titular em algumas situações: a) quando há envolvimento de terceiros que não mantêm relação direta com o titular para o tratamento de seus dados; b) por conta da natureza do dado coletado: dados sensíveis; c) em razão da condição de vulnerabilidade do titular do dado: crianças e adolescentes; e d) na transferência internacional para um país sem o mesmo nível de proteção de dados que o Brasil. Trata-se de uma camada adicional de proteção, normalmente vinculada ao maior nível de clareza de exposição, quando se trata dessas hipóteses que merecem proteção legal mais estreita[240].

Na sequência, o art. 6º da LGPD[241] elenca os princípios a serem observados quando do tratamento dos dados pessoais. Uma primeira observação importante é a colocação da boa-fé em um papel de destaque, visto que o único princípio disposto no *caput* do artigo. Sustenta-se que tal técnica de construção legislativa indica que a boa-fé, principalmente a objetiva, deve permear toda a interpretação da norma, inclusive em seus aspectos principiológicos. Serviria a boa-fé, então, como uma espécie de *pedra de toque*[242] no bojo do universo da proteção de dados.

---

[240] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[241] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[242] Para usar a expressão de Celso Antônio Bandeira de Mello do direito administrativo.

Os primeiros três princípios – finalidade, adequação e necessidade –, que parecem os mais abstratos e relevantes, em muito se assemelham com os critérios para o teste de proporcionalidade[243] no âmbito dos direitos fundamentais, na medida em que se fala da relação possibilidade de o tratamento atingir o fim almejado (e informado pelo responsável), sempre com o respeito ao conceito europeu de minimização dos dados (só se trata o que for estritamente necessário para o fim).

Os demais sete princípios elencados, de modo não exaustivo, são mais técnicos e relacionados à operacionalização do tratamento em si: os dados dever ter qualidade, o que é de suma relevância pelo contexto de decisões automatizadas; o titular deve ter livre acesso aos dados tratados e à duração da operação; deve haver transparência quanto ao tratamento (um dever lateral natural da boa-fé); os dados devem estar submetidos a rígidos mecanismos de segurança e prevenção à ocorrência de danos; é impossível discriminar, ilícita ou abusivamente, o titular dos dados a partir do tratamento – perceba-se que a discriminação lítica (no sentido de diferenciação) é permitida, já que essa é a própria finalidade macro do tratamento –; e os responsáveis pelo tratamento devem prestar contas sobre as medidas de resguardo dos dados pessoais.

Tais princípios, como de praxe no ordenamento jurídico, são vetores interpretativos para a aplicação de todos os demais dispositivos, mais concretos, da LGPD. Invariavelmente, não excluem tantos outros concorrentes à melhor tutela dos dados pessoais e inspirarão densamente a análise empírica a ser feita.

Por sua vez, o art. 7º estabelece as hipóteses em que é viável o tratamento dos dados pessoais. Dentre outras circunstâncias, as mais relevantes para o presente trabalho são (i) o fornecimento de consentimento pelo titular do dado e (ii) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Ou seja, mais uma vez é explicitado o tênue balanceamento entre a tutela dos interesses empresariais e dos direitos do usuário.

Também é de se mencionar, especificamente para os aplicativos governamentais, a possibilidade de tratamento pela administração pública para a execução de políticas públicas. No caso concreto do presente trabalho, os aplicativos selecionados não parecem exatamente aderentes ao universo das políticas públicas – na medida em que oferecem serviços e funcionalidades muito específicos –, mas essa hipótese é testada em concreto na sequência.

---

[243] BARROSO, Luís Roberto. Os princípios da razoabilidade e da proporcionalidade no direito constitucional. Boletim de Direito Administrativo. Doutrina, pareceres e atualidades. Março/97. Pp. 156-166, p. 161.

Por sua vez, o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (art. 7º, § 3º), sendo inclusive dispensado o consentimento do titular (§ 4º). Ou seja, a tutela dos dados cujo acesso é público é minorada em relação àqueles eminentemente privados, mas ainda deve resguardar a boa-fé objetiva, com todos os seus deveres laterais já explicitados. Assim, mesmo a eventual dispensa do consentimento não minora a responsabilidade de seguir todos os demais preceitos da norma (§6º).

De certo modo, portanto, parece adequado o balizamento legal, na medida em que se chancela a boa-fé e se prescreve a necessária observância do contexto em que publicizada a informação, com propósitos legítimos e específicos (art. 7º, § 7º). Em comparação ao RGPD, a norma europeia parece até menos protetiva no ponto, por permitir inclusive o tratamento de dados sensíveis tornados públicos – a LGPD permite apenas o de dados pessoais não sensíveis. Por sua vez, relevante pontuar que, para que o dado pessoal seja compartilhado com outros controladores, deve haver consentimento específico do titular do dado (§ 5º)[244].

O art. 8º da LGPD[245] dá maior profundidade às balizas do consentimento. Ele deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular

---

[244] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...)
§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

[245] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

– os *checks* na tela de um celular parecem adequados. Embora se fale que a cláusula deva ser destacada se o consentimento for por escrito – dando a entender que seria somente nesse caso –, entende-se que deve haver destaque também no caso desse consentimento manifestado em meios eletrônicos, que nada mais são do que *por escrito lato sensu*. Quando do cotejo feito no § 1º, o legislador provavelmente se referiu à dissociação entre consentimento oral e por escrito.

Na sequência, transfere-se o ônus da prova de que o consentimento foi obtido corretamente ao controlador do tratamento, que é em nome de quem o operador do tratamento empreende seus esforços (§ 2º). O consentimento obtido de forma viciada é vedado (§ 3º), devendo ele se referir a finalidades específicas, sem autorizações genéricas, que são nulas (§ 4º). O consentimento pode ser revogado pelo titular, de modo gratuito e facilitado, sendo válido o tratamento anteriormente realizado, se respeitadas as demais balizas legais (§ 5º). O RGPD, nesse ponto, fala que o consentimento deve ser tão fácil de retirar quanto de dar, o que parece ser também o espírito da legislação brasileira, embora esses termos não tenham sido usados. Por fim, fala-se que as principais alterações no modo de tratamento dos dados devem ser informadas ao titular de modo destacado e específico, para que o titular possa delas discordar.

O art. 9º[246] trata do direito de livre acesso do titular às informações sobre o tratamento de seus dados, que devem ser claras, adequadas e ostensivas, identificando a finalidade do tratamento, forma e duração, identificação do controlador, responsabilidades, com menção aos direitos do titular e às responsabilidades dos agentes.

O interesse legítimo do controlador, como se viu, pode ser um fundamento para o tratamento dos dados pessoais, desde que para a promoção das próprias atividades do controlador ou para a prestação de serviços que beneficiem o titular, respeitadas as legítimas expectativas do usuário e seus direitos fundamentais. Nesses casos, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, desde que garantida a devida transparência (art. 10).

A ANPD pode solicitar, ao controlador, relatório de impacto à proteção dos dados quando o tratamento for baseado no legítimo interesse. É nesse contexto que surge a

[246] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
I - finalidade específica do tratamento;
II - forma e duração do tratamento, observados os segredos comercial e industrial;
III - identificação do controlador;
IV - informações de contato do controlador;
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI - responsabilidades dos agentes que realizarão o tratamento; e
VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

exigibilidade do teste de adequação, em que o responsável pelo tratamento deve registrar que, no caso concreto, seu legítimo interesse de tratar os dados sobrepujou o interesse do titular dos dados de mantê-los protegidos sob o manto da privacidade. Trata-se de um mecanismo interessante, mas cuja efetividade só poderá ser aferida na prática, a depender de quão exigente a ANPD for com esse teste de adequação.

Para os casos de aplicativos móveis, é possível que a justificativa para a coleta e tratamento dos dados pessoais seja bivalente: (i) de um lado, o provedor de aplicações tem o interesse de acessar os dados pessoais dos usuários para fins de promover o funcionamento do aplicativo e de monetizá-los para fins de publicidade comportamental; e, (ii) de outro lado, a própria publicidade comportamental pode ser encarada como um serviço que beneficia o titular do dado, na medida em que, em uma sociedade de consumo, o usuário que é submetido a um consumo mais específico e direcionado pode se sentir satisfeito em *poupar energia*: se ele tem interesse em carros, não deseja ver anúncio de bolsas.

O art. 11 da LGPD[247] dispõe que o tratamento de dados pessoais sensíveis só pode ocorrer (i) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas ou (ii) quando (para o que interessa ao trabalho), mesmo sem o consentimento do titular, for indispensável para o exercício regular de direitos, inclusive contratuais. Embora o exercício regular de direitos contratuais possa parecer um pouco abstrato e aberto, é razoável supor que se trata de caso de um consentimento prévio, em que o titular dos dados provavelmente consentiu com o tratamento quando assinou o contrato inicial.

O mais relevante desse artigo, no entanto, é possibilitar o tratamento dos dados sensíveis *apenas* com o consentimento qualificado do titular – ou seja, não é possível alegar legítimo interesse para tratar dados sensíveis. E, fazendo-se uma leitura sistemática com os §§ 4º e 5º – que vedam o uso compartilhado de dados de saúde para fins de obter vantagem econômica, inclusive seleção de riscos para a aceitação e o enquadramento de beneficiários –, parece ser o caso de se concluir que, para esses dados de saúde, nem mesmo o consentimento do titular poderia autorizar o tratamento.

O art. 12, além de versar sobre a anonimização dos dados – o que já se viu –, afirma que são considerados dados pessoais os utilizados para fins de formação de perfil comportamental de determinada pessoa identificada (§ 2º). A técnica de *profiling* se presta

[247] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: (...)
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem).

justamente a identificar a pessoa, mas a LGPD parece ter dito menos do que o necessário ao não mencionar a possibilidade de a pessoa ser identificável – mas tão somente a pessoa identificada. À luz de que o próprio conceito de dado pessoal versa também sobre a pessoa identificável, parece correto interpretar tal dispositivo no sentido de que mesmo o perfilamento que torna a pessoa meramente identificável é tratamento de dados pessoais, visto que o eventual processo de anonimização é reversível.

O art. 14 da LGPD[248] dispõe que o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado no seu melhor interesse, com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal – o controlador deve empreender esforços razoáveis para verificar que foi o responsável que deu o consentimento – , sendo que os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares.

Ademais, é vedado que os controladores condicionem a participação dos titulares dos dados em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade. Ou seja, trata-se de mais uma manifestação do requisito da estrita utilidade dos dados (minimização). Contudo, é claro que os provedores podem interpretar o termo "estritamente necessárias à atividade" como um salvo-conduto para acessar todas as informações que desejarem. Afinal, aos olhos de alguns, pode ser estritamente necessário monetizar os dados pessoais para disponibilizar o jogo gratuitamente.

Outra disposição muito relevante de tal artigo é o §6º, que manifesta a necessidade de as informações sobre o tratamento serem fornecidas de modo simples, claro, acessível, dadas

[248] Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

as características de baixo desenvolvimento do usuário (criança ou adolescente). Fala-se, inclusive, em uso de recursos audiovisuais para o adequado entendimento da criança. Entende-se que essa deveria ser a regra para todos os casos de tratamento de dados pessoais, e não apenas quando se tratar de crianças ou adolescentes. Com efeito, se sequer juristas e profissionais da tecnologia da informação conseguem entender adequadamente os termos de uso e políticas de privacidade, é impensável que um usuário ordinário tenha pleno entendimento.

Quanto ao art. 15 da LGPD, que versa sobre o término do tratamento dos dados, é obscura a possibilidade de o fim se dar a partir de uma comunicação do titular em casos de tratamento baseado no legítimo interesse do controlador. Isso porque, em seu inciso III, o dispositivo faz uma menção ao exercício da revogação do consentimento, sem explicitar com clareza se essa seria a única hipótese ou apenas um exemplo. Se apenas um exemplo, não seria necessário, na medida em que a revogação do consentimento seria um motivo de término do tratamento.

De acordo com o art. 17 da LGPD[249], toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Poder-se-ia discutir se pessoas jurídicas também teriam direito à proteção de dados – o que parece fazer sentido –, mas é fato que a LGPD não se imiscuiu no tema, que ainda pode ser tutelado pelas legislações mais específicas. Mas, nesse artigo, também sequer faria sentido falar de liberdade, intimidade e privacidade das pessoas jurídicas.

De acordo com o art. 18 da LGPD[250], alguns dos direitos básicos do usuário titular dos dados são: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o ordenamento

---

[249] Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

[250] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento;
II - acesso aos dados;
III - correção de dados incompletos, inexatos ou desatualizados;
IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

jurídico; (v) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador.

Além disso, fala-se em (vi) eliminação dos dados pessoais tratados com o consentimento do titular; (vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e (ix) revogação do consentimento inicialmente fornecido.

Sobre o direito de acesso aos dados – que é um dos mais basilares instrumentos para o titular auditar o tratamento de seus dados pessoais –, parece haver uma contradição entre o art. 18, II, e o art. 19, § 3º, na medida em que este denota uma restrição à solicitação de cópia integral dos dados pessoais apenas aos casos em que o tratamento tiver origem no consentimento do titular, ao passo que aquele dá a entender que o direito de acesso é amplo e independe da hipótese autorizativa inicial do tratamento. Parece mais correto entender que o § 3º retro disse menos do que deveria, devendo ser aplicado à luz do inciso II.

Mas, dentre os direitos elencados, aquele que parece ter maior relevância é justamente o fornecimento de informações claras sobre a consequência da não concessão de consentimento. É justamente a falta de transparência que se critica nesse trabalho e a proposta central de melhoria: se o provedor de aplicações fosse suficientemente claro sobre a consequência de o titular dos dados não querer fornecê-los de modo específico – *e.g.*, o não fornecimento do dado X poderia implicar o mau funcionamento do aplicativo em seu aspecto Y –, seria um importante passo rumo à tutela satisfatória dos direitos à privacidade. Isso se correlaciona com o conceito de *níveis de aplicativo* que se pretende desenvolver no presente trabalho, mas está longe de ser uma prática dos provedores de aplicação analisados.

Outro trecho muito relevante desse dispositivo é seu § 2º, que afirma que o titular do dado pode se opor ao tratamento realizado em caso de descumprimento ao disposto na LGPD. O dispositivo fala apenas em casos de dispensa do consentimento, mas se sustenta que mesmo em casos com consentimento, se ele for viciado, pode haver a oposição. Em tese, tal dispositivo permitiria ao titular opor-se ao tratamento realizado com base no legítimo interesse, com os naturais temperamentos pela boa-fé; afinal, se o usuário baixou o aplicativo e usou a ferramenta, com algum nível de consentimento (mesmo que mínimo), concordou com algum nível de tratamento (mesmo que mínimo). Supor o contrário talvez fosse um incentivo ao comportamento contraditório.

Por sua vez, o art. 20 traz a importante ferramenta de revisão de decisões unicamente automatizadas – que são cada vez mais comuns – baseadas no tratamento de dados pessoais e que afetem os interesses do titular, tais como a definição de perfil pessoal, profissional, de consumo ou de crédito e os aspectos de sua personalidade.

No que tange ao panorama específico do tratamento de dados, é relevante salientar que, embora os provedores de aplicações disponibilizem seus produtos no Brasil, esses dados fazem parte de um fluxo global, indo para países onde fazer o tratamento é mais barato ou onde há especialistas na conversão estatística de dados abstratos em informações mais concretas.

Nesse sentido, o art. 33 da LGDP[251] estabelece que a transferência internacional dos dados só é possível, dentre outros: (i) para países que proporcionem grau de proteção de dados pessoais adequado e quando o controlador oferecer e comprovar garantias de bom cumprimento das normas relativas à proteção de dados; (ii) quando houver garantias de cumprimentos dos direitos do titular, principalmente com normas corporativas globais e selos de *credibilidade*; e (iii) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

De modo geral, o primeiro conceito é fluido, apesar de haver alguns índices[252] – e, pelo art. 34 da LGPD[253], há previsão expressa de que a autoridade nacional crie um *ranking* próprio – que classificam os países quanto ao rigor na tutela do sigilo de dados – o Brasil, por exemplo, não é considerado um país adequado em termos de proteção de dados. Tais indicativos estatísticos abarcam também a segunda hipótese.

Por sua vez, o terceiro conceito envolve toda a problemática do consentimento, que, muitas das vezes, não é informado e adequado, na medida em que não é dada oportunidade ao usuário para efetivamente ler e entender aquilo com o que está consentindo. E, diga-se, qual é a possibilidade de o usuário recusar a transferência internacional se ela vai ocorrer de toda forma? Talvez fosse possível se cogitar de um consentimento mais granular ainda nessa hipótese: se o usuário quiser que seus dados fiquem apenas no Brasil, sob o manto da LGPD,

---

[251] Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: (...)
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

[252] CNIL. Data protection around the world. Disponível em: <https://www.cnil.fr/en/data-protection-around-the-world>. Acesso em: 24 mar. 2021.

[253] Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração: (...).

ou perderá algumas funcionalidades da aplicação, ou precisará fazer o pagamento pecuniário do valor adequado. Se essa solução é viável do ponto de vista técnico, não se sabe, mas seria o mais adequado para se apostar em um consentimento para essas transferências internacionais.

Na sequência, o art. 37 da LGPD dispõe que os responsáveis pelo tratamento, controlador e operador, devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Esse dado é muito relevante para que a legalidade das operações seja posteriormente auditada, seja pela ANPD, seja pelo próprio titular dos dados, seja por outras autoridades competentes (Ministério Público, por exemplo).

Por fim, resta uma lamentação quanto ao § 2º do art. 46, que dá a entender que, no Brasil, a preocupação do *privacy by design* só se aplica aos requisitos de segurança lógica dos dados. Em verdade, deveria se aplicar a todo o funcionamento do produto, sobretudo quanto às hipóteses autorizativas do tratamento.

Feita a análise descritiva pormenorizada dos pontos mais relevantes da Lei, é importante pontuar que, para Ana Frazão, "em se tratando de agentes detentores de posições dominantes ou quase monopolistas nos mercados em que atuam, tal como é o caso das grandes plataformas digitais, a LGPD certamente não será suficiente para, sozinha, endereçar todos os problemas decorrentes da atuação desses entes", de modo que será necessário um esforço do Direito da Concorrência para evitar o abuso de poder econômico[254].

Por sua vez, Patrícia Peck esquematiza algumas mudanças que os controladores de dados pessoais precisam fazer para se adequaram à LGPD: atualização de "tabela de temporalidade de guarda de logs de consentimento; Termo de uso e Política de privacidade (atualizar batendo tratamento x finalidade de uso x justificativa jurídica x matriz de consentimentos, novos direitos dos usuários como portabilidade, exclusão, minimização de uso, limitação e outros)"[255]. Como é visto na parte empírica do trabalho, as políticas de privacidade não foram atualizadas sequer para fazer constar formalmente a LGPD como norma aplicável, quanto mais para efetivamente promover uma adequação de conteúdo material.

Outros aspectos mais específicos do regulamento brasileiro de proteção de dados e do Marco Civil da Internet são tratados nos tópicos apartados, para que a verificação de seus

---

[254] FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[255] PINHEIRO, Patrícia Peck. Proteção de dados pessoais – comentários à Lei n. 13.709/2018. São Paulo: Saraiva, 2018.

efeitos seja mais clara e próxima. Passada a análise desse panorama jurídico específico sucinto, convém fazer um breve aporte sobre aspectos atinentes à teoria contratual moderna e ao direito do consumidor, vistas como o arcabouço jurídico existente para soluções de questões relativas à privacidade e à proteção de dados pessoais antes do surgimento do MCI e, principalmente, da LGPD. É o que se passa a brevemente fazer.

2.6 A privacidade, a proteção dos dados pessoais e sua disponibilidade

No conceito de Beltrão, os direitos da personalidade são o conjunto de direitos havidos por todos, mas que guardam especificidades que marcam a distinção de cada pessoa, sendo umbilicalmente ligados a cada pessoa que com ela se confundem e ajudam a expressar sua personalidade a terceiros. Inegavelmente, a privacidade é um dos direitos clássicos da personalidade[256]. Não se deve esquecer, contudo, a lição de que os direitos da personalidade são uma noção inacabada que deve ser cultivada, o que é especialmente relevante na atual sociedade de massificação dos dados pessoais[257].

Na teoria clássica, que inspirou a elaboração do atual Código Civil, os direitos da personalidade são considerados indisponíveis, compreensão que passou a ser relativizada, na medida em que se passou a compreender, dada a nova dinâmica fenomenológica do direito civil, que a tutela de referidos direitos não se restringe ao seu âmbito protetivo, mas também ao âmbito de exercício positivo. Ou seja, pode haver disponibilidade, renúncia ou limitação parcial dos direitos da personalidade, desde que voluntariamente – com consentimento – e dentro de certos limites de razoabilidade e tempo[258].

Compreende-se, assim, que a indisponibilidade não impede que determinados aspectos dos direitos da personalidade – como a imagem ou o nome, por exemplo – sejam objeto de negócios jurídicos. Para que essa disposição seja válida, é necessário, contudo, que se proceda a uma análise contextualizada e de acordo com as cláusulas constitucionais e legais[259].

A concepção de que os direitos da personalidade são relativamente disponíveis passa pela própria compreensão da autodeterminação dos interesses pessoais no tocante ao livre

---

[256] BELTRÃO, Silvio Romero. Direitos da personalidade. 2. ed. São Paulo: Atlas, 2014, p. 10.
[257] MARTINS-COSTA, Judith. *Pessoa, personalidade, dignidade*: ensaio de uma qualificação. Tese (Livre-docência) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2003. p. 107: "Por isso mesmo, a noção de direitos da personalidade é inacabada, transitiva – em uma palavra, é cultivável".
[258] CANTALI, Fernanda Borghetti Direitos da Personalidade: disponibilidade relativa, autonomia privada e dignidade humana. Dissertação (Mestrado em Direito) – Faculdade de Direito, PUCRS, Porto Alegre, 2008, 271f.
[259] ROSENVALD, Nelson; NETTO, Felipe Braga; FARIAS, Cristiano Chaves de. Manual de Direito Civil – Volume único. 4. Ed. rev, ampl. e atual. – Salvador: Ed. JusPodivm, 2019, p. 239.

desenvolvimento da personalidade, que também são dimensões da dignidade humana, que protege o projeto de desenvolvimento espiritual e moral da pessoa em si mesma. Ou seja, se uma pessoa acha que é vantajoso ceder temporariamente seu direto personalíssimo à imagem a uma campanha publicitária, por exemplo, não se pode pretender impedir esse tipo de ajuste sob o fundamento de que o direito à personalidade seria indisponível[260].

Primando por um sistema centrado na dignidade humana, deve haver coexistência entre a ideia de que os direitos da personalidade são essencialmente indisponíveis, mas que possuem aspectos compatíveis com uma disponibilidade relativa. Dessa coexistência, constata-se que a solução para casos limítrofes deve ser balizada pela ponderação no caso concreto, num verdadeiro teste de proporcionalidade para aferir qual direito fundamental – autonomia privada ou direito da personalidade, do mesmo indivíduo titular – deve prevalecer no caso, sem que se fira o núcleo essencial de qualquer deles: a dignidade humana.

Como já se enunciou, a possibilidade de dispor dos direitos da personalidade, em algum grau, é uma verdadeira necessidade para a efetiva deferência à dignidade humana. Diz-se que "é a partir da renúncia total ou parcial do exercício de direitos da personalidade que uma pessoa pode ser o que ela é ou pretende ser (livre desenvolvimento da personalidade), sentindo-se bem consigo mesma, e buscar seus projetos de vida". Tal conclusão, claro, deve estar acompanhada de asteriscos pontuais, na medida em que a disponibilidade do exercício dos direitos da personalidade "não pode se traduzir em autolesão à dignidade humana, tampouco atrofiamento das singularidades de cada fase do desenvolvimento humano"[261].

Assim, é de se concluir que os direitos da personalidade podem sofrer limitações, ainda que não especificamente previstas em lei, não podendo ser exercidos com abuso de direito de seu titular ou em contrariedade à boa-fé objetiva, função social, solidariedade e aos bons costumes. Tais limitações devem ser voluntárias, não permanentes e não gerais. Valoriza-se, pois, a autonomia privada, desde que balizada pelos critérios mais abertos retro, o que representa uma espécie de emancipação da outrora cultura paternalista de indisponibilidade dos direitos de personalidade. Fala-se, assim, em uma espécie de autonomia digna[262].

---

[260] CANTALI, Fernanda Borghetti Direitos da Personalidade: disponibilidade relativa, autonomia privada e dignidade humana. Dissertação (Mestrado em Direito) – Faculdade de Direito, PUCRS, Porto Alegre, 2008, 271f.

[261] DOS REIS, Jorge Renato; BOLESINA, Iuri. A disponibilidade (no exercício) dos direitos da personalidade como deferência à dignidade humana no direito civil constitucionalizado. Revista Em Tempo, [S.l.], v. 14, p. 11-30, mar. 2016. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/1287>. Acesso em: 22 maio 2021.

[262] DOS REIS, Jorge Renato; BOLESINA, Iuri. A disponibilidade (no exercício) dos direitos da personalidade como deferência à dignidade humana no direito civil constitucionalizado. Revista Em Tempo, [S.l.], v. 14, p. 11-30, mar. 2016. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/1287>. Acesso em: 22 maio 2021.

É verdade que os critérios abertos para a aferição da validade da disposição dos direitos da personalidade tendem a causar dificuldades teóricas e práticas na análise do jurista, na medida em que carregam percepções imprecisas, vagas e influenciáveis por outros critérios também fluidos, como tecnologia, ciência, justiça, moral, religião, dentre outros[263].

A questão, então, parece paradoxal: ao mesmo tempo em que se aceita que o livre desenvolvimento da personalidade demanda uma liberdade ampla – inclusive com possibilidade de disposição de parcelas dos direitos previstos, numa verdadeira deferência à dignidade humana –, recorta-se a manifestação ampliativa por manifestações mais comuns, como os bons costumes. Dá-se liberdade, mas nem tanto[264].

E, sabendo que, dos direitos da personalidade, decorrem a autodeterminação informativa, a proteção dos dados pessoais e a privacidade, é também fato que, na medida em que relacionados à identificação, potencial ou efetiva, de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual, da privacidade e do livre desenvolvimento da personalidade, sob pena de lesão a esses direitos[265].

Assim, é certo que, hoje, se admite a possibilidade de disponibilidade dos direitos de personalidade, na medida em que são verdadeiros bens jurídicos[266]. Fala-se, assim, em indisponibilidade relativa, revestida de caráter voluntário, específico e temporário, devendo ser respeitados os limites inicialmente construídos no contrato, sob pena de responsabilidade civil.

Ingo Sarlet afirma, dessa forma, que não é possível, em termos abstratos e genéricos, afirmar a (in)disponibilidade de determinado direito da personalidade, na medida em que isso depende de "um conjunto de circunstâncias e pressupostos objetivos e subjetivos, inclusive e especialmente a repercussão do ato individual de renúncia em relação a interesses e direitos fundamentais ou mesmo interesses coletivos"[267].

Afirma-se, dessa forma, que a renúncia, ainda que parcial, pressupõe a capacidade do titular e o seu livre consentimento informado, além de encontrar limites na dignidade da pessoa humana e no conteúdo do direito renunciado, bem como a necessária satisfação de

---

[263] SCHREIBER, Anderson. Direitos da personalidade. 2. ed. São Paulo: Atlas, 2013, p. 34.
[264] BOLESINA, Iuri; SCHROEDER, Helena Carolina. A "limitação" voluntária dos direitos da personalidade no direito civil contemporâneo. XII Seminário Nacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea. Unisc, ed. 2016.
[265] BRASIL. Supremo Tribunal Federal. ADI-MC nº 6.387/DF, Rel. Min. Rosa Weber, julgamento em 7/5/2020.
[266] BORGES, Roxana Cardoso Brasileiro. Disponibilidade dos direitos de personalidade e autonomia privada. 2. Ed. São Paulo: Saraiva, 2007.
[267] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilhere; MITIDIERO, Daniel. Curso de direito constitucional. 2. Ed. São Paulo: Editora Revista dos Tribunais, 2013, p. 403.

exigências de proporcionalidade e razoabilidade. Dignidade da pessoa humana é, assim, fundamento da renúncia e limite à sua amplitude.

Dentro do panorama de proteção de dados pessoais, o mais importante é conseguir fixar o sentido e o alcance da dignidade humana em termos práticos, à luz de seus três elementos essenciais: o valor intrínseco de cada pessoa, sua autonomia individual e o valor comunitário[268], colocando a pessoa na centralidade do ordenamento jurídico como verdadeiro sujeito de direitos, e não mais o objeto de outrora[269].

Entendendo a privacidade como uma manifestação direta da dignidade da pessoa humana – sobretudo em tempos atuais de novas tecnologias, com uso massificado e ampla exposição –, Bessa afirma que a "a necessidade humana de não compartilhar com outros - ou de restringir a pessoas mais próximas - alguns fatos, desejos e informações pessoais é tão patente que o senso comum considera a privacidade, ao contrário do que defendem os estudiosos, um valor em si mesmo"[270].

No mesmo sentido, Ingo Sarlet leciona que "as conexões entre o princípio da dignidade da pessoa humana e o direito fundamental à proteção dos dados pessoais são intensas, embora nem sempre compreendidas do mesmo modo no âmbito das diferentes ordens jurídicas. Os dois principais pontos de contato, todavia, são o princípio autonômico (autodeterminação) e os direitos de personalidade, representados aqui, por sua vez, pelo direito (de natureza geral) ao livre desenvolvimento da personalidade e os direitos especiais à privacidade e à autodeterminação informativa, igualmente conectados entre si, mas que não esgotam o leque de alternativas"[271].

Além disso, necessário pontuar que a disponibilidade relativa dos direitos de personalidade também encontra limite nos interesses de terceiros, na medida em que a dignidade humana possui uma dimensão intersubjetiva e relacional. Numa perspectiva interna, afirma-se que a disponibilidade parcial do direito – ou de seus aspectos patrimoniais – deve ser pautada pelo real desenvolvimento da personalidade humana, não podendo chegar ao ponto extremo de objetificação da pessoa. Aceita-se, assim, a disponibilidade como ferramenta necessária à plena dignidade humana, mas não como uma forma de mercantilização da pessoa.

---

[268] BARROSO, Luis Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo: A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016, p. 9-87.
[269] SCHREIBER, Anderson. Direitos da personalidade. 2. ed. São Paulo: Atlas, 2013. p. 7.
[270] BESSA, Leonardo Roscoe. O consumidor e os limites dos bancos de dados de proteção ao crédito. São Paulo: Revista dos Tribunais: 2003, p. 88.
[271] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz. Tratado de proteção de dados pessoais. São Paulo: Forense: 2021.

Diante desses enxutos ensinamentos[272], é de se admitir que os termos de privacidade invariavelmente carregam a intrínseca discussão sobre disponibilidade dos direitos da personalidade. Sendo a privacidade uma das manifestações e necessidades da personalidade, é certo que também guarda um caráter de disponibilidade relativa. E, quando da aceitação dos termos de privacidade, é também certo que, em algum grau, o usuário e titular do direito abre mão de parcela do seu direito antes intocável em troca do benefício consistente na utilização da aplicação no seu celular.

A questão é saber se essa disponibilização de parcela de seu direito da personalidade atendeu os requisitos antes expostos: boa-fé objetiva, função social, solidariedade, bons costumes, temporariedade, especificidade, respeito ao núcleo da dignidade humana, não objetificação do titular, proporcionalidade, razoabilidade e voluntariedade. O cerne do debate, portanto, remonta à averiguação de respeito ou não a referidos critérios.

Entende-se que a LGPD acabou por materializar todos os requisitos discutidos no pretérito para a disponibilidade dos direitos de personalidade. Assim, havendo aderência à LGPD, quaisquer critérios abstratos de validade da disposição de parcelas dos direitos da personalidade são plenamente atendidos.

Com efeito, quanto à boa-fé objetiva, o termo de privacidade deve guardar boa relação com os deveres de informação, colaboração e cooperação – e justamente esses são pressupostos para que haja consentimento válido ou para que o interesse legítimo também seja critério para viabilizar o tratamento dos dados, na medida em que se deve declinar qual é o interesse. Quanto à função social e à solidariedade, é certo que se tutela externamente os efeitos dos termos de privacidade, mas também há nítida preocupação com a tutela interna, mormente no tocante à necessidade de algum nível de equivalência negocial entre as partes.

Os bons costumes, no atual ambiente de não respeito às normas de proteção de dados pessoais, não parecem a melhor referência limitante. Mas, havendo evolução rumo a um maior comprometimento dos provedores de aplicação com as normas de proteção de dados, é possível que se comece a criticar de modo mais consistente um ou outro aplicativo que não tutele adequadamente a privacidade e os dados de seus usuários em face de outros que assim procedem.

Por sua vez, temporariedade e especificidade são dois conceitos relevantes, na medida em que o usuário, na maioria das vezes, é obrigado a dar consentimento a tratamentos

[272] Em que se ignorou deliberadamente o intenso debate histórico sobre a possibilidade ou não de dispor dos direitos da personalidade, na medida em que se aceitou, de antemão, que hoje é razoavelmente pacífica na discussão jurídica a conclusão de indisponibilidade relativa ou essencial.

para além do estritamente necessário ao correto funcionamento da plataforma – o que também viola o princípio da necessidade –, além de perder o rastreio de seus dados pessoais. Isso é, não consegue ter uma espécie de *cadeia de custódia* do seu dado, sem saber se ele já foi eliminado – em tese, deveria ser assim que o tratamento perdesse a justificativa – ou não.

A voluntariedade é aferida, como já se enunciou, na própria manifestação do consentimento do usuário, que deve ser qualificado. Contudo, a prática demonstra que o consentimento quase nunca se dá como a lei pretendeu que ocorresse, normalmente por não ser informado e efetivamente livre, dada a metodologia do *tudo ou nada*.

Proporcionalidade e razoabilidade são critérios expressamente previstos na LGPD para a hipótese de se utilizar o legítimo interesse do responsável pelo tratamento para justifica-lo. Deve-se respeitar o já clássico desenvolvimento das etapas de adequação, necessidade e proporcionalidade em estrito sentido. Contudo, os termos de privacidade acabam não demonstrando de modo satisfatório os resultados do teste – se é que o teste é efetivamente empreendido antes do tratamento.

Por fim, o respeito ao núcleo essencial da dignidade humana e a não objetificação do usuário são duas finalidades e requisitos essenciais do tratamento dos dados pessoais no bojo dos aplicativos de celular. Fala-se que, em uma miríade de serviços ditos gratuitos, a mercadoria é o próprio titular dos dados. Contudo, não se pode aceitar esse panorama, devendo haver verdadeira inversão conceitual, justamente para que não se chancele a subsistência da coisificação humana.

Dessa forma, como pontua Ana Frazão, é inequívoco que o grau de disponibilidade sobre os dados pessoais têm naturais limitações[273]. No bojo do presente estudo, a disponibilidade relativa é normalmente manifestada pelo próprio consentimento do usuário, solução de mercado já antiga e que foi naturalmente positivada na LGPD.

Convém, agora, fazer um rápido retrospecto sobre como era possível proteger os dados pessoais antes do advento das normas específicas sobre direito e internet. É verdade que Bioni diz ser inviável, no passado, proteger de forma adequada os dados pessoais à luz da proteção contratual do consumidor, na medida em que se trata de uma posição *ex post*, ao passou que a racionalidade de proteção de dados pessoais é forjada no funcionamento *ex ante*[274].

---

[273] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[274] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas]: "A extensa adjetivação empregada ao consentimento visa a garantir previamente ao cidadão o controle dos seus dados pessoais. Por isso, ainda que válida, a proteção contratual do consumidor no âmbito das políticas de privacidade seria frustrante, já que, na

Mesmo assim, fato é que a proteção contratual foi, praticamente até o ano passado, a única existente no Brasil, de modo que discorrer brevemente sobre seus principais conceitos e princípios é útil à análise aqui proposta.

O próprio autor, aliás, apresenta uma proposta de compatibilização, à luz do diálogo das fontes, entre a LGPD e o restante do ordenamento jurídico brasileiro, mormente o Marco Civil da Internet, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Código de Defesa do Consumidor e o Código Civil. Há diversos regimes de coexistência – complementariedade, subsidiariedade, coerência sistemática, coordenação e adaptação sistêmica – no tocante a diversos aspectos: bases legais para o tratamento dos dados, dever de informação, transparência, consentimento informado, meios de obtenção do consentimento, arestas para o consentimento livre, expresso e específico, além de balizas para a legítima expectativa e o legítimo interesse. Assim, importante fazer sucinta análise acerca de alguns aspectos desse panorama normativo.

2.7 Um passo atrás: aspectos de direito contratual e de direito do consumidor

Nesse momento, busca-se proceder à colocação dos termos de privacidade de aplicativos móveis no ordenamento jurídico: trata-se de contratos eletrônicos. Pela relevância do ponto para a posterior análise crítica a ser empreendida, também importante tecer comentários acerca dos princípios basilares que orientam o direito contratual.

Antes de começar, porém, é necessário salientar que Shoshana Zuboff classifica os termos de privacidade e de uso de aplicações de internet que têm como base a economia de dados como verdadeiros *não contratos*, na medida em que não se prestam a efetivamente mitigar a inevitabilidade e a incerteza, como classicamente pensado sob a lógica econômica contratual. Isso porque, no atual cenário de datificação, não há incertezas por parte dos controladores dos dados pessoais, mas apenas a certeza do lucro[275].

Mas, para além dessa contundente e inevitável crítica, é de se dizer que Orlando Gomes define, em abordagem inicial, contrato como "uma espécie de negócio jurídico que se distingue, na formação, por exigir a presença de pelo menos duas partes. Contrato é, portanto,

melhor das hipóteses, a prometida esfera de controle seria a posteriori. Por isso, a proteção contratual do consumidor no âmbito das políticas de privacidade não deve ser vista como o mecanismo ideal para a proteção dos dados pessoais. Deve ser encarada como uma ação paliativa se a causa regulatória primária falhar, qual seja, o empoderamento ex ante do cidadão para exercer um controle genuíno sobre seus dados pessoais".

[275] ZUBOFF, Shoshana. Big other: surveillance capitalism and the propects of an information civilization. Journal of Information Technology, 30, 2015, p. 75-89, p. 80-81.

negócio jurídico bilateral, ou plurilateral"[276]. De modo mais analítico, Caio Mário estabelece o segundo conceito para contrato:

> é um negócio jurídico bilateral, e de conseguinte exige o consentimento; pressupõe, de outro lado, a conformidade com a ordem legal, sem o que não teria o condão de criar direitos para o agente; e, sendo ato negocial, tem por escopo aqueles objetivos específicos. Com a pacificidade da doutrina, dizemos então que o contrato é um acordo de vontades, na conformidade da lei, e com a finalidade de adquirir, resguardar, transferir, conservar, modificar ou extinguir direitos. Dizendo-o mais sucintamente, e reportando-nos à noção que demos de negócio jurídico, podemos definir contrato como o "acordo de vontades com a finalidade de produzir efeitos jurídicos[277].

Portanto, o contrato é constituído por duas espécies de declaração de vontade: uma proposta/oferta e uma aceitação/consentimento. Assim, só se fala em contrato quando três aspectos são atingidos: (i) um alinhamento acerca da natureza e da própria existência do contrato; (ii) um alinhamento sobre o objeto do contrato; e (iii) um alinhamento sobre as suas cláusulas.

Ademais, é inevitável, dentro do contexto do presente trabalho, que se diga que os contratos eletrônicos são uma modalidade de contrato atípico que traduz uma transação eletrônica em que as declarações de vontade são também eletrônicas, inclusive automaticamente, normalmente com a aceitação, pelo consumidor, de uma oferta pública por meio de um simples clique no computador ou na tela do celular[278].

Partindo-se de todo o exposto, é fora de cogitação que os termos de privacidade de aplicativos móveis são verdadeiros contratos, na medida em que chancelam o alinhamento de vontades: de um lado, a provedora de aplicações quer atingir mais um usuário, para resguardar seus válidos interesses econômicos; de outro lado, o usuário quer acessar as facilidades promovidas pela aplicação; e o contrato que chancela essa convergência de vontades, no que toca à proteção de dados e ao respeito à privacidade, é justamente a política de privacidade de cada aplicativo.

Por se dar em ambiente notadamente informático – aparelhos celulares –, também é certo que se trata de um contrato eletrônico. De modo ainda mais específico, em sua modalidade de contratos interativos, na medida em que se trata de verdadeiros contratos de

---

[276] GOMES, Orlando. Contratos. 25. ed. Rio de Janeiro: Forense, 2002.
[277] PEREIRA, Caio Mário Silva. Instituições de Direito Civil: Contratos. 20 ed. Rio de Janeiro: Forense, 2016. v.3.
[278] PINHEIRO, Patrícia Peck. Contratos digitais: apenas um meio ou nova modalidade contratual? Disponível em: <https://www.conjur.com.br/2016-jul-29/patricia-peck-contratos-digitais-sao-modalidade-contratual>. Acesso em: 23 mar. 2021.

adesão entre o usuário e as regras postas pelo provedor de aplicações. O usuário *conversa* apenas com o sistema, previamente programado[279].

Passado esse sintético espectro da discussão sobre o conceito de contrato, é relevante trazer à baila alguns de seus princípios norteadores, que, sobretudo, funcionam como sua baliza interpretativa. A importância dessa sucinta discussão é notória, afinal, as cláusulas gerais são a *porta de entrada* dos valores constitucionais nas relações privadas[280]. De modo semelhante, nas palavras de Bandeira de Mello, "a desatenção ao princípio implica ofensa não apenas a um específico mandamento obrigatório, mas a todo o sistema de comandos. É a mais grave forma de ilegalidade ou inconstitucionalidade"[281].

De modo preambular, a discussão sobre o princípio da autonomia da vontade (ou autonomia privada, em uma visão mais moderna sob o holofote da função social do contrato) ganha destaque, na medida em que a vontade racional – diferente do instinto, portanto – é o elemento propulsor da qualidade de humano, que o diferencia de todas as demais espécies. Trata-se de uma herança do liberalismo em sua acepção clássica do final do século XIX, incorporada pela Constituição Federal em seu art. 1º, IV[282], que tutela a liberdade de iniciativa, recentemente regulamentada pela lei de liberdade econômica.

Nessa esteira, ao passo que a liberdade de contratar guarda relação com a "plena liberdade para a celebração dos pactos e avenças com determinadas pessoas, sendo o direito à contratação inerente à própria concepção da pessoa humana, um direito existencial da personalidade advindo do princípio da liberdade" – ou seja, uma liberdade de escolher com quem contratar –, a liberdade contratual se relaciona "com o conteúdo do negócio jurídico, ponto em que residem limitações ainda maiores à liberdade da pessoa humana"[283].

A autonomia privada, portanto, constitui verdadeira liberdade que a pessoa tem de regular os seus próprios interesses. Essa autonomia não é absoluta, na medida em que conformada por normas de ordem pública. Assim, e de modo sistematizado, a autonomia privada é o regramento básico, particular influenciado por normas de ordem pública, por que se consideram no contrato fatores psicológicos, econômicos, políticos e sociais para além da própria vontade das partes. É uma manifestação da basilar expressão da dignidade humana de

---

[279] LOVATO, Luiz Gustavo. Contratos Eletrônicos. Rio de Janeiro: Lumen Juris. 2011.
[280] SUPREMO TRIBUNAL FEDERAL. RE nº 201.819/RJ, voto do Min. Gilmar Mendes, Segunda Turma, Diário da Justiça - 27/10/2006.
[281] MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. São Paulo: Malheiros, 2000.
[282] Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) IV - os valores sociais do trabalho e da livre iniciativa.
[283] TARTUCE, Flávio. Direito civil, v. 3: teoria geral dos contratos e contratos em espécie. 13. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.

autorregulamentar interesses, desde que com alinhamento mínimo aos princípios sociais contratuais[284].

Uma das limitações ao amplo exercício da autonomia privada é o princípio da função social do contrato, que busca a tutela da igualdade em seu aspecto material, ao partir do pressuposto de que a posição de debate volitivo não é a mesma entre os contratantes. Partindo-se desse paradigma, afirma-se que "os contratos devem ser interpretados de acordo com a concepção do meio social onde estão inseridos, não trazendo onerosidade excessiva às partes contratantes, garantindo que a igualdade entre elas seja respeitada, mantendo a justiça contratual e equilibrando a relação onde houver a preponderância da situação de um dos contratantes sobre a do outro". Valorizam-se, assim, equidade, razoabilidade, bom senso e boa-fé, afastando-se o enriquecimento sem causa[285].

Ou seja, a função social dos contratos visa à proteção da parte mais vulnerável na relação contratual, sendo que, "à luz da personalização e constitucionalização do Direito Civil, pode-se afirmar que a real função do contrato não é a segurança jurídica, mas sim atender os interesses da pessoa humana"[286]. Nessa linha, sob a ótica constitucional, a função social do contrato é matéria de ordem pública abarcada pelo âmbito de proteção da tutela da função social da propriedade (art. 5º, XXIII[287], e art. 170, III[288], da Constituição).

Por fim[289], é também possível falar em eficácia interna da função social dos contratos, que se manifesta pela mitigação da força obrigatória do contrato, proteção da parte mais vulnerável (consumidores, aderentes, usuários de aplicativos), vedação da onerosidade excessiva, conservação contratual e autonomia privada, proteção dos direitos individuais e nulidade de cláusulas abusivas. Por sua vez, a eficácia externa da função social do contrato é extraída quando o ajuste gera efeitos perante terceiros ou quando a conduta de outrem repercute no contrato[290]. No âmbito dos aplicativos, como já se viu pelo *case* do *Facebook*, é possível

---

[284] Ibidem.
[285] TARTUCE, Flávio. Direito civil, v. 3: teoria geral dos contratos e contratos em espécie. 13. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.
[286] TARTUCE, Flávio. Direito civil, v. 3: teoria geral dos contratos e contratos em espécie. 13. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.
[287] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXIII - a propriedade atenderá a sua função social.
[288] Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: (...) III - função social da propriedade.
[289] A função social do contrato ganha contornos especialmente relevantes no âmbito do direito do consumidor, mas, por critérios de melhor organização do presente trabalho, essa discussão é mais detalhada no tópico seguinte.
[290] TARTUCE, Flávio. Direito civil, v. 3: teoria geral dos contratos e contratos em espécie. 13. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.

mencionar a necessidade da aplicação das duas esferas da função social do contrato, na medida em que não se costuma respeitar os dados do próprio usuário principal, o que também significa, não raras vezes, o acesso a dados de terceiros – a exemplo do caso da Cambridge Analytica.

Por outro lado, princípio histórico que merece comentário mais analítico é o da força obrigatória dos contratos (*pacta sunt servanda*). Trata-se de uma preocupação com a tutela da estabilização de expectativas da sociedade – que, *ultima ratio*, é a finalidade precípua do Direito[291]. De modo ainda incipiente, é de se considerar que tal vetor interpretativo é direcionado ao sentido de dar às cláusulas consensualmente previstas a armadura da supremacia do interesse público.

Em razão do contexto de um mundo pós-moderno em que o individualismo vem cedendo espaço, é fora de dúvida que o princípio do *pacta sunt servanda* vem perdendo espaço. Concorda-se aqui com a posição para a qual é provável que, no futuro, a força obrigatória tende a ser substituída pela tutela da conservação dos contratos ou da própria boa-fé objetiva, em sua acepção de proteção à confiança[292].

Nesses termos, o princípio da boa-fé objetiva impõe o dever de agir probo, leal e com respeito à confiança recíproca entre as partes. Trata-se de norma positivada no art. 422 do Código Civil[293], e que emana seus efeitos para todos os momentos contratuais, desde as tratativas para a sua conformação, passando pela execução, até chegar ao momento pós-contratual, de eventual aferição de responsabilidades.

Trata-se da ideia de proteção contra a violação aos deveres anexos, laterais ou secundários do contrato, ou seja, para além das próprias cláusulas contratuais – que seriam notadamente o dever primário –, os contratantes deveriam respeitar diversos outros padrões de conduta objetivamente impostos. E, nesse caso, a violação a esses padrões esperados implicaria verdadeira violação positiva ao contrato. De posse desse panorama, pode-se inclusive pensar na seguinte *fórmula matemática*: Boa-fé Objetiva = Boa-fé Subjetiva (boa intenção) + Probidade (Lealdade)[294].

Alguns dos deveres anexos mais citados são: a) o dever de cuidado em relação à outra parte negocial; b) o dever de respeito; c) o dever de informar a outra parte quanto ao conteúdo do negócio; d) o dever de agir conforme a confiança depositada; e) o dever de lealdade

---

[291] LUHMANN, Niklas. *El derecho de la sociedad*. Cidade do México: Editorial Herder, 2006, p. 192.
[292] TARTUCE, Flávio. Direito civil, v. 3: teoria geral dos contratos e contratos em espécie. 13. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.
[293] Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé.
[294] Ibidem.

e probidade; f) o dever de colaboração ou cooperação; g) o dever de agir conforme a razoabilidade, a equidade e a boa razão; h) *tu quoque* (não fazer ao outro o que não faria contra si); e i) *venire contra factum proprium* (evitar o comportamento contraditório); j) *duty to mitigate the loss* (dever de o credor mitigar o prejuízo ou a própria perda), entre outros[295].

Para além da teoria dos deveres laterais, também se concebe a existência de três funções parcelares da boa-fé. A primeira é a função interpretativa (art. 113 do CC[296]), que indica que a boa-fé deve servir como paradigma de interpretação dos negócios jurídicos. A referida norma, aliás, impõe a mesma função para os costumes, para a racionalidade econômica do ajuste e para a preservação de eventual benesse interpretativa à parte aderente. Também chama atenção a interpretação à luz do comportamento das partes após a celebração do negócio jurídico, o que é uma manifestação do princípio geral de vedação ao comportamento contraditório.

No caso dos aplicativos, o provedor poderia, por exemplo, alegar que, por o usuário continuar *usando* a aplicação diuturnamente, estaria manifestando um eventual consentimento continuado com o tratamento dos dados; ou, o legítimo interesse do provedor, que está fornecendo um serviço *continuamente gratuito*, também poderia ser atendido. Entende-se que essa não é a melhor interpretação, na medida em que não é o uso continuado da aplicação que suplantará eventuais lacunas no *enforcement* em concreto das normas protetivas dos dados pessoais. Mas, de toda forma, por ser mais aberta, é naturalmente aplicável ao presente contexto de discussão acerca de privacidade e proteção de dados.

Por sua vez, a função integrativa (art. 422 do CC) significa colocar em holofote os próprios deveres anexos delineados anteriormente, ou seja, ainda que determinadas cláusulas não estejam contratualmente previstas, elas devem ser respeitadas. Uma das aplicações mais práticas dessa função para o presente trabalho é o dever lateral de prestar informações relevantes de que conheça.

---

[295] Ibidem.

[296] Art. 113. Os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração.
§ 1º A interpretação do negócio jurídico deve lhe atribuir o sentido que:
I - for confirmado pelo comportamento das partes posterior à celebração do negócio;
II - corresponder aos usos, costumes e práticas do mercado relativas ao tipo de negócio;
III - corresponder à boa-fé;
IV - for mais benéfico à parte que não redigiu o dispositivo, se identificável; e
V - corresponder a qual seria a razoável negociação das partes sobre a questão discutida, inferida das demais disposições do negócio e da racionalidade econômica das partes, consideradas as informações disponíveis no momento de sua celebração.
§ 2º As partes poderão livremente pactuar regras de interpretação, de preenchimento de lacunas e de integração dos negócios jurídicos diversas daquelas previstas em lei.

Por fim, a função limitadora ou de controle (art. 187 do CC[297]) impõe que o exercício de determinado direito subjetivo deve ser balizado pela própria boa-fé. Aplicando-se ao presente trabalho, seria possível associar tal função ao dever de os provedores de aplicação não acessarem mais dados pessoais do que aqueles estritamente necessários para os legítimos fins pretendidos. É necessário ressaltar que, ao passo que a probidade envolve a justiça, o equilíbrio e a comutatividade das prestações, a boa-fé exige a transparência, a honestidade e a clareza das cláusulas.

O equilíbrio contratual, por sua vez, chama atenção para outro princípio basilar das relações contratuais: o da equivalência das prestações[298]. Com efeito, referido princípio indica a necessidade de que o contrato realmente seja voltado à sua essência – um congresso de vontades com vistas à formação de um negócio jurídico –, e não a funcionar como um mecanismo de institucionalização da exploração do homem pelo homem. Nesse diapasão, tal princípio impõe a inexistência de vantagens excessivas de uma parte em detrimento da outra, sob pena de, a longo prazo, inexistir vontade de celebrar outros contratos – afinal, ninguém negociaria sabendo, de antemão, que iria *perder*[299].

A priori, parece haver respeito à equivalência das prestações em termos de privacidade de aplicativos móveis, na medida em que os provedores de aplicação disponibilizam funcionalidade realmente útil à facilitação da vida cotidiana, ao passo que, com maior ou menor transparência, coletam os dados pessoais para gerarem renda por meio de publicidade comportamental.

Contudo, quando se coloca o tratamento de dados em contexto, sobretudo à luz de que há uma espécie de *trade-off* diferido – na medida em que os aplicativos deterão os dados pessoais durante muito tempo e o usuário poderá perder de perspectiva a real contraprestação que ofereceu pelo uso da aplicação –, também não parece subsistir uma adequada equivalência de prestações no atual modelo de negócios, de tratamento massivo dos dados pessoais dos usuários.

Por último – mas não menos relevante –, também importante tecer breves comentários sobre o princípio da relatividade dos efeitos contratuais (*res inter alios acta, aliis neque nocet neque prodest*). Como sugerido pelo próprio nome, tal princípio estabelece que as consequências decorrentes do contrato só atingem aqueles que participam da relação contratual,

---

[297] Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
[298] RIZZARDO, Arnaldo. Contratos. 16. ed. Rio de Janeiro: Forense, 2017.
[299] Ibidem.

não prejudicando ou beneficiando terceiros alheios. Trata-se da mera decorrência lógica de que apenas podem ser vinculados aos efeitos da vontade manifestada aqueles que efetivamente a manifestaram. Seria, aliás, curioso que a regra geral admitisse os efeitos exógenos[300].

Essa análise é particularmente relevante no que tange ao fato de que quase todos os aplicativos analisados informam ter acesso aos dados de terceiros existentes nos celulares de seus usuários. Com efeito, as aplicações acessam dados de perfil, dados telefônicos e outros pelo mero fato de o terceiro ser um *contato* ou *amigo de rede social* do usuário da aplicação. A discussão central é saber até que ponto esse tipo de acesso é legítimo, na medida em que o consentimento não foi dado pelo *detentor* da privacidade em questão. O ponto é avaliado no decorrer do trabalho.

Passado o panorama geral sobre direito contratual, viu-se que os termos de privacidade ou de uso de aplicativos móveis constituem verdadeiros contratos. Isso traz a necessidade de se discutir, de maneira breve, alguns aspectos principais da teoria consumerista, naturalmente sem qualquer pretensão de esgotá-la.

Tal apresentação é fundamental, uma vez que, por força do art. 7º, XIII, do MCI[301], aplicam-se as normas de defesa do consumidor às relações de consumo realizadas pela internet. A mesma intelecção é extraída do art. 2º, V, do MCI[302], e do art. 2º, VI[303], da LGPD, que colocam a defesa do consumidor como fundamento da proteção de dados pessoais e do uso da internet no Brasil. Por essa razão, é essa breve exposição que se passa a fazer nesta seção.

Inicialmente, cumpre frisar que a Constituição Federal elenca a tutela do consumidor como um direito fundamental (art. 5º, XXXII[304]), submetido à competência legislativa concorrente[305] – ou seja, um interesse público tão relevante a ponto de ser tutelado pelos dois níveis de entes federados mais centrais –, e como um princípio fundante da ordem

---

[300] É claro, contudo, que existem algumas exceções legais, dentre as quais a mais relevante à presente análise é a posição do CDC de prever a existência de um consumidor por equiparação ou *bystander*.

[301] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

[302] Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como: (...) V - a livre iniciativa, a livre concorrência e a defesa do consumidor.

[303] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: (...) VI - a livre iniciativa, a livre concorrência e a defesa do consumidor.

[304] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor.

[305] Art. 24. Compete à União, aos Estados e ao Distrito Federal legislar concorrentemente sobre: (...)
V - produção e consumo; (...)
VIII - responsabilidade por dano ao meio ambiente, ao consumidor, a bens e direitos de valor artístico, estético, histórico, turístico e paisagístico.

econômica (art. 170, V[306]). Trata-se, uma vez mais, da preocupação com a promoção de verdadeira igualdade substantiva, na medida em que, tradicionalmente, o consumidor está em posição fragilizada na relação de consumo.

E, inclusive por força legal (art. 1º do CDC[307]), a defesa do consumidor consiste em norma de ordem pública – aplicação cogente, *ex officio* – e de interesse social, ou seja, é admitida a eventual intervenção do Ministério Público. As principais definições, de consumidor e fornecedor, estão na própria legislação e são relevantes para a presente análise[308].

A relação de consumo é, portanto, o elo entre o consumidor e o fornecedor (elementos subjetivos da relação de consumo), um interessado em haver para si bem ou serviço (elementos objetivos da relação de consumo) e o outro, a remuneração por isso. O consumidor é o destinatário final (elemento teleológico da relação de consumo) do bem ou serviço, ou seja, o destinatário fático vulnerável. Por sua vez, o fornecedor é aquele que promove determinada atividade de natureza econômica de modo habitual[309].

Partindo-se desses conceitos, parece relativamente fácil classificar a relação entre usuário de aplicativo e o provedor da própria aplicação como uma relação de consumo. Afinal: (i) o usuário é consumidor, na medida em que é destinatário fático do produto (bem imaterial que é o *software*) e vulnerável frente à provedora de aplicações; (ii) o provedor de aplicações é fornecedor, na medida em que sua provedoria tem natureza econômica – afinal, os aplicativos auferem renda com a utilização de seu *software*[310], embora o *download* seja, em geral, fraqueado gratuitamente – e supre o requisito da habitualidade –, é a atividade profissional da empresa, na medida em que seu produto está constantemente disponível para novos *downloads*;

---

[306] Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: (...) V - defesa do consumidor.

[307] Art. 1° O presente código estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos arts. 5°, inciso XXXII, 170, inciso V, da Constituição Federal e art. 48 de suas Disposições Transitórias.

[308] Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.

Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo.

Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.

§ 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.

§ 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

[309] NUNES, Rizzatto Curso de direito do consumidor. 12. ed. São Paulo: Saraiva Educação, 2018.

[310] TARTUCE, Flávio. Manual de direito do consumidor: direito material e processual. 7. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018.

e (iii) o aplicativo é verdadeiro produto, em sua acepção de bem imaterial, pois se trata de um *software*. Essa também é a posição adotada pelo STJ[311].

De modo ainda mais específico, é também fora de dúvida que os contratos firmados entre o provedor do aplicativo e o seu usuário são típicos contratos de adesão[312]. Por conceito, um contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo (art. 54 do CDC[313])[314].

Nesse tipo de contrato, as cláusulas que implicarem limitação de direito do consumidor deverão ser redigidas com destaque, permitindo sua imediata e fácil compreensão (trata-se do dever de transparência informativa material, a ser tratado em seção posterior). O que se pode adiantar é que, em tese, diversas das cláusulas dispostas nas políticas de privacidade dos aplicativos deveriam ganhar destaque, na medida em que são, em sua maioria, restritivas aos direitos do consumidor.

Poder-se-ia pensar, por exemplo, na utilização dos quadros-resumo previstos para os contratos de loteamento e de incorporação imobiliária (Lei nº 13.786/2018). Ou, para ser ainda mais interativo e explicativo, na disponibilização de curtos vídeos ou imagens fazendo referência aos principais pontos da política de privacidade, para que qualquer usuário pudesse

---

311 Veja-se, a título meramente exemplificativo: "A exploração comercial da internet sujeita as relações de consumo daí advindas à Lei nº 8.078/90. O fato de o serviço prestado pelo provedor de serviço de internet ser gratuito não desvirtua a relação de consumo, pois o termo mediante remuneração, contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor". BRASIL. Superior Tribunal de Justiça, REsp nº 1.308.830/RS, Rel. Min. Nancy Andrighi, DJe 19/06/2012.

312 Técnica de formação contratual se tornou necessária em virtude da massificação das relações negociais no ambiente capitalista, para o atingimento de maior eficiência econômica. *In*: ZANINI, Leonardo Estevam de Assis. Contratação na sociedade massificada. Revista Brasileira de Direito Civil – RBDCivil | Belo Horizonte, vol. 14, p. 75-98, out./dez. 2017, p. 76.

313 Art. 54. Contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo.
§ 1° A inserção de cláusula no formulário não desfigura a natureza de adesão do contrato.
§ 2° Nos contratos de adesão admite-se cláusula resolutória, desde que a alternativa, cabendo a escolha ao consumidor, ressalvando-se o disposto no § 2° do artigo anterior.
§ 3º Os contratos de adesão escritos serão redigidos em termos claros e com caracteres ostensivos e legíveis, cujo tamanho da fonte não será inferior ao corpo doze, de modo a facilitar sua compreensão pelo consumidor.
§ 4° As cláusulas que implicarem limitação de direito do consumidor deverão ser redigidas com destaque, permitindo sua imediata e fácil compreensão.

314 Um contrato é de adesão quando todas as cláusulas são predispostas por uma das partes, restando à outra apenas a possibilidade de aceitar ou recusar todas as condições impostas. E, mesmo que o consumidor/aderente insira alguma cláusula no formulário, não resta desfigurada a natureza adesiva do contrato (§ 1º). Esse conceito pode ser facilmente aplicado ao paradigma das políticas de privacidade, em que o usuário/consumidor até tem a possibilidade de marcar ou desmarcar algumas caixas pré-selecionadas – para o tratamento de alguns dados, por exemplo. Mas fato é que o cerne do objeto contratual ainda é de pura adesão.

entender sem gastar tanta energia nessa árdua tarefa[315]. Talvez, com essas duas mudanças, fosse possível cogitar de um consentimento mais informado.

Nesse contexto em que não há negociações preliminares e concordância estrita entre as partes, institui-se um mecanismo de obtenção de consentimento geral: exibir as condições antes da efetiva contratação, obrigando o consumidor a teoricamente lê-las e ratificá-las, por assinatura ou mero *check* eletrônico. Essa simplificação do modo de consentir – comum nos contratos de adesão feitos pela internet – é chamada de *clickwrap agreements* ou *point and click agreements*. Essas licenças se submetem "à concordância do usuário do produto ou serviço, contendo cláusulas acerca da sua prestação, sendo assim denominadas, pois sua validade se baseia no ato de apertar o botão de aceitação"[316, 317].

Esta parece ser a regra no universo dos aplicativos móveis: fornecer ao usuário um excesso desnecessário, confuso e complexo de informações, para que ele, efetivamente, não tenha nenhum interesse ou potencial de ler e entender o que está lendo. Na complexa leitura dos termos, certamente muitos brasileiros se sentiriam verdadeiros *analfabetos funcionais*.

Nessa esteira, estima-se que a leitura das políticas de privacidade atuais de empresas mais conhecidas toma um tempo médio de 26 minutos de seus usuários[318], o que é desproporcional para a média nacional de leitura do brasileiro, de apenas 2,5 livros inteiros por ano[319]. Para a leitura das políticas de privacidade dos 20 aplicativos mais utilizados, estima-se o tempo gasto de 6h40min (média de 20 minutos de leitura), 58% mais longas do que em 2008[320]. Aliás, é justamente de 2008 famoso estudo americano que concluiu que o custo de

---

315 Em rápida pesquisa nas ferramentas de busca, não se achou nenhum vídeo confeccionado pelos provedores de aplicação explicando suas políticas de privacidade, em inglês ou português.

316 MARTINS, Guilherme Magalhães. Contratos Eletrônicos de Consumo. 3 ed. São Paulo: Atlas. 2016. No mesmo sentido: LORENZETTI, Ricardo L. Comércio Eletrônico. São Paulo: Editora Revista dos Tribunais. 2004.

317 Ou seja, os *clickwrap agreements* significam que o simples clique sobre o botão "aceito" ou o mero download do produto implicam a aceitação das condições gerais. Nesse sentido, a leitura das condições apresentadas em advertência pelos fornecedores ganha especial relevo para os consumidores, na medida em que significam a verdadeira aceitação de todas as cláusulas. Assim, é temerária a prática de simplesmente rolar toda a barra de termos e aceitar genericamente, sem lê-la. É claro que se pode discutir a real importância de todas as condições lá impostas – questionando-se se as cláusulas seriam excessivas, por exemplo, apenas com o intuito de dissuadir o consumidor de fazer a leitura integral –, mas o maior problema é quando sequer essa advertência básica é feita pelo fornecedor.

318 YAHOO FINANÇAS. Políticas de privacidade: aceitar sem ler é hábito comum entre os internautas. Disponível em: <https://br.financas.yahoo.com/noticias/pol%C3%ADticas-privacidade-aceitar-sem-ler-121900683.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMjCWlBlCge6yfMCtSRxC35HGpfh0cIdF4TZXCu1lw-LQXzcYMuZobDwPbgJPjkY7t5uThYjHVp-hxgJkb3C1a4wdzhVbjZFQ13_8-LL5sB7mb6oNy2-PqLcdNbTG31QYilkVSbg60b6F5YTPACln2Tr26wvXtW_JQjNF6tmdxkz>. Acesso em: 6 abr. 2021.

319 BRASIL. Empresa Brasileira de Comunicação. Brasil perde 4,6 milhões de leitores em quatro anos. Disponível em: <https://agenciabrasil.ebc.com.br/educacao/noticia/2020-09/brasil-perde-46-milhoes-de-leitores-em-quatro-anos#:~:text=O%20brasileiro%20l%C3%AA%2C%20em%20m%C3%A9dia,tamb%C3%A9m%20como%20o%20mais%20marcante>. Acesso em: 6 abr. 2021.

320 INTO THE MINDS. Reading privacy policies of the 20 most-used mobile apps takes 6h40. Disponível em:

oportunidade nacional para a leitura das políticas de privacidade dos sites mais usados era da ordem de $ 781 bilhões[321]. Certamente o custo seria muito maior hoje, em que as políticas se alongaram e as plataformas de acesso, em conexão e aplicação, à internet se massificaram.

Nesses termos, classificam-se os termos de privacidade de aplicativos móveis como verdadeiros contratos eletrônicos de adesão, que baseiam o seu consentimento na licença *point and click agreement*. E, justamente por serem contratos de adesão, ao passo que facilitam o trabalho dos fornecedores para a realização de negócios em massa, acabam permitindo a inserção de eventuais cláusulas abusivas, que certamente passarão despercebidas pelo usuário – que, como se viu, sequer lê os enormes termos de privacidade.

Nesse diapasão, uma prática é considerada abusiva quando está em desconformidade com a boa-fé a ser dispensada ao consumidor e com os padrões do mercado, sendo geralmente proveniente do próprio abuso de direito. O CDC prevê, em seus arts. 39 e 51, um rol exemplificativo de práticas abusivas, situações em que claramente se abusa da boa-fé do consumidor e de sua vulnerabilidade para impor-lhe restrições indevidas[322].

Nenhuma das situações elencadas em tais dispositivos se aplica especificamente ao caso da presente análise, mas é possível fazer relação lateral entre algumas delas: (i) vedação à obtenção de vantagem manifestamente excessiva pelo fornecedor – dados pessoais do usuário em detrimento do fornecimento do *software*, que, determinadas vezes, sequer é tão relevante ao usuário –; (ii) vedação à publicidade enganosa – na medida em que os *softwares* costumam ser pouco transparentes –; (iii) vedação à alteração unilateral das cláusulas – é frequente receber uma notificação no sentido de que os termos de privacidade foram atualizados –; e (iv) vedação à transferência da responsabilidade para terceiros – é comum que os provedores de aplicações transfiram a responsabilidade pelo tratamento de dados a suas empresas parceiras comerciais.

Exemplo recente de atualização da política de privacidade é o caso do *WhatsApp*, que repercutiu na imprensa[323]. As mudanças, que permitiriam o compartilhamento mais amplo das atividades empreendidas no aplicativo com o *Facebook*, que é seu controlador e parceiro comercial, entrariam em vigor no início de fevereiro de 2021, mas, como a repercussão negativa

---

<https://www.intotheminds.com/blog/en/reading-privacy-policies-of-the-20-most-used-mobile-apps-takes-6h40/>. Acesso em: 6 abr. 2021.

[321] MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. I/S: A JOURNAL OF LAW AND POLICY. Vol. 4:3, pp. 543-568, 2008.

[322] BENJAMIN. Antônio Herman de Vasconcellos e. Capítulo V – Das Práticas Comerciais. In: GRINOVER, Ada Pellegrini et al. Código de Defesa Brasileiro do Consumidor: comentado pelos autores do anteprojeto. 10 ed. Rio de Janeiro: Forense. 2011. v.1. p. 259-510.

[323] GLOBO. WhatsApp muda política de privacidade e compartilha dados com o Facebook. Disponível em: <https://www.techtudo.com.br/noticias/2021/01/whatsapp-muda-politica-de-privacidade-e-compartilha-dados-com-o-facebook.ghtml>. Acesso em: 6 abr. 2021.

foi tanta, adiou-se a vigência para meados de maio. Durante esse lapso, em tese, o aplicativo investiu em dar publicidade às mudanças, inclusive por meio dos pequenos vídeos sugeridos no âmbito da ferramenta (os *status* do *WhatsApp*)[324].

Essa constante modificação das cláusulas das políticas de privacidade podem acabar frustrando as expectativas iniciais dos usuários, o que torna o consentimento ainda menos relevante em concreto. O *WhatsApp*, afinal, ganhou muitos usuários por supostamente proteger muito bem a sua privacidade; mas, logo no futuro, firmou parceria negocial com *Facebook*, que não tem o mesmo retrospecto positivo. Trata-se quase de uma erosão das políticas de privacidade e das legítimas expectativas dos usuários[325].

Tal fato apenas corrobora tudo o que foi afirmado até o momento, na medida em que não houve qualquer modificação na política de privacidade nesse lapso – subsistiu a unilateralidade. Ou seja, mesmo quando há *comoção social* ampla entre os usuários dos aplicativos, o máximo que esses consumidores conseguem é o adiamento da vigência seguido de explicações um pouco mais claras sobre o que está mudando. Sem a *comoção*, segue-se o padrão de não haver informações claras e de as mudanças serem rápidas.

E a não aceitação das mudanças também segue tendo o mesmo destino de sempre: o impedimento da utilização do aplicativo. Os órgãos de defesa do consumidor se imiscuíram na discussão específica, mas a probabilidade de que algo concreto em benefício efetivo dos usuários seja atingido é baixa. No entanto, um alerta fica às empresas que não valorizam muito a boa tutela dos dados pessoais e da privacidade: os concorrentes do *WhatsApp* tiveram um grande crescimento no número de usuários após a pretensão de mudança nas políticas de privacidade, o que indica que o usuário está começando a se atentar à importância dos dados pessoais[326].

Por todo o exposto, partindo-se do pressuposto de que existe uma relação de consumo entre usuário de aplicativo e o seu provedor (desenvolvedor que disponibiliza para *download*), é necessário tecer alguns comentários sintéticos acerca dos princípios que balizam as relações de consumo. É o que se passa a fazer.

---

[324] GLOBO. WhatsApp terá novo alerta sobre mudanças na política de privacidade no app. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/18/whatsapp-tera-novo-alerta-sobre-mudancas-na-politica-de-privacidade-no-app.ghtml>. Acesso em: 6 abr. 2021.

[325] OPSAHL, Kurt. Facebook's Eroding Privacy Policy: a timeline. Disponível em: <https://www.eff.org/deeplinks/2010/04/facebook-timeline>. Acesso em: 6 abr. 2021.

[326] TUDO CELULAR. WhatsApp recua frente aos protestos e adia mudança na política de privacidade. Disponível em: <https://www.tudocelular.com/seguranca/noticias/n169019/ministerio-justica-whatsapp-termo-privacidade.html>. Acesso em: 6 abr. 2021.

Com efeito, o art. 4º do CDC[327] estabelece alguns dos princípios aplicáveis à relação de consumo – em rol exemplificativo –, dos quais alguns são: respeito à dignidade humana, vulnerabilidade do consumidor (art. 4º, I), hipossuficiência do consumidor (art. 6º, VIII[328]), boa-fé objetiva (art. 4º, III), transparência ou confiança (art. 4º e art. 6º, III), função social do contrato, e reparação integral do dano (art. 6º, VI).

De modo geral, a dignidade humana aplicada ao âmbito do direito consumerista implica verdadeira necessidade de promoção da igualdade material, na medida em que a pessoa deve ser colocada em posição de centralidade no ordenamento jurídico, o que implica limites ao Estado e aos demais particulares e lhes impõe a necessidade de políticas, públicas e privadas, positivas.

In casu, a dignidade humana acaba ratificando o próprio paradigma do protecionismo do consumidor, na medida em que as normas consumeristas são de interesse social e ordem pública e que, processualmente, as cláusulas contratuais devem ser interpretadas de modo mais favorável ao consumidor (art. 47, CDC[329]).

Como decorrência da própria dignidade humana, o princípio da vulnerabilidade do consumidor se preocupa com o fato de que, por consequências naturais do liberalismo, a relação entre consumidor e fornecedor não é mais discutida em patamar de igualdade, de modo que o poder de barganha existente em relações negociais passa a ser meramente residual.

Trata-se, portanto, de uma posição *standard* de reconhecimento da condição jurídica vulnerável do consumidor, ante a massificação dos contratos: contudo, nada impede que ela seja afastada no caso concreto, a depender das provas produzidas nos autos. Dessa

---

[327] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo; (...)
III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;

[328] Art. 6º São direitos básicos do consumidor: (...)
II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações;
III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; (...)
VI - a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos; (...)
VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências.

[329] Art. 47. As cláusulas contratuais serão interpretadas de maneira mais favorável ao consumidor.

forma, fala-se que a vulnerabilidade é um elemento posto da relação de consumo, e não um elemento pressuposto (que é a própria condição de consumidor)[330].

Por sua vez, o princípio da hipossuficiência do consumidor pressupõe um conceito fático, efetivamente constatado em uma discrepância no caso concreto. Assim, por conceito, todo consumidor é vulnerável, mas nem todo consumidor é hipossuficiente. Regra geral, a hipossuficiência é atinente a aspectos processuais que pretendem garantir ao consumidor um acesso menos dificultoso à Justiça, como a inversão do ônus probatório em juízo – ante a dificuldade do consumidor, por quaisquer aspectos, de realizar prova no processo civil.

Dentro da órbita consumerista, a boa-fé objetiva também apresenta as três funções básicas já discutidas: criadora (servir como fonte de novos deveres especiais de conduta, os deveres anexos); limitadora (evitar exercício abusivo de direitos subjetivos); e interpretadora (paradigma de concreção e interpretação dos contratos).

Essa exigência de máximo respeito e colaboração entre as partes visa à manutenção do maior equilíbrio negocial. Um dos exemplos mais básicos de conduta alinhada à boa-fé é a exigência de prestação de informações completas, fidedignas e relevantes.

Com efeito, o princípio da transparência ou da confiança tutela justamente o dever de informar e o direito de ser informado em um mundo caraterizado pelo volume infinito de informações velozes. Nessa verdadeira sociedade de consumo de massa, as *armas de sedução* usadas pelos fornecedores para a atração de consumidores impõem um relevante déficit informacional.

Por próprio conceito legal, é um direito básico dos consumidores a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem. A jurisprudência do Superior Tribunal de Justiça também já se deteve sobre o tema[331].

---

[330] TARTUCE, Flávio. Manual de direito do consumidor: direito material e processual. 7. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018.

[331] Veja-se: "A exposição de motivos do Código de Defesa do Consumidor, sob esse ângulo, esclarece a razão de ser do direito à informação no sentido de que: 'O acesso dos consumidores a uma informação adequada que lhes permita fazer escolhas bem seguras conforme os desejos e necessidades de cada um' (Exposição de Motivos do Código de Defesa do Consumidor. Diário do Congresso Nacional, Seção II, 3 de maio de 1989, p. 1.663). (...). A informação ao consumidor, tem como escopo: 'i) consciencialização crítica dos desejos de consumo e da priorização das preferências que lhes digam respeito; ii) possibilitação de que sejam averiguados, de acordo com critérios técnicos e econômicos acessíveis ao leigo, as qualidades e o preço de cada produto ou de cada serviço; iii) criação e multiplicação de oportunidades para comparar os diversificados produtos; iv) conhecimento das posições jurídicas subjetivas próprias e alheias que se manifestam na contextualidade das séries infindáveis de situações de consumo; v) agilização e efetivação da presença estatal preventiva, mediadora, ou decisória, de conflitos do mercado de consumo' (Alcides Tomasetti Junior. O objetivo de transparência e o regime jurídico dos deveres e riscos de informação das declarações negociais para consumo, in *Revista de Direito do Consumidor*, n.

Legalmente, o tratamento não é diferente. Com efeito, o art. 46 do CDC[332] prevê que os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance. Ou seja, é estabelecido o requisito de existência de informações claras. Nesse ponto, é de se ressaltar que um dos direitos básicos do consumidor é o acesso à informação adequada e clara (art. 6º, III, CDC), além de necessárias a correção e a relevância dos dados informados.

Tutela-se, portanto, a informação em seu aspecto material, na medida em que o consumidor deve compreender o seu conteúdo. A preocupação aqui é com a percepção de que o excesso de informação não informa. Tal norma significa não apenas que o contrato deve assegurar o prévio conhecimento de informações relevantes pelo consumidor, mas que o próprio contrato tenha sido escrito de modo a ser entendido pelo consumidor[333]. Há relação estreita com a própria ideia de equivalência negocial, ainda que mínima.

Para além dessa verdadeira tutela das informações transparentes e da confiança, também emerge o princípio da função social do contrato, que guarda relação intrínseca com a manutenção do equilíbrio contratual, com sua equidade e com a plena possibilidade de revisão dos negócios jurídicos, protegendo o consumidor das abusividades do fornecedor, justamente por ausência de poder de barganha em razão dos contratos massificados

Por força legal, por exemplo, a onerosidade excessiva imposta ao consumidor, decorrente de fato superveniente, poderá implicar a revisão contratual, mesmo que o fato não seja imprevisível (art. 6º, V, do CDC[334]). Mas, de modo geral, ainda se deve tutelar o princípio da máxima utilidade dos contratos, com a sua consequente preservação.

Em relação ao direito à adequação das cláusulas por fatos supervenientes, é possível verificar clara relação entre referida disposição e a ideia de que os usuários de aplicativos estão submetidos a uma espécie de *trade-off* diferido ou continuado, na medida em que acabam

---

4, São Paulo: Revista dos Tribunais, número especial, 1992, pp. 52-90). (...). Deveras, é forçoso concluir que o direto à informação tem como desígnio promover completo esclarecimento quanto à escolha plenamente consciente do consumidor, de maneira a equilibrar a relação de vulnerabilidade do consumidor, colocando-o em posição de segurança na negociação de consumo, acerca dos dados relevantes para que a compra do produto ou serviço ofertado seja feita de maneira consciente". BRASIL. Superior Tribunal de Justiça, REsp nº 976.836/RS, Rel. Min. Luiz Fux, DJe 05/10/2010.

[332] Art. 46. Os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance.

[333] PEREIRA, Caio Mário Silva. Instituições de Direito Civil: Contratos. 20 ed. Rio de Janeiro: Forense, 2016. v.3.

[334] Art. 6º São direitos básicos do consumidor: (...) V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas.

fornecendo os dados pessoas hoje – e continuamente – em troca de utilização do serviço no presente; contudo, perde-se de vista a real possibilidade de aqueles dados tratados no presente serem usados no futuro, ainda que distante, *contra* o consumidor ou usuário. Essa utilização futura de dados presentes ou passados poderia, numa leitura ampla, ser enquadrada como um fato superveniente apto a implicar a modificação de eventuais cláusulas contratuais que permitiram o tratamento dos dados.

Por fim, o princípio da reparação integral de danos assegura que os consumidores sejam efetivamente prevenidos e reparados de quaisquer danos suportados. No caso do presente trabalho, é mais aplicável a tutela da personalidade, por meio da reparação por danos morais sofridos em razão do afastamento indevido do paradigma de proteção de dados pessoais. Mas, dado o contexto de tratamento amplo de dados pessoais, não é improvável que existam verdadeiros danos materiais ao usuário dos aplicativos: como exemplo, cita-se o case de um financiamento a juros mais altos em virtude de acesso a dados pessoais em aplicativos com abuso de confiança e fora dos padrões legais. Ou seja, pode haver uma profusão de danos.

Além disso, sabe-se que a tutela reparatória também pode alcançar direitos coletivos e difusos, caso se trate de interesses transindividuais, indivisíveis de grupos ligados por relação jurídica prévia ou pessoas indeterminadas ligadas por circunstância de fato, respectivamente (art. 81 do CDC[335]).

No âmbito do presente trabalho, é de se ver a possibilidade de tutela coletiva ganhou relevância, na medida em que se noticiou o fato de que o Ministério Público[336] e o Ministério da Justiça[337] abriram inquéritos administrativos internos para proceder à investigação e possível responsabilização do *Facebook* pelo grande vazamento de dados descoberto em meados de 2018[338].

---

[335] Art. 81. A defesa dos interesses e direitos dos consumidores e das vítimas poderá ser exercida em juízo individualmente, ou a título coletivo.
Parágrafo único. A defesa coletiva será exercida quando se tratar de:
I - interesses ou direitos difusos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível, de que sejam titulares pessoas indeterminadas e ligadas por circunstâncias de fato;
II - interesses ou direitos coletivos, assim entendidos, para efeitos deste código, os transindividuais, de natureza indivisível de que seja titular grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base;
III - interesses ou direitos individuais homogêneos, assim entendidos os decorrentes de origem comum.

[336] CONJUR. MP-DF vai investigar vazamento de dados do Facebook. Disponível em: <https://www.conjur.com.br/2018-out-01/mp-df-investigar-vazamento-dados-facebook>. Acesso em: 24 mar. 2021.

[337] FOLHA DE SÃO PAULO. Facebook vira alvo do Ministério da Justiça por vazamento de dados. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/03/facebook-vira-alvo-do-ministerio-da-justica-por-vazamento-de-dados.shtml>. Acesso em: 24 mar. 2021.

[338] No âmbito da tutela coletiva, é comum haver uma diferenciação conceitual entre danos morais coletivos e danos sociais ou difusos. Enquanto (i) aqueles atingem diversos direitos da personalidade, consistem em direitos individuais homogêneos ou coletivos de vítimas determinadas ou determináveis (coletivos *stricto sensu*) e a sua

Discorridos os modos mais clássicos de como lidar com a tutela dos dados pessoais e da privacidade – por mecanismos contratuais civis modernos ou do próprio âmbito do direito do consumidor –, é preciso admitir que seria viável pensar em uma tutela jurídica dos aspectos atinentes à privacidade e à proteção de dados pessoais dos usuários de aplicativos móveis mesmo antes da vigência do MCI ou da LGPD. É claro, contudo, como se viu, que as legislações específicas, bem como o forte desenvolvimento doutrinário no novo campo, criaram mecanismos mais diretos de aferição da validade do tratamento dos dados pessoais.

Feita essa discussão relevante, passa-se à análise empírica propriamente dita, que contará com os devidos aportes jurídicos específicos em cada caso necessário.

indenização é destinada para as próprias vítimas, (ii) estes causam um verdadeiro rebaixamento no nível de vida da coletividade, atingindo verdadeiros direitos difusos – toda a sociedade é vítima, sem possibilidade de singularização –, razão por que a sua indenização se volta para um fundo de proteção ou instituição de caridade. No caso concreto, a diferenciação é tênue, mas parece mais correto classificar a indevida invasão de privacidade de usuários de aplicativos móveis como tutela moral coletiva, na medida em que as vítimas podem ser determinadas – afinal, a aplicação tem conhecimento de quem são os seus usuários. Contudo, não se descarta que possa haver uma indenização para determinado fundo de proteção consumerista, na medida em que é relevante a aplicação da teoria dos *punitive damages* para que se dissuada as empresas de tecnologia de eventual atitude temerária de indevida invasão de privacidade de seus usuários. Mais detalhes em: TARTUCE, Flávio. Manual de direito do consumidor: direito material e processual. 7. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018.

3 PESQUISA EMPÍRICA

Para que a análise fosse mais efetiva – sobretudo para fins de comparação entre aplicativos semelhantes –, os *softwares* foram agrupados por cada segmento de utilidade abordado. Assim, categorizaram-se todos os aplicativos em ferramentas de: (i) comunicação e redes sociais; (ii) navegadores e e-mails; (iii) entretenimento, vídeos e músicas; (iv) comer e beber; (v) infantis e jogos; (vi) finanças e crédito; (vii) compras; (viii) notícias e revistas; (ix) turismo, locais, mapas e navegação; (x) educação; (xi) produtividade e antivírus; e (xii) governamentais. A ordem foi pensada com base em uma estimativa, de própria autoria, de aplicativos mais utilizados por um brasileiro médio.

E as categorias foram organizadas com base em classificação aproximada existente na própria loja de aplicativos da *Google*, ou seja, não foi utilizada como referência a loja da *Apple*, pelos motivos já expostos. Veja-se:

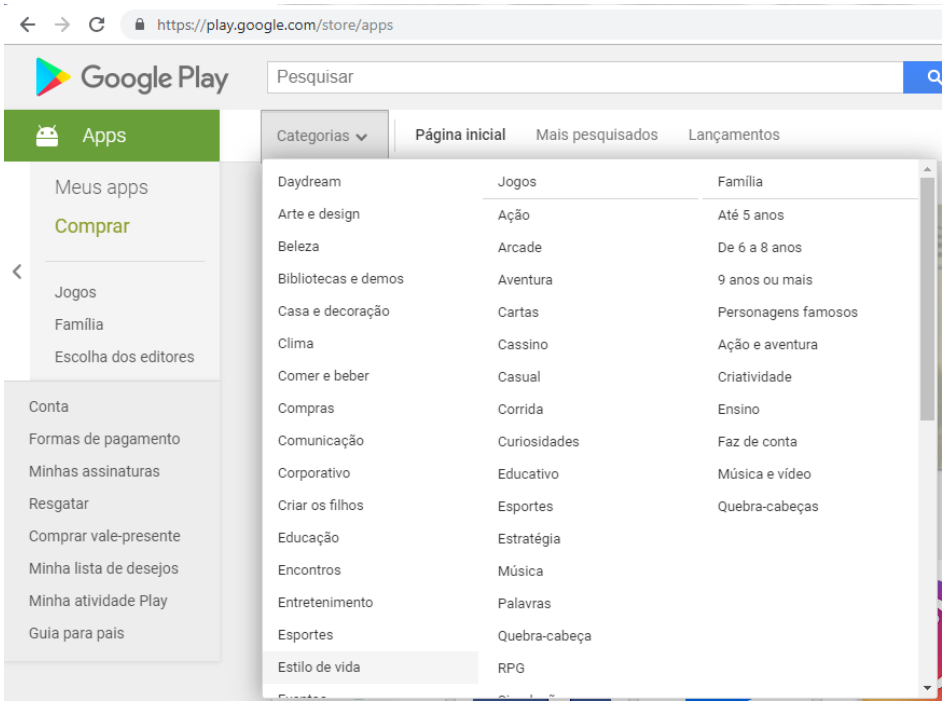

Figura 1 – Categorias aplicativos *Google Play*

Para cada desses segmentos – que parecem representar as ferramentas mais utilizadas do mercado –, foram selecionados os aplicativos com maior número de *downloads*,

de acordo com os próprios *rankings* da *Google*[339] e em diversas fontes jornalísticas[340,341,342]. Além disso, também se utilizou por base o relatório *State of Mobile 2021*, construído pela consultoria *App Annie*, respeitada no segmento[343].

Desse relatório, aliás, algumas conclusões são interessantes: o brasileiro gastou em média cerca de 4,8 horas diárias no seu celular em 2020, um aumento de 1 hora em relação a 2019; também vem se preocupando mais com aplicativos de finanças (mais *downloads* e mais horas gastas), embora ainda esteja abaixo da média mundial nos aplicativos de investimentos; incrementou muito seu uso de aplicativos de compras online, de *streaming* de vídeos, de aplicativos de comer e beber, de aplicativos de saúde e *fitness* e de aplicativos de reuniões de trabalho; a colocação de publicidade nos aplicativos aumentou 175% no Brasil de 2019 para 2020, principalmente no modo intersticial[344].

Procede-se, a partir de agora, à análise detalhada de cada segmento retro. Em síntese, a avaliação se dará por meio da investigação de um tripé: (i) o modo de obtenção do consentimento do usuário para o tratamento dos seus dados ou a disponibilização clara sobre as balizas do legítimo interesse; (ii) as permissões relevantes concedidas pelo usuário para a utilização do aplicativo, de modo a aferir o respeito ao princípio do mínimo privilégio no acesso; e (iii) os pontos mais relevantes da política de privacidade de cada aplicativo, aí sim com pretensões de tecer comentários das mais variadas espécies à luz do ordenamento jurídico afeto à proteção de dados.

Antes de se começar, vale colocar sob prisma o fato de que, segundo pesquisa da Universidade de Stanford, 97% dos usuários não leem os termos de privacidade e de uso dos aplicativos que estão instalando, ou seja, a regra é a do *não li, mas concordo ainda assim*[345]. Ou seja, o universo que virá é extremamente pantanoso.

---

339 GOOGLE. Plataforma *Google Play*. Disponível em: <https://play.google.com/store>. Acesso em: 26 mar. 2021.

340 OLHAR DIGITAL. WhatsApp é o app mais usado por brasileiros; veja ranking. Disponível em: <https://olhardigital.com.br/2020/12/21/noticias/whatsapp-e-o-app-mais-usado-por-brasileiros-veja-ranking/>. Acesso em: 7 abr. 2021.

341 CANALTECH. Os aplicativos mais baixados de 2020. Disponível em: <https://canaltech.com.br/apps/aplicativos-mais-baixados-2020-176201/>. Acesso em: 7 abr. 2021.

342 EXAME. Saiba quais foram os aplicativos mais baixados no Brasil e no mundo. Disponível em: <https://exame.com/tecnologia/saiba-quais-foram-os-aplicativos-mais-baixados-no-brasil-e-no-mundo/>. Acesso em: 7 abr. 2021.

343 APP ANNIE. State of mobile 2021. Disponível em: <https://f.hubspotusercontent20.net/hubfs/8885028/App%20Annie%20-The%20State%20Of%20Mobile%202021%20.pdf>. Acesso em: 7 abr. 2021.

344 "Os intersticiais são blocos de anúncios de página inteira veiculados entre as telas durante a navegação em apps para dispositivos móveis. Eles proporcionam aos usuários experiências em tela cheia nos pontos de transição naturais do app, como na inicialização, em anúncios precedentes em vídeo ou durante o carregamento de níveis". Disponível em: <https://support.google.com/admanager/answer/10320506?hl=pt-BR>. Acesso em: 7 abr. 2021.

345 SUPER INTERESSANTE. Não li e concordo. Disponível em: <https://super.abril.com.br/tecnologia/nao-li-e-

3.1 Modo de obtenção do consentimento do usuário e referências ao legítimo interesse

Antes de se passar à análise detida das cláusulas descritas nos termos de privacidade dos aplicativos e das permissões relevantes concedidas, é preciso voltar um passo. Com efeito, é necessário analisar como se deu o consentimento do usuário para que todas essas operações de tratamento pudessem ser feitas pelo provedor de aplicações. Ou, por outro lado, se há menções específicas ao fato de se utilizar do critério do legítimo interesse para o tratamento.

O consentimento, como já se viu, nada mais é do que o ajuste qualificado de vontades. Desde o CDC, com a percepção de que as relações sociais passariam a ser massificadas a ponto de ser necessário criar a figura da contratação por adesão, a vontade do aderente passou a ser tutelada com um pouco mais de rigidez pelo ordenamento jurídico nacional, sobretudo com a imposição de obrigações ao elaborador das cláusulas. Obrigações essas eminentemente adjetivas, no sentido de dar transparência e clareza ao consumidor, para que ele tivesse à mão todos os critérios relevantes para decidir pela contratação ou não.

No âmbito da internet, o MCI passou a qualificar essa vontade como *consentimento*, que deveria ser dado de forma livre, expressa, informada e para uma finalidade específica e pertinente à concessão da permissão. A LGPD seguiu a mesma linha, dando ao consentimento as adjetivações de ser livre, expresso, informado, inequívoco e também para uma finalidade determinada. A Lei estabelece mais algumas balizas, já dispostas nesse trabalho.

O ordenamento jurídico confere, pois, posição nuclear ao consentimento, na medida em que esse é visto como a base jurídica para o tratamento de dados pessoais. Embora haja os requisitos gerais de especificidade do consentimento e de que ele se dê por escrito, o exato *modo* de sua obtenção não é regulado em lei – sequer poderia, sob o risco de afastar integralmente a liberdade de iniciativa, em sua vertente de liberdade de conformação contratual.

Poder-se-ia cogitar, eventualmente, de uma espécie de contrato padronizado com requisitos mínimos, mas essa ainda não é a realidade brasileira –, o que dá margem à criação de formatos diversos, que garantem de modo melhor ou pior a decisão consciente e informada do usuário. Aliás, a própria LGPD remete à existência de cláusulas-padrão contratuais, mas somente no capítulo de transferência internacional de dados. Ou seja, eventual *exportação* do conceito para a padronização do modo de obtenção do consentimento não seria tão destoante

---

concordo/>. Acesso em: 13 abr. 2021.

assim. De toda forma, na inexistência, *a priori*, de um formato padronizado, é justamente essa divergência que se busca analisar.

Antes de entrar no mérito da avaliação da política de registro de consentimento de cada aplicativo, é importante registrar que os provedores de aplicações realmente veem no consentimento a materialização da *autodeterminação informativa* dos titulares dos dados. Ou seja, vê-se no consentimento uma forma de transferência integral da responsabilidade sobre com o que se concorda para os titulares das respectivas informações.

Um verdadeiro *disclaimer*[346], pois, partindo dessa premissa, os provedores de aplicações acabam explorando a posição vulnerável em que se encontra o usuário – e consumidor – do aplicativo, sob a ótica jurídica (não compreende a relevância do seu consentimento dentro daquele contrato), técnica (não compreende o que está sendo feito com seus dados), econômica (não tem poder de discutir as cláusulas contratuais, que são nitidamente de adesão) e informacional (submete-se unicamente às informações unilateralmente disponibilizadas pelo provedor, sem mecanismos de controle efetivo). Essas são algumas das razões pelas quais se fala na própria insuficiência do consentimento hoje em dia[347].

É sob esse enfoque que se passa à análise pormenorizada dos mecanismos de obtenção de consentimento. Uma crítica é válida desde já para todos os aplicativos avaliados e para a própria loja que disponibiliza os *softwares* ao usuário: durante o *download* pela loja de aplicativos *Google Play*, a política de privacidade de cada respectivo aplicativo só é exibida quando se procura pela opção "Contato do desenvolvedor", ao final da barra de rolagem no celular. Ou seja, o usuário precisa passar por todos os comentários sobre o aplicativo, abrir um menu pouco intuitivo (o "Contato do desenvolvedor"), para, dentre as opções ali dispostas, encontrar a espécie "Política de Privacidade"). O mais correto seria aparecer logo abaixo do próprio botão "Instalar", com destaque suficiente.

Por sua vez, as permissões concedidas ao *software* a ser instalado também só são conhecidas caso se procure especificamente por "Sobre este app", role a página até o final e, na última opção, clique em "Ver mais – permissões". Ou seja, falta transparência quando do momento inicial da adesão do consumidor/usuário ao contrato dos aplicativos. Seria mais alinhado às boas práticas de tutela da privacidade que as referidas informações fossem colocadas em posição de destaque, inclusive mediante aceite expresso e específico do usuário

[346] Termo aqui entendido como justificativa ou isenção de responsabilidade.
[347] BIONI, Bruno R. Autodeterminação informacional: Paradigmas inconclusos entre os direitos da personalidade, regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2016.

desde o *download*. Por mais que isso pudesse ser considerado *chato* e *pedante* para a maioria, seria essencial para o resguardo do consentimento informado e consciente do usuário.

Outra crítica a se fazer – aplicável a quase todos os aplicativos analisados, de modo geral – diz respeito à notoriedade dada à política de privacidade dentro da própria ferramenta. Como se sabe, a legislação exige que os contratos de adesão sejam escritos de modo ostensivo e legível, com tamanho razoável de fonte (corpo doze), o que facilitaria a compreensão pelo consumidor (art. 54, § 3º, do CDC). A própria LGPD estabelece a transparência como um dos princípios mais basilares para o tratamento de dados, com informações claras, precisas e facilmente acessíveis. Ora, se nem a política de privacidade o usuário consegue acessar facilmente, quanto mais exercer todos os seus direitos elencados na norma.

O que se vê, contudo, é que aqueles aplicativos que exibem sua política de privacidade logo na tela inicial optam pelo caminho de dar-lhes uma espécie de *transparência oculta*, ou seja, apesar de estarem ali logo na página inicial – o que, diga-se, embora um requisito legal, é aderente à tutela da privacidade que se entende como adequada, dado o contexto pernicioso a nível macro –, estão escritos em locais de difícil visualização: normalmente uma letra muito pequena, no canto da tela, com a letra em um contraste ruim com o próprio fundo da tela.

Nesse ponto, pensa-se que, como as políticas de privacidade são os verdadeiros contratos de adesão no ambiente digital hodierno, a sua transparência deveria ser mais efetiva. Essa é uma crítica aplicável a quase todos os aplicativos analisados, mas é verdade que alguns fazem o devido destaque aos contratos; contudo, opta-se desde já por ignorar esse aspecto para o restante da análise mais específica, por uma escolha pessoal. Antes de se começar a análise específica, é importante salientar que porções mais descritivas da análise estão dispostas no Apêndice A, para que o texto principal do presente trabalho fique mais enxuto.

Mas, desde logo, embora haja maior detalhamento no Apêndice A sobre os respectivos gráficos, cumpre exibir tabela e gráfico que resumem os resultados alcançados na análise empírica empreendida, que seguiu critérios principalmente baseados na transparência: exibição da política de privacidade no primeiro uso, na interface do aplicativo e em português, possibilidade de revogação do consentimento (em alguma medida, mesmo que mínima) e clareza quanto à possibilidade de compras nos aplicativos e à existência de anúncios nas plataformas. Os critérios foram propositadamente bastante objetivos, na medida em que a análise mais detalhada e subjetiva sobre a aderência das políticas de privacidade analisadas às normas brasileiras terá seu lugar na terceira parte da análise. Veja-se a tabela:

Tabela 1 – Resultados alcançados para cada grupo de aplicativos nos respectivos critérios

	Critério 1 Política de privacidade no primeiro uso	**Critério 2 Política de privacidade na interface do *app***	**Critério 3 Termos de uso e política de privacidade em português**	**Critério 4 Possibilidade de revogação do consentimento**	**Critério 5 Possibilidade de compras no aplicativo**	**Critério 6 Existência de anúncios na plataforma**	**Média pelos 4 primeiros critérios**
Grupo 1: Com. e Redes	93,75%	93,75%	82,35%	43,75%	29,41%	58,82%	**78,40%**
Grupo 2: Nav. e E-Mails	100,00%	100,00%	100,00%	83,33%	14,29%	57,14%	**95,83%**
Grupo 3: Entret., vídeos e músicas	47,37%	78,95%	60,00%	17,65%	50,00%	75,00%	**50,99%**
Grupo 4: Comer e Beber	28,57%	85,71%	100,00%	14,29%	0,00%	42,86%	**57,14%**
Grupo 5: Infantis e jogos	53,85%	53,85%	38,46%	15,38%	86,67%	53,33%	**40,38%**
Grupo 6: Finanças e crédito	53,33%	87,50%	61,54%	14,29%	6,67%	13,33%	**54,16%**
Grupo 7: Compras	40,00%	70,00%	60,00%	20,00%	0,00%	30,00%	**47,50%**
Grupo 8: Notícias e Revistas	38,46%	53,85%	66,67%	30,77%	46,15%	92,31%	**47,44%**
Grupo 9: Turismo e Mapas	42,86%	64,29%	78,57%	21,43%	7,14%	35,71%	**51,79%**
Grupo 10: Educação	33,33%	66,67%	33,33%	0,00%	33,33%	22,22%	**33,33%**
Grupo 11: Produtiv. e Antiv.	57,14%	78,57%	57,14%	50,00%	78,57%	57,14%	**60,71%**
Grupo 12: Govern.	12,50%	6,25%	100,00%	0,00%	0,00%	0,00%	**29,69%**
Média	**50,10%**	**69,95%**	**69,84%**	**25,91%**	**29,35%**	**44,82%**	**53,95%**

Dela, é possível extrair que não é francamente acessível ao usuário, em seu primeiro uso da aplicação, a respectiva política de privacidade (apenas 50,10%), sendo que os aplicativos governamentais, os de comer e beber e os de educação são particularmente negativos no aspecto. Mas, mesmo que não seja franqueado o acesso às *regras do jogo* logo no início dele – o que, *per se*, já é contrário à LGPD em seu foco de boa-fé –, a maioria dos aplicativos disponibiliza o acesso às políticas de privacidade dentro de sua interface (69,95%). A exceção aqui é o grupo dos aplicativos governamentais, em que, via de regra, as políticas de privacidade só são disponibilizadas no site da entidade pública.

Quanto ao critério de haver termos de uso em português, sustenta-se que essa é uma característica fundamental para a adequada tutela da proteção dos dados dos usuários no sentido do direito-dever de informação. Afinal, não é crível que usuários brasileiros tenham que ler políticas de privacidade em russo ou mandarim, tampouco em inglês. Se há disponibilização dos produtos no Brasil – e há –, o mínimo a se fazer era traduzir as políticas para o português, o que praticamente qualquer software online é capaz de proceder.

Nesse atributo, embora o resultado médio geral seja até razoável (69,84%), são negativas duas categorias de aplicativos mais frequentes em usuários infantis: jogos e educação. Tal constatação é ainda mais caricata da falta de respeito ao dever de transparência ativa, na medida em que a LGPD possui critérios até mais rigorosos sobre os termos quando o público majoritário da aplicação não é adulto.

Por sua vez, é na possibilidade de revogação do consentimento que os resultados são mais chamativos. Com uma média de apenas 25,91% de possibilidades revogatórias, em qualquer medida (uma simples não permissão para *cookies* foi contada como resultado positivo nessa análise), parece ser sintomático que os aplicativos não estão tutelando adequadamente o direito de o usuário efetivamente consentir ou não consentir com o tratamento de seus dados. Fosse um teste de escola, apenas a categoria de e-mails e navegadores conseguiria ser aprovada – e justamente porque há possibilidade de revogações dos simples *cookies* ou exibição de anúncios feitos com base em publicidade comportamental.

Outra conclusão possível dessa análise, mas que não se aferiu na prática – na medida em que os aplicativos tampouco são transparentes quanto a isso, embora haja imposição legal –, é no sentido de que os provedores não franqueiam a possibilidade de revogação de consentimento ou permissões pelo motivo de o tratamento de dados não ter, preponderantemente, essa base legal autorizativa. Os aplicativos governamentais, por exemplo, podem apostar a autorização no fazimento genérico de políticas públicas; os demais, no seu legítimo interesse. De toda forma, fato é que isso não fica claro quando do uso preambular de cada aplicação, embora, por dever de transparência, assim devesse.

Por fim, os dois últimos critérios (compras e anúncios) buscam aferir quão transparente é a própria relação dos aplicativos com a loja *Google Play*. Ora, embora seja inerente à funcionalidade, entende-se que aplicativos de *compras* e de *comer e beber* deveriam ratificar a possibilidade de haver como comprar em suas aplicações. Por mais que seja, como se disse, esperado, é necessário enfatizar isso, por dever de transparência. Por sua vez, o critério de informar sobre publicidade na plataforma indica que quase metade das ferramentas aposta, sim, na publicidade comportamental para seus usuários a partir dos dados coletados.

Dentro de todo esse panorama, e fazendo-se uma *média geral* dos principais critérios para essa primeira etapa da análise – os quatro primeiros –, é possível extrair uma *nota* de que 53,95% dos aplicativos são aderentes à LGPD nesses aspectos mais formais do primeiro uso das ferramentas. Os que puxaram a média para cima foram as redes sociais, os aplicativos de comunicação, os e-mails e os navegadores, que são justamente as empresas de maior porte, as *big techs*, que podem – e devem – investir mais em proteção de dados e respeito à privacidade. As demais categorias ficam dentro de um padrão de nota entre 40-60, à exceção dos governamentais (uma vez mais) e dos aplicativos educacionais, duas categorias que deveriam ter mais zelo pelos dados pessoais. Para além da tabela, e para facilitar o entendimento, é possível analisar o seguinte gráfico:

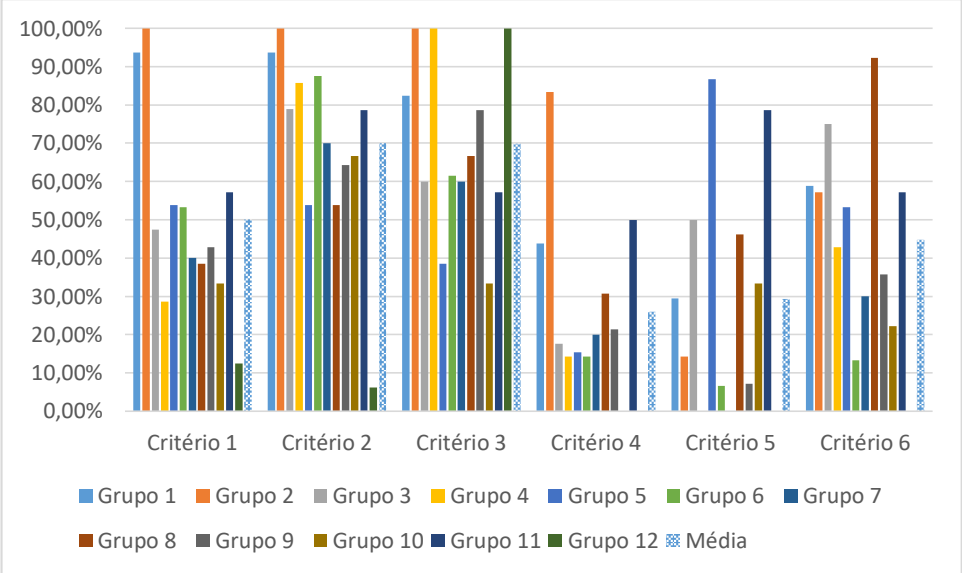

Figura 2 – Resultados alcançados para cada grupo de aplicativos nos respectivos critérios

Com isso, é mais fácil entender quem está tutelando de modo minimamente adequado os dados pessoais de seus usuários. Doravante, passa-se a fazer a análise mais específica de cada categoria, mas ainda enxuta, na medida em que maiores detalhamentos estão no Apêndice A.

3.1.1 Comunicação e redes sociais

Dentro dessa categoria, foram avaliados os aplicativos *WhatsApp*, *Facebook*, *Instagram*, *Viber*, *Twitter*, *Skype*, *Tinder*, *Tumblr*, *Snapchat*, *WeChat*, *Telegram*, *Messenger*, *LinkedIn*, *Pinterest*, *Zoom*, *Google Meet* e *Signal*. Nenhuma das ferramentas avaliadas exige

qualquer permissão prévia ao *download*. Dos dezessete aplicativos, cinco informam haver possibilidade de compras na ferramenta (*Messenger*, *WeChat*, *Tinder*, *Viber* e *Facebook*). Em sentido semelhante, dez deles informam haver anúncios na plataforma (à exceção de *WhatsApp*, *WeChat*, *Telegram*, *Zoom*, *Google Meet*, *Signal* e *Messenger*).

Ou seja, à exceção do *Viber*, percebe-se a clara tendência de os meros aplicativos de mensagens instantâneas não disporem de anúncios em suas plataformas. Além disso, a classificação indicativa é variável entre "Livre", "12 anos" (*LinkekIn*, *Pinterest*, *Messenger*, *Snapchat*, *Viber*, *Instagram* e *Facebook*) e "14 anos" (*Telegram*, *Tumblr*, *Twitter* e *Tinder*).

Em um primeiro momento, soa estranho que os aplicativos de mensagens instantâneas tenham classificação indicativa diferente (em três categorias), na medida em que oferecem produtos muito semelhantes e são concorrentes diretos. A única explicação para isso é a existência de alguma funcionalidade pouco intuitiva e, por consequência, desconhecida.

Quanto ao *Messenger*, na própria interface do aplicativo, é possível solicitar o *download* de um arquivo compilado com todas as informações que a rede social tem sobre o usuário, o que parece aderente ao princípio do livre acesso. O mesmo ocorre com o *Tumblr* e com o *Viber*. Quanto a este último, pode-se solicitar a exclusão dos dados pessoais armazenados, o que parece aderente ao direito de o titular requerer o apagamento de seus dados (o direito ao esquecimento do RGPD). Essas possibilidades certamente existem nos demais aplicativos, mas não são tão claras quanto nos aqui comentados.

O *WeChat*, por sua vez, aposta na metodologia de rolagem, logo no primeiro uso, da página dos termos de privacidade para posterior aceitação ao final, o que difere dos demais aplicativos analisados, que sequer essa metodologia de *leitura ficta* utilizam. Quanto ao *Instagram*, parece adequado que as permissões mais sensíveis (câmera, localização, gravação de áudio e acesso a arquivos) apenas sejam solicitadas em momento específico em que serão realmente úteis.

Há outros aplicativos que funcionam com essa mesma metodologia, mas o usuário precisa não concordar com todos os acessos requisitados pela aplicação logo no seu primeiro uso. Ou seja, se o usuário não der acesso a tudo logo no início de sua relação com o provedor – o que, imagina-se, não é o mais comum na realidade brasileira –, o aplicativo vai novamente solicitar as permissões quando efetivamente precisar delas para o *software* fluir. Isso indica que, ao solicitar tudo logo no início da operação, o aplicativo acaba cometendo um excesso no acesso aos dados pessoais, em aparente desrespeito à máxima no menor privilégio.

Por fim, o *WhatsApp* chama atenção por, aparentemente, não comportar qualquer revogação de consentimento quanto aos aspectos de privacidade. Diversos outros aplicativos

aqui analisados também não comportam revogações (*Zoom*, *Signal*, *Google Meet*, dentre outros), o que não parece aderente ao § 5º do art. 8º da LGPD.

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Essa prática está na contramão dos requisitos do consentimento expressos no art. 8º da LGPD. E, aliás, não há sequer que se mencionar suposta dificuldade de adequação à recente Lei, na medida em que o MCI já balizava a necessidade de consentimento expresso e inequívoco.

Nessa categoria, contudo, quase todos os aplicativos exibem as informações de privacidade logo no primeiro uso e na própria interface da aplicação, quase sempre em português, o que certamente torna menos difícil a compreensão do usuário. Analisar a política em si é a meta da terceira etapa dessa parte empírica: aqui, a busca é apenas pelos *formalismos* necessários. É de se frisar, contudo, que, como se passará a ver, esse contexto positivo está longe – muito longe – de ser a realidade do mercado.

Uma possível razão para que os aplicativos aqui analisados sejam mais transparentes nesse sentido caminha no sentido de que talvez as redes sociais tenham maior preocupação com a privacidade justamente por causa do recente escândalo envolvendo o *Facebook* e porque são realmente empresas muito grandes, que podem deslocar equipe de programadores exclusivamente à seção de *privacy policy*.

Chama atenção o fato de que menos do que a metade dos aplicativos permite revogações mais expressivas de consentimento, o que seria particularmente relevante na categoria, dada a capilaridade das redes sociais no atual mundo interativo e de hiperconexão. E esse fato é especialmente preocupante porque são as redes sociais que geralmente fazem o mapeamento do usuário para fins de posterior publicidade de *targeting* (publicidade "no alvo"), por todos os outros aplicativos e quaisquer fornecedores. Apesar de todas as críticas, é preciso ressaltar que, dentre os aplicativos aqui analisados, e sob a ótica do respeito aos necessários formalismos para a adequada proteção de dados, apenas *Twitter* e *Viber* passariam num eventual teste de conformidade com as expectativas.

3.1.2 Navegadores e e-mails

Dentro dessa categoria, foram avaliados os aplicativos *Google Chrome*, *UC Browser*, *Mozilla Firefox*, *MS Edge*, *Gmail*, *Outlook* e *Yahoo*. Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Dos sete aplicativos, um informa haver

possibilidade de compras na ferramenta (*Yahoo*). Em sentido semelhante, quatro deles informam haver anúncios na plataforma (*Yahoo, Outlook, UC Browser* e *Gmail*).

Na contramão disso, todos são de classificação indicativa "Livre", ou seja, crianças teoricamente podem usar – e aqui ainda é mais peculiar, na medida em que crianças sequer podem fazer operações financeiras, já que são absolutamente incapazes. Nesse ponto, parece que a classificação indicativa deveria guardar maior verossimilhança com a realidade.

De modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Essa prática, como já se enunciou, é contrária às normas da LGPD ou mesmo do MCI.

Nessa categoria, contudo, todos os aplicativos exibem as informações de privacidade logo no primeiro uso e na própria interface da aplicação, sempre em português, o que certamente torna menos difícil a compreensão do usuário. Nessa categoria, os aplicativos que pareceram tutelar mais adequadamente os aspectos formais do consentimento foram o *Gmail* e o *MS Edge*.

3.1.3 Entretenimento, vídeos e músicas

Dentro dessa categoria, foram avaliados os aplicativos *Netflix, SBT, Band, GShow, RecordTV, Now Net e Claro, YouTube, YouTube Kids, TikTok, Vigo, Shazam, Palco MP3, Spotify, Google Music, Globoplay, Twitch, Disney+, Likee, Amazon Prime* e *Deezer*. Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Dos vinte aplicativos, dez informam haver possibilidade de compras na ferramenta (*Deezer, Spotify, Vigo, TikTok, Globoplay, Twitch, Disney+, Likee, Amazon Prime* e *Netflix*).

Em sentido semelhante, doze deles informam haver anúncios na plataforma (à exceção de *Shazam, Now Net e Claro, Disney+, Likee* e *Netflix*). Além disso, a classificação indicativa é variável entre "Livre", "12 anos" (*Twitch, Likee, Spotify, Vigo* e *TikTok*), "14 anos" (*Deezer, Google Music, Palco MP3* e *Shazam*) e "16 anos" (*Netflix, Amazon Prime, Disney+* e *Globoplay*).

No *Deezer*, a transparência chama a atenção, na medida em que o aplicativo tenta realmente explicar o porquê das concessões. O *Spotify* também permite que o usuário baixe um arquivo consolidado com todos os dados de que a plataforma dispõe sobre ele, o que permite um maior *accountability* pelo usuário. Essas duas características, especialmente a de explicar com clareza o motivo das concessões requeridas, encampa o espírito da LGPD.

O *Shazam* permite a utilização sem que seja criada uma conta, ou seja, *a priori*, não é feito o *targeting* do usuário que navega sem *login* na plataforma, o que é positivo pelo cenário de que quase todos os demais aplicativos dessa categoria exigem o cadastro para o acesso. No *TikTok*, há termos de privacidade específicos para usuários que residem na União Europeia, em razão de o regime de proteção de dados ser mais apertado lá.

O *YouTube Kids*, por sua vez, apresenta ferramentas interessantes de controle parental dos acessos da criança, inclusive no tocante ao tratamento, como exige a LGPD. Contudo, isso era exatamente o esperado por uma plataforma que se diz inteiramente voltada ao público infantil. Ainda na tela inicial, é exibida uma espécie de resumo dos termos de privacidade (que são mostrados em formato mais analítico quando do menu específico de configurações, em português), cuja leitura é muito mais fácil e intuitiva do que de todos os demais aplicativos analisados, o que coaduna com o § 6º do art. 14 da LGPD.

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Essa prática está na contramão do consentimento expresso legalmente exigido.

Nesse sentido, a minoria dos aplicativos exibe os termos de privacidade e de uso quando da abertura da tela inicial. Chama negativamente a atenção o fato de que apenas três dos aplicativos avaliados possibilita a revogação de consentimento, ao passo que a maioria informa haver anúncios e opções de compra nas plataformas respectivas. Quanto à revogação, a baixa adesão a esse direito é particularmente sintomática de que algo não vem funcionando bem no *enforcement* da LGPD, sobretudo em uma categoria com aplicativos consolidados e com muitos usuários, ou seja, que poderiam investir energia na garantia desse direito.

E também não foi encontrada, ao menos *prima facie*, qualquer menção ao tratamento de dados tendo por base o legítimo interesse – o que, em tese, afastaria a possibilidade de revogação do consentimento. Ou seja, o resultado parece ruim. Mas, de toda forma, nessa categoria, o *Spotify* parece ser o aplicativo que mais se preocupa com a tutela da privacidade de acordo com as balizas da LGPD.

3.1.4 Comer e beber

Dentro dessa categoria, foram avaliados os aplicativos *Ifood*, *Rappi*, *Uber Eats*, *Zé Delivery*, *McDonalds*, *Tudo Gostoso* e *Foursquare*. Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Dos sete aplicativos, nenhum informa haver

possibilidade de compras na ferramenta – apesar de essa ser a própria funcionalidade principal dos *softwares* em questão, pensa-se que o primado da transparência orientaria no sentido de que, ainda assim, todos os aplicativos deveriam informar esse dado.

Do contrário, passa-se uma conotação de que a categorização feita pela *Google Play* não é confiável nesse ponto, o que pode ser ruim se se pensar que algum usuário pode resolver utilizar apenas aplicações que não tenham possibilidade de compra – a exemplo de um pai querendo instalar aplicativos para o filho, mas com a pretensão de garantir que a criança não fará inúmeras compras no software[348].

Na sequência, três deles informam haver anúncios na plataforma (*Rappi*, *Tudo Gostoso* e *Foursquare*). Além disso, a maioria afirma ser de classificação indicativa "Livre" (à exceção de *Foursquare*, que é recomendado para maiores de 12 anos), ou seja, crianças teoricamente podem usar, o que novamente não faz sentido, na medida em que as crianças não deveriam poder fazer as compras pelos aplicativos.

O *Foursquare* ainda é interessante por prever permissão para que o aplicativo veicule anúncios de segmentação comportamental fora da própria plataforma. A postura da empresa – embora seja uma configuração *opt-out*, ao passo que o mais correto seria a *opt-in* – parece aderente à tutela da privacidade que se entende como adequada.

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Nesse sentido, a minoria dos aplicativos exibe os termos de privacidade e de uso quando da abertura da tela inicial, o que também é temerário pela própria capilaridade desses aplicativos.

Chama negativamente a atenção o fato de que apenas um dos aplicativos avaliados possibilita a revogação de consentimento, ao passo que quase a metade informa haver anúncios e opções de compra nas plataformas respectivas. Mas, de toda forma, nessa categoria, o *Foursquare* parece ser o aplicativo que mais se preocupa com a tutela da privacidade.

3.1.5 Infantis e jogos

Dentro dessa categoria, foram avaliados os aplicativos *Garena*, *Subway Surfers*, *Meu Talking Tom 2*, *Pou*, *Fifa*, *Angry Birds*, *Candy Crush*, *Demo Minecraft*, *Minecraft*,

[348] UOL. Criança gasta mais de R$30 mil com jogos no celular durante pandemia sem o pai saber. Disponível em: <https://paisefilhos.uol.com.br/familia/crianca-gasta-mais-de-r30-mil-com-jogos-no-celular-durante-pandemia-sem-o-pai-saber/>. Acesso em: 7 abr. 2021.

Pokémon Go, *Fruit Ninja*, *GTA*, *Paint Pop 3D*, *Buddy Toss* e *Hopping Ball*. Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*.

Dos quinze aplicativos, treze informam haver possibilidade de compras na ferramenta (à exceção de *Demo Minecraft e Minecraft*). Em sentido semelhante, oito deles informam haver anúncios na plataforma (*Subway Surfers*, *Meu Talking Tom 2*, *Pou*, *Angry Birds*, *Fruit Ninja*, *Paint Pop 3D*, *Buddy Toss* e *Hopping Ball*).

Na contramão disso, quase todos são de classificação indicativa "Livre" (à exceção de *Garena* e *GTA*, que são indicados para maiores de 12 e 18 anos, respectivamente), ou seja, crianças teoricamente podem usar, sendo submetidas a perniciosas publicidades infantis e ainda podendo fazer compras no próprio aplicativo, sem que exista exatamente uma etapa de validação da compra pelos pais – e, se existir, não é de fácil fiscalização, na medida em que a criança pode muito bem colocar os dados do cartão de crédito de seu responsável. Nesse aspecto, parece haver violação às regras insertas no art. 14 da LGPD.

Embora se debata, de longa data, a preocupação com a exposição infantil a propagandas voltadas a si, os aplicativos móveis parecem ter criado um novo paradigma para a discussão, na medida em que os impactos dos anúncios ali existentes podem ser muito mais imediatos e subliminares do que em outros contextos. Os anúncios são exibidos de diferentes maneiras: desde *banners* nas extremidades da tela, até vídeos cuja função seja de conceder benefícios ao usuário – moedas, desbloqueio de fases e opções restritas, etc.

Além desse contexto de publicidade, o problema de compras dentro do aplicativo também não é novo. O modo como os termos de privacidade de cada aplicativo tratam o tema é avaliado em tópico apartado, mas é relevante frisar que, atentas à possibilidade de responsabilização civil por eventuais danos causados, as principais lojas de *download* dos aplicativos – *iTunes*[349] e *Google Play*[350] – instituíram ferramentas para dificultar a opção de compra exclusivamente feita pela criança. Ainda há algumas arestas sobre como o controle é feito – conta na loja, conta no celular, etc. –, mas essa discussão também foge do tema central do presente trabalho.

Quanto ao *Subway Surfers*, é de se dizer que, antes da entrada em vigor da LGPD, o acesso ao jogo era condicionado à aceitação dessas cláusulas. No menu de configurações, até era possível acessar os mesmos termos e revogar o consentimento anterior de modo amplo.

---

[349] APPLE. *Solicitar e fazer compras com o "Pedir para comprar"*. Disponível em: <https://support.apple.com/pt-br/HT201089>. Acesso em: 17 mar. 2021.

[350] GOOGLE. *Exigir senha ou autenticação para compras*. Disponível em: <https://support.google.com/googleplay/answer/1626831>. Acesso em: 17 mar. 2021.

Contudo, a revogação do consentimento implicava o não funcionamento do jogo. Veja-se a seguinte imagem:

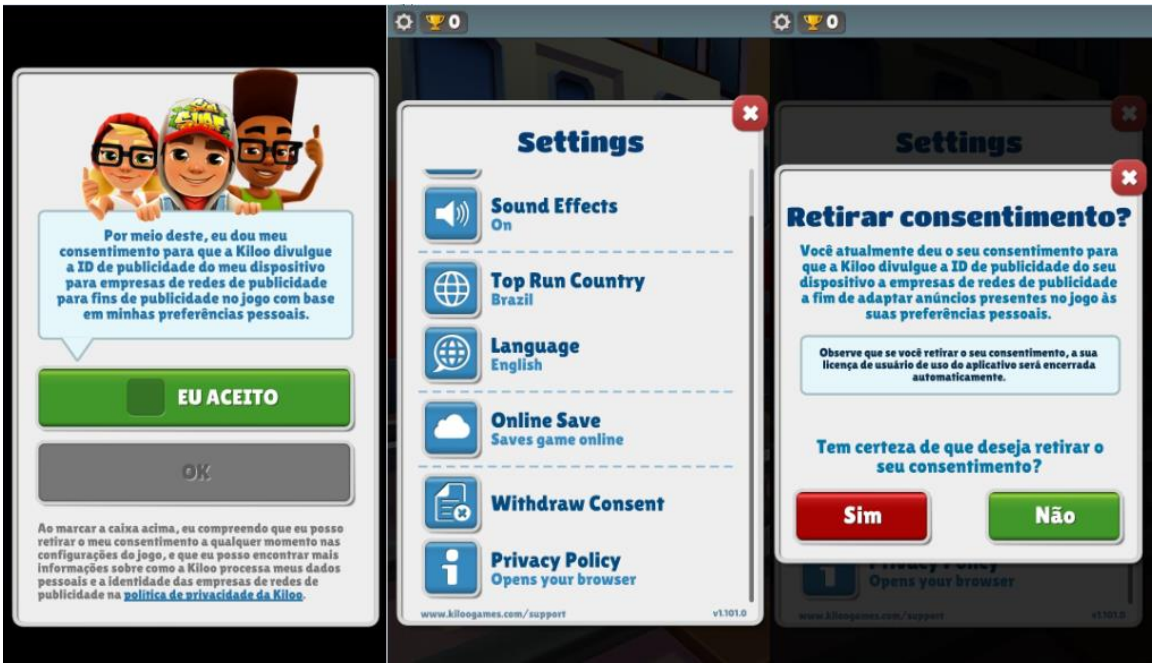

Figura 3 – Tela de revogação de consentimento aplicativo *Subway Surfers*

A postura da desenvolvedora do aplicativo não parecia aderente à tutela da privacidade que se entende como adequada: ou você consentia inteiramente com a publicidade comportamental – sem possibilidade de revogação específica –, ou não tinha acesso ao jogo. Com a entrada em vigor da LGPD, o trato do tema mudou ligeiramente: agora, ao não consentir com a coleta dos dados para o *profiling*, o usuário pode continuar com a aplicação em funcionamento, mas é informado de que a publicidade no aplicativo poderá perder a eficácia dos interesses mais próximos do usuário.

Ou seja, a pessoa que gosta de carros passaria a ver anúncio de bolsas. Entende-se que essa nova abordagem feita pela provedora é razoável e compatível com a LGPD, pois o desenvolvedor tenta legitimamente convencer o usuário a dar os seus dados – para ter anúncios mais personalizados. Se houver consentimento, bem; do contrário, o usuário que *arque* com a utilização não personalizada do jogo. Parece justo para os dois lados da relação.

O *Garena* exibe uma "descrição de acesso", para a qual, apesar da transparência explicativa, a única opção é aceitar. O aplicativo também pede permissão expressa de "acesso às fotos, mídia e arquivos do dispositivo", de "fazimento e gerenciamento de chamadas telefônicas" e de "gravação de áudio", sendo todos os pedidos vinculados.

O *Meu Talking Tom 2* tem política de privacidade aparentemente aplicável a todos os aplicativos desenvolvidos pela empresa responsável, ou seja, não atende ao requisito da especificidade. O *Buddy Toss*, o *Hopping Ball* e o *Paint Pop 3D* parecem alinhados ao conceito de níveis de aplicativos, na medida em que indicam uma versão paga como supostamente a solução para evitar a enxurrada de anúncios nas plataformas.

Contudo, como não há qualquer referência à política de privacidade, não é possível aferir se esse pagamento impediria a coleta de dados e, por consequência, todo o ciclo produtivo da publicidade comportamental, ou se consistiria apenas em um filtro da última etapa – a exibição do anúncio direcionado. Sendo esta a opção, parece se tratar dos casos de aplicativos *freemium* já comentados, que não fazem real diferenciação do funcionamento entre versões paga e gratuita.

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Apesar de a ligeira maioria dos aplicativos exibir os termos de privacidade e de uso quando da abertura da tela inicial, a minoria é em português, o que certamente dificulta a compreensão do usuário.

Chama negativamente a atenção o fato de que apenas dois dos aplicativos avaliados possibilitam a revogação de consentimento, ao passo que a maioria informa haver anúncios e opções de compra nas plataformas respectivas. Além disso, no que toca aos aspectos formais dessa etapa inicial da coleta dos dados, não parece haver muito respeito às balizas postas no art. 14 da LGPD.

Como os jogos são, em maioria, destinados ao público infanto-juvenil, é peculiar o fato de a publicidade comportamental não poder ser evitada, na medida em que as crianças são certamente mais suscetíveis às propagandas. Nessa categoria, o *Fifa* parece ser o aplicativo que mais se preocupa com a tutela da privacidade. Quanto aos aplicativos que disponibilizam uma versão paga, não é trivial descobrir se há minoração no tratamento ou só na publicidade no âmbito da plataforma, o que também denota falta de transparência nesse aspecto.

No que tange aos jogos, por fim, é interessante observar que, na Europa, há uma plataforma para que crianças e jovens entendam os seus direitos de proteção de dados pessoais e desenvolvam uma preocupação com o tema[351]. Parece não haver paralelo no Brasil, embora fosse extremamente recomendável que o assunto efetivamente ganhasse as escolas.

---

[351] EUROPA. Cyber Chronix, a game to understand data protection rights and raise awareness on privacy risks. Disponível em: <https://ec.europa.eu/jrc/en/research-topic/security-privacy-and-data-protection/cyber-chronix>.

3.1.6 Finanças e crédito

Dentro dessa categoria, foram avaliados os aplicativos *Banco do Brasil*, *Caixa*, *Itaú*, *Bradesco*, *Santander BR*, *Santander ESP*, *Santander UK*, *Nubank*, *Serasa Consumidor*, *Mercado Pago*, *Digio*, *PayPal*, *Banco Inter*, *PicPay* e *Investing*. Aqui, foram voluntariamente selecionados dois aplicativos de banco internacional – e também o seu respectivo aplicativo nacional –, justamente para fins de avaliar se há alguma diferença substancial entre as aplicações reguladas por normas internacionais e as brasileiras.

Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Na interface, o único que parece mais preocupado com a tutela dos dados é o *Serasa*, por exibir uma mensagem falando "fique tranquilo, seus dados estão seguros com a gente". Pode ser insuficiente para a adequação à LGPD, mas certamente é um passo que tranquiliza o consumidor. É a mesma ideia do *Itaú*, que vem investindo em campanhas publicitárias na televisão falando que "proteger seus dados não é brincadeira. O *Itaú* cuida da sua privacidade"[352]. É o simbolismo relevante, inclusive para chamar atenção para a discussão.

Dos quinze aplicativos, um informa haver possibilidade de compras na ferramenta (*Investing*). Em sentido semelhante, dois deles informam haver anúncios na plataforma (*Bradesco* e *Investing*). Nesse ponto, é peculiar que um aplicativo de instituição financeira – que claramente já aufere renda com seus serviços bancários – afirme promover anúncios em sua plataforma, o que normalmente envolve a publicidade comportamental. E, dada a sensibilidade dos dados de que o banco dispõe, isso ganha especial relevo.

Na contramão disso, todos são de classificação indicativa "Livre", ou seja, crianças teoricamente podem usar – e aqui ainda é mais peculiar, na medida em que crianças sequer podem fazer operações financeiras, já que são absolutamente incapazes. Nesse ponto, parece que a classificação indicativa deveria guardar maior verossimilhança com a realidade.

Antes de seguir, vale enfatizar que, nesta categoria, é possível que a análise do consentimento não seja tão conclusiva e enfática, na medida em que não pretendeu, no estudo, criar contas em todas as instituições financeiras aqui avaliadas – e, geralmente, sem essa etapa, é inviável a correta utilização do aplicativo.

Acesso em 4 jun. 2021.

[352] ITAÚ UNIBANCO. Privacidade – Autógrafo. Disponível em: <https://www.youtube.com/watch?v=c83z_su9Ty4&ab_channel=Ita%C3%BA>. Acesso em: 7 abr. 2021.

Mas dentre todas as observações, a que pareceu mais relevante se refere ao *Bradesco*, que, ao iniciar, solicita cinco permissões expressas: (i) acesso à localização do dispositivo; (ii) acesso a fotos, mídia e arquivos; (iii) permissão para o fazimento e gerenciamento de chamadas telefônicas; (iv) permissão para gravar áudio; e (v) permissão para tirar fotos e gravar vídeos. Em um primeiro momento, foi possível recusar todas. Ao clicar na opção seguinte de "abrir conta", entretanto, a ferramenta informa ser necessário conceder as permissões (ii), (iv) e (v) retro, de modo vinculado, o que não parece fazer tanto sentido.

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Além disso, quando da abertura da ferramenta, a minoria dos aplicativos exibe a política de privacidade e os termos de privacidade, e somente a minoria permite a revogação de qualquer permissão concedida. O aplicativo que parece ter possibilidades mais interessantes e completas de revogação é o *Banco do Brasil*.

3.1.7 Compras

Dentro dessa categoria, foram avaliados os aplicativos *Mercado Livre*, *Wish*, *OLX*, *Magazine Luiza*, *AliExpress*, *Amazon*, *Americanas*, *Shopee*, *Enjoei* e *Ebay*. Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Dos dez aplicativos, nenhum informa haver possibilidade de compras na ferramenta – apesar de essa ser a própria funcionalidade principal dos *softwares* em questão, pensa-se que o primado da transparência orientaria no sentido de que, ainda assim todos os aplicativos deveriam informar esse dado.

Na sequência, três deles informam haver anúncios na plataforma (*OLX*, *Amazon* e *Ebay*). Além disso, a maioria afirma ser de classificação indicativa "Livre" (à exceção de *Wish*, *AliExpress* e *Ebay*, que são recomendados para maiores de 14 anos), ou seja, crianças teoricamente podem usar.

O *OLX* requer permissão de acesso à localização do aparelho, para supostamente ficar mais fácil visualizar anúncios da região do usuário. Particularmente, não se entende como adequada essa justificativa para o acesso a informação tão sensível, na medida em que, durante a utilização da ferramenta, não é difícil fazer os filtros das localidades manualmente. Embora seja naturalmente possível revogar o consentimento para tal permissão, sustenta-se que ela sequer deveria ser pretendida pela aplicação. O *Amazon*, por sua vez, apresenta um menu

específico para explicar o funcionamento dos anúncios baseados em interesses, o que parece adequado ao dever de informação ativa balizado pela LGPD.

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro, o que contraria as boas práticas previstas na LGPD.

Noutro giro, é de se salientar que boa parte dos aplicativos só exibe a política de privacidade *no primeiro uso* se o usuário realmente tentar efetivar o cadastro na plataforma. Como muitas delas funcionam sem o cadastro para a navegação – só se exigiria para a formalização da compra em si –, o usuário pode não ter contato com a política de privacidade tão facilmente quanto se esperaria como adequado.

Além disso, somente a minoria permite a revogação de qualquer permissão concedida. O aplicativo que parece ter possibilidades mais interessantes e completas de revogação é o *Ebay*, embora elas, aparentemente, não sejam aplicáveis ao usuário brasileiro, talvez por a plataforma ter seu mercado mais destinado ao exterior. Dito isso, dentre todos os avaliados, o *Wish* parece guardar maior respeito à privacidade dos usuários, segundo os critérios estabelecidos até este ponto.

3.1.8 Notícias e revistas

Dentro dessa categoria, foram avaliados os aplicativos *G1*, *Folha de SP*, *UOL Notícias*, *El País*, *CNN*, *Fox News*, *NY Times*, *Le Figaro*, *Le Monde*, *BBC*, *Der Spiegel*, *The Guardian* e *Flipboard*. Aqui, foram voluntariamente selecionados diversos aplicativos de meios de comunicação internacionais, justamente para fins de avaliar se há alguma diferença substancial entre as aplicações reguladas por normas de proteção de dados internacionais e as brasileiras.

Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Dos treze aplicativos, seis informam haver possibilidade de compras na ferramenta (*Folha de SP*, *NY Times*, *Le Figaro*, *Le Monde*, *Der Spiegel* e *The Guardian*). Em sentido semelhante, doze deles informam haver anúncios na plataforma (à exceção do *Folha de SP*), o que é esperado, já que o jornalismo dito *gratuito* é fortemente baseado na publicidade comportamental dentro das plataformas para sua própria subsistência. Na contramão disso, todos são de classificação indicativa "Livre", ou seja, crianças teoricamente podem usar.

Dentro do menu de configurações do *CNN*, o aplicativo oferece uma opção específica de "*ad choices*" (escolhas de publicidade), com possibilidade de revogação específica da transmissão das informações pessoais para determinadas empresas. Veja-se a seguinte imagem:

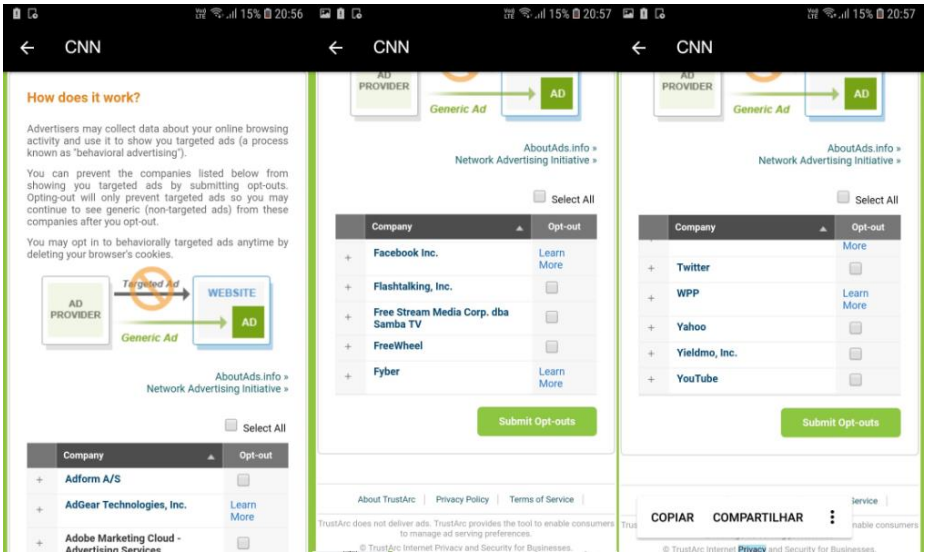

Figura 4 – Tela de revogação de consentimento aplicativo *CNN*

Essa possibilidade de revogação do consentimento para a publicidade comportamental feita por determinadas empresas especializadas no ramo é bastante específica e parece aderente à tutela da privacidade que se entende como adequada. Embora não seja simples retirar o consentimento em relação a todas as empresas, há muitas opções em que o mero *check* da caixa já gera o *opt-out*. Veja-se que, em verdade, o padrão da privacidade de dados indica que se trabalhe em um *software opt-in*, ou seja, uma plataforma em que o usuário expressamente conceda o consentimento expresso para o tratamento dos dados.

Contudo, essa está longe – muito longe – de ser a realidade do mercado, como se vê no presente trabalho. Assim, a iniciativa de possibilitar a remoção do consentimento em formato de *opt-out* tão específico parece aderente à tutela da privacidade que se entende como adequada e prevista na LGPD. É claro que a revogação não implica a inexistência de publicidade, mas, como indicado na própria foto, o anúncio será genérico, e não especificamente dirigido ao usuário, à semelhança do que ocorre no jogo *Subway Surfers* já comentado. Diante da realidade do mercado, tal possibilidade é razoável.

Após a marcação da submissão da opção de *opt-out*, o aplicativo exibe a informação de que "a empresa coloca um *cookie* no navegador para indicar que o usuário deseja desativar

a publicidade personalizada ao veicular anúncios nas páginas visitadas". É possível que isso indique que o aplicativo, em verdade, continua coletando e transmitindo os dados, sendo que o bloqueio se dá apenas na exibição da propaganda, ou seja, seria um filtro na última etapa do processo. Sendo o bloqueio apenas para a exibição da publicidade comportamental no site específico, parece não ter tanta diferença entre aceitar ou rejeitar as caixinhas da imagem.

O *Fox News* segue exatamente o mesmo padrão do *CNN*, inclusive com a possibilidade de retirar o consentimento da publicidade comportamental de todas as empresas responsáveis por isso. Trata-se, como o aplicativo prevê, de uma posição de deferência à "Digital Advertising Alliance (DAA)[353], que estabelece e aplica práticas de privacidade responsáveis em toda a indústria para publicidade digital relevante, proporcionando aos consumidores maior transparência e controle através de Princípios multifacetados que se aplicam a Dados Multi-Site e Dados entre Aplicativos reunidos em ambientes de *desktop* ou móveis".

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Além disso, quando da abertura da ferramenta, a minoria dos aplicativos exibe a política de privacidade e os termos de privacidade, e ainda menor parte permite a revogação de qualquer permissão concedida.

No que tange à revogação, aliás, os aplicativos *CNN* e *Fox News* pareceram alinhados ao requisito de consentimento do usuário para ser viável o tratamento de dados, nem que seja por meio da disponibilização da opção *opt-out*, ao passo que o mais adequado seria a *opt-in* – o que parece distante do atual mercado. Dito isso, dentre todos os avaliados, o *Fox News* parece guardar maior respeito à privacidade dos usuários, segundo os critérios estabelecidos até este ponto.

3.1.9 Turismo, locais, mapas e navegação

Dentro dessa categoria, foram avaliados os aplicativos *Uber*, *99*, *Cabify*, *Google Maps*, *Maps.ME*, *Waze*, *Trivago*, *Decolar*, *Booking*, *TripAdvisor*, *Airbnb*, *Skyscanner*, *Google Street View* e *Google Earth*. Nenhuma das ferramentas avaliadas exige qualquer permissão

[353] DIGITAL ADVERTISING ALLIANCE. Disponível em: <https://digitaladvertisingalliance.org/>. Acesso em: 7 abr. 2021.

prévia ao *download*. Dos catorze aplicativos, apenas um informa haver possibilidade de compras na ferramenta (*Maps.ME*).

Em sentido semelhante, cinco deles informam haver anúncios na plataforma (*Maps.ME, TripAdvisor, Skyscanner, Waze* e *Google Maps*). Na contramão disso, todos são de classificação indicativa "Livre", ou seja, crianças teoricamente podem usar.

Ao iniciar, o *Cabify* indica que continuar significa "aceitar os termos, a política de dados e o uso de cookies do *Facebook* e a política de privacidade e os termos de serviço do Cabify". Nesse caso, parece haver uma perniciosa *venda casada* dos aplicativos, o que é peculiar. Afinal, não necessariamente o usuário de aplicativos de transporte está seguro em fornecer seus dados pessoais ao *Facebook*, sendo que o contexto em que aqueles dados foram coletados foi o de um simples transporte privado.

Não é demais afirmar que os deslocamentos do cidadão são uma informação relevante – embora não seja sensível para os fins da LGPD –, já que demonstra o perfil de locomoção e de interação social daquele usuário. Supondo que o usuário se utilize do aplicativo de locomoção para ir a encontros íntimos, talvez até extraconjugais, é pernicioso que o *Facebook* tenha acesso a esse tipo de informação[354].

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Além disso, quando da abertura da ferramenta, a minoria dos aplicativos exibe a política de privacidade e os termos de privacidade, e ainda menor parte permite a revogação de qualquer permissão concedida. Dentre todos os aplicativos avaliados, o *Skyscanner* parece guardar maior respeito à privacidade dos usuários, segundo os critérios estabelecidos até este ponto.

3.1.10 Educação

Dentro dessa categoria, foram avaliados os aplicativos *Duolingo, Brainly, Babbel, TED, Khan Academy, Khan Academy Kids, Google Classroom, Kahoot!* e *Google Tradutor*. Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Dos nove aplicativos, três informam haver possibilidade de compras na ferramenta (*Duolingo, Babbel* e *Kahoot!*). Em sentido semelhante, dois deles informam haver anúncios na plataforma (*Duolingo* e *TED*). Na contramão disso, todos são de classificação indicativa "Livre", ou seja, crianças

[354] E aqui sem qualquer juízo de valor acerca do exemplo, que apenas pretendeu ser caricato da situação.

teoricamente podem usar. Nesse caso, faz sentido, na medida em que os aplicativos analisados realmente podem ser muito úteis para o público infantil.

Assim, de modo geral, é possível notar que quase todos os aplicativos avaliados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Quando da abertura da ferramenta, contudo, a maioria dos aplicativos exibe a política de privacidade e os termos de privacidade, mas nenhum permite a revogação de qualquer permissão concedida. Isso parece particularmente infringente aos direitos dos usuários, especialmente pelo contexto de que esses aplicativos contêm acessos amplos (câmera, microfone, contatos, arquivos, etc.), como se verá na próxima seção do trabalho.

Dentre todos, não parece haver nenhuma vantagem notória de qualquer dos aplicativos no que tange à etapa de aferição do consentimento do usuário. Ao revés, fosse um teste escolar – à semelhança da sua alegada finalidade dentro da categoria –, é provável que todos reprovassem ou, no mínimo, ficassem de recuperação. Mas, dentre todos, aquele que pareceu mais alinhado a essa etapa formal da aferição dos requisitos para o tratamento foi o *Babbel*.

3.1.11 Produtividade e antivírus

Dentro dessa categoria, foram avaliados os aplicativos *MS Word*, *Polaris Office*, *WPS Office*, *Google Docs*, *Google Drive*, *4Shared*, *Share It*, *Adobe Reader*, *Dropbox*, *Clean Master*, *Avast*, *AVG*, *Kaspersky* e *McAfee*. Nenhuma das ferramentas avaliadas exige qualquer permissão prévia ao *download*. Dos catorze aplicativos, onze informam haver possibilidade de compras na ferramenta (exceções ao *Google Docs*, *4Shared* e *Share It*). Em sentido semelhante, oito deles informam haver anúncios na plataforma (exceções ao *MS Word*, *Google Docs*, *Google Drive*, *Dropbox*, *Adobe Reader* e *Kaspersky*). Na contramão disso, todos são de classificação indicativa "Livre".

No *Kaspersky*, há o aviso de que, ao prosseguir, o usuário concorda com a política de privacidade e os termos de serviço, cujos links remetem a materiais escritos em português. Há, contudo, uma situação curiosa: se o aplicativo for usado na União Europeia, há mecanismo específico de consentimento. Pela relevância do tema, veja-se a comparação:

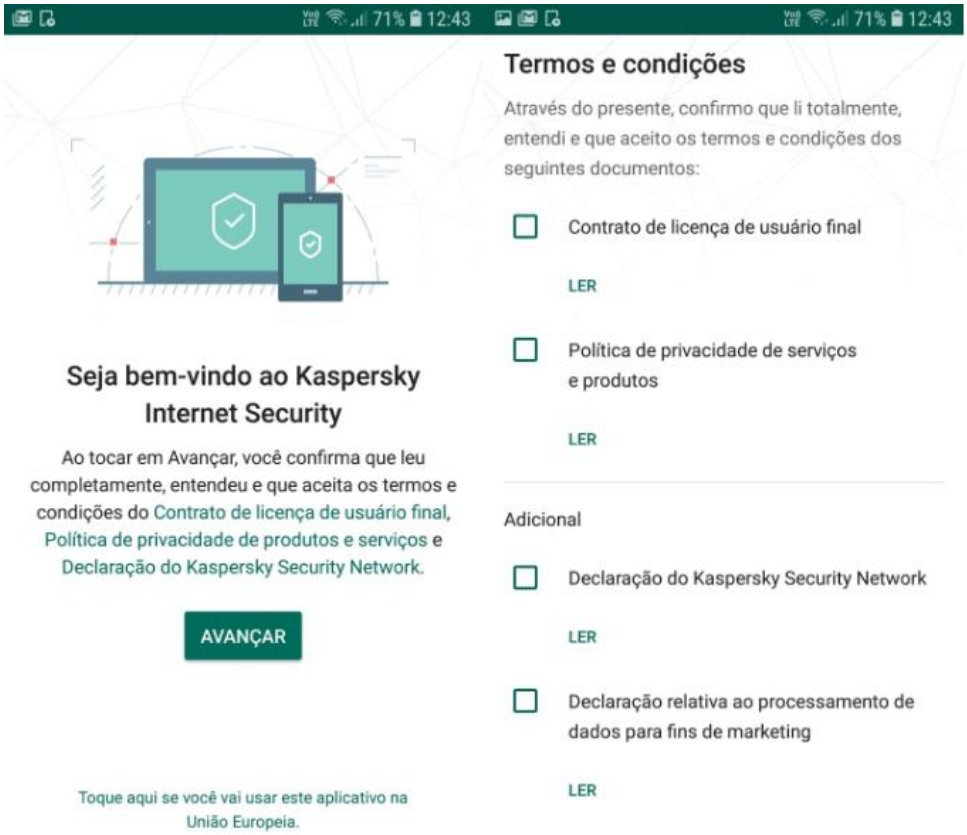

Figura 5 – Comparação entre o consentimento nas versões europeia e brasileira do aplicativo *Kaspersky*

A tela à esquerda é a padronizada para os aplicativos nacionais que mais prezam pela privacidade, isto é, nem todos exibem a tela de concordância com os termos de privacidade e com a política de privacidade. A tela à direita exibe a tela de consentimento alinhada ao RGPD, ou seja, mais expresso e, teoricamente, informado.

Mesmo que não haja muita diferença prática no resultado, o caminho percorrido para a obtenção do consentimento é diferente. E, aqui, parece que a obrigação de meio é realmente a mais importante: o caminho de transparência é muito útil para que haja um tratamento válido dos dados pessoais, seja ele baseado no legítimo interesse ou no consentimento do usuário. Essa é a interpretação mais alinhada à boa-fé objetiva.

Uma vez mais, a posição do *software* parece aderente à tutela da privacidade que se entende como adequada. Nas configurações, há como fazer revogações pontuais de concessões prévias. Mesmo na versão gratuita, não há previsão de exibição de anúncios na plataforma, o que parece aderente à tutela da privacidade que se entende como adequada.

Assim, de modo geral, é possível notar que quase todos os aplicativos analisados optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro.

Quando da abertura da ferramenta, contudo, a maioria dos aplicativos exibe a política de privacidade e os termos de privacidade, também permitindo revogações pontuais de permissões concedidas. Dentre todos, o aplicativo *Kaspersky* foi o que mais demonstrou preocupações com essa etapa mais formal de aferição do consentimento dos usuários.

3.1.12 Governamentais

A priori, a Administração Pública deveria unicamente visar ao interesse público, com a finalidade de garantia dos direitos fundamentais e de respeito aos princípios básicos da legalidade, impessoalidade, moralidade, publicidade e eficiência (art. 37 da CRFB/88[355]). Isso deveria afastar qualquer pretensão de alargamento indevido do consentimento ou do legítimo interesse como bases jurídicas para o tratamento indiscriminado de dados pessoais pelo Estado, que já não deveria mais ser policialesco. Esse panorama é também retratado na LGPD[356].

Assim, o consentimento obtido ou a informação de legítimo interesse em aplicativos governamentais devem ser analisados sob duplo foco: de um lado, a Administração tem o ônus majorado de garantir controle efetivo dos dados pessoais aos seus titulares; de outro, isso não pode inviabilizar a própria eficiência na prestação dos serviços públicos.

Em verdade, é de se dizer que a Administração sequer precisaria recorrer a essas duas hipóteses legais de autorização para o tratamento dos dados pessoais, na medida em que dispõe de uma autorização legal específica: aquela para a execução de políticas públicas previstas em lei, regulamentos, contratos, convênios ou afins (inciso II do art. 7º da LGPD). Ou seja, deve haver o atingimento da finalidade pública.

---

[355] Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: (...).

[356] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; e

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Mas, ainda assim, é requisito que sejam fornecidas informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para o tratamento dos dados, com facilidade de acesso pelo usuário (art. 23, I, da LGPD).

Ainda se fala que as empresas públicas e as sociedades de economia mista que atuam no regime concorrencial, a mercado, devem ser submetidas às mesmas regras gerais da LGPD. Esse é o caso, por exemplo, dos aplicativos analisados do *Banco do Brasil* e da *Caixa Econômica Federal*, que operam no livre mercado. Contudo, quando essas pessoas jurídicas de direito privado estiverem operacionalizando políticas públicas – pagamento do auxílio emergencial, informações sobre empregos ou sobre o direitos trabalhistas, por exemplo –, devem se submeter às regras específicas do tratamento de dados no bojo da Administração (art. 24 da LGPD).

De modo geral, o panorama normativo da LGPD é permitir o compartilhamento de dados na Administração apenas no âmbito de finalidades específicas à execução de políticas públicas ou prestação de serviços públicos, desde que respeitados todos os princípios gerais da proteção de dados.

É também relevante a observação de que o Poder Público não pode transferir a entidades privadas informações pessoais de que dispõe, saldo se se tratar de execução descentralizada das políticas públicas, ou, dentre outras hipóteses restritivas, se a informação for acessível publicamente (art. 26 da LGPD).

Nesse ponto, parece que a LGPD acabou indo além do que pretendia, pois, lida em sua literalidade, essa disposição permitiria que a Administração compartilhasse os rendimentos de servidores públicos com instituições financeiras, por exemplo, já que essas informações são públicas na internet. Esse comportamento claramente seria uma violação da expectativa do titular do dado, sob o foco da privacidade contextual, na medida em que não sabia que seus dados de rendimentos seriam facilmente entregues às instituições financeiras, por exemplo.

E, colocando ainda mais em contexto, parece que o art. 27 da LGPD dispensa, nesse caso, sequer a necessidade de consentimento do titular do dado ou a comunicação à ANPD para que haja esse compartilhamento da Administração com pessoa jurídica de direito privado. Sustenta-se, entretanto, que a observância dos princípios da LGPD deve permear mesmo esse capítulo com regras mais concretas, sobretudo para que se respeitem os mínimos critérios de transparência, finalidade, necessidade (menor privilégio), adequação e privacidade contextual.

Salientados os aspectos mais relevantes da legislação acerca do tratamento de dados no bojo da Administração Pública, é de se afirmar que, dentro dessa categoria, foram avaliados os aplicativos *FGTS*, *Sisu*, *Caixa Trabalhador*, *Caixa Auxílio Emergencial*, *Coronavírus – SUS*,

Meu Imposto, *Bolsa Família*, *e-Título*, *CNH Digital*, *DigiSUS*, *Sine*, *Caesb*, *CEB*, *Novacap*, *Denatran* e *Meu INSS*. Esses foram os aplicativos considerados mais relevantes para o cidadão brasileiro – em especial para aqueles que moram no Distrito Federal –, na medida em que estão diretamente relacionados a serviços cotidianos na relação Estado-cidadão.

Da análise mais formal dessa primeira interface dos aplicativos, observou-se a necessidade de que os aplicativos do governo passem a investir em iniciativas mais robustas de garantia de controle efetivo de usuários e usuárias sobre suas informações. Isso contempla diversas ações: o desenvolvimento de aplicativos com uma preocupação com privacidade e segurança da informação desde a concepção (*privacy by design*); a redução da coleta e do uso de dados pessoais ao mínimo necessário para o funcionamento do aplicativo; e a educação de usuários e usuárias sobre tecnologias que envolvem fluxo de dados. Fazendo isso, a Administração Pública estará atuando alinhada com o interesse público.

Assim, de modo geral, foi possível notar que quase todos os aplicativos governamentais optam pelo consentimento implícito – por ter baixado o programa e estar usando, pressupõe-se que o usuário tenha concordado com os termos e políticas do desenvolvedor, em âmbito macro. Essa prática está na contramão do consentimento expresso, exigido pela LGPD e pelo próprio MCI, um requisito ainda mais essencial quando se trata de aplicativos governamentais, na medida em que o Estado deve observar o princípio da transparência e de ainda menor acesso aos dados pessoais de seus administrados, sob pena de se voltar a um Estado policialesco.

Quanto ao *Coronavírus – SUS*, é interessante observar que, logo em sua primeira tela de funcionamento, exibe a mensagem "Sua privacidade está segura", o que é complementado com as informações de que o aplicativo não coleta dados do perfil, não consegue determinar a identidade do usuário ou de com quem entrou em contato, não coleta dados de geolocalização (não há rastreamento), os dados são criptografados, os dados são mantidos no Brasil e excluídos até o final de 2020 (o que não faz sentido, dada a utilização em 2021).

Após ver essa tela, o usuário precisa dar um *check* no sentido de ter lido a política de privacidade para continuar. Na tela seguinte, o aplicativo pede acesso à localização do celular e ao seu *bluetooth*, para supostamente registrar contatos com outros usuários, mas é possível não habilitar essa "notificação de exposição". Esse modelo de operação do aplicativo parece adequado às normas da LGPD, na medida em que se aposta no consentimento do usuário para lhe oferecer um serviço de interesse – rastreamento do vírus.

Quanto a esse aplicativo, é preciso admitir que talvez seja o melhor exemplo de como legitimar o tratamento de dados pela Administração Pública para a tutela de políticas públicas sanitárias. Com o rastreamento eficiente do vírus e de pessoas que tiveram contato com vetores virais, é possível conter a disseminação da doença, o que traz inúmeros benefícios à população e ao próprio sistema de saúde pública. Há exemplos exitosos no exterior desde o início da pandemia[357,358,359].

É claro que há preocupações com a privacidade – afinal, o aplicativo conseguirá efetivamente rastrear os movimentos do usuário e suas interações sociais –, mas esse parece ser um dos melhores exemplos em que o interesse coletivo de controlar a doença sobrepuja o interesse individual de ver sua privacidade tutelada em detrimento da saúde coletiva. A discussão não é trivial e, claro, perpassaria por um mínimo consentimento dos usuários – afinal, teriam que baixar o aplicativo –, mas, caso o governo tivesse feito uma campanha transparente e explicativa sobre os benefícios do aplicativo no Brasil, talvez a adesão fosse substancialmente maior e não tivessem sido registrados tantos óbitos no país pela pandemia do coronavírus[360].

Dentre todos os analisados, o aplicativo *FGTS* é o que mais parece se preocupar com a etapa de aferição do consentimento do usuário ou com a disponibilização de informações claras acerca do tratamento baseado no legítimo interesse ou nas próprias prerrogativas da Administração de boa execução das políticas públicas. Por fim, é de se ressaltar que todos os aplicativos desta categoria são de classificação indicativa "Livre" e nenhum deles informa haver publicidade durante o uso da ferramenta.

Nesse caso específico, observa-se que há certa padronização de resultados: todos os aplicativos têm política de privacidade em português, apenas um deles a exibe antes do *download* (*FGTS*), dois no primeiro uso (*FGTS* e *Coronavírus*) e na interface do aplicativo (para os demais, o usuário precisa consultar externamente, geralmente no site da entidade pública); nenhum informa haver anúncios ou possibilidade de compras na plataforma; nenhum possibilita a revogação de permissões pela retirada do consentimento – o que indica, *a priori*,

---

[357] BBC. Coronavirus: How does the test-and-trace system work? Disponível em: <https://www.bbc.com/news/explainers-52442754>. Acesso em: 8 abr. 2021.

[358] GLOBO. Coronavírus: países europeus apostam em aplicativos de rastreamento para retornar à normalidade. Disponível em: <https://oglobo.globo.com/mundo/coronavirus-paises-europeus-apostam-em-aplicativos-de-rastreamento-para-retornar-normalidade-24378133>. Acesso em: 8 abr. 2021.

[359] PODER 360. Conheça os aplicativos de rastreamento da covid-19 usados pelos países. Disponível em: <https://www.poder360.com.br/coronavirus/conheca-os-aplicativos-de-rastreamento-da-covid-19-usados-pelos-paises/>. Acesso em: 8 abr. 2021.

[360] VARELLA, Marcelo Dias; XAVIER, Izabella Ribeiro; ROCHA, Antônio Glauter Teófilo da; PINTO, Marcos Cesar de Oliveira. Rastreamento de contatos como ferramenta de combate à transmissão do SARS-CoV-2: benchmark internacional, soluções tecnológicas e considerações éticas. Revista do Programa de Pós-Graduação em Direito da UFC. v. 40 n. 1 (2020): jan/jun 2020, pp. 99-122, p. 118.

que o tratamento não tem essa base legal, e alguns poucos pedem permissões durante o funcionamento da ferramenta e para casos específicos (*Sine, Caesb, Novacap, Meu Imposto* e *Denatran*).

Feita essa breve análise sobre a política de obtenção de consentimento do usuário do aplicativo, passa-se a uma breve análise das permissões relevantes de cada aplicativo, sobretudo à luz dos princípios da necessidade e da finalidade, que representam a ideia de menor privilégio ou acesso aos dados pessoais dos usuários.

3.2 Necessidade e permissões relevantes concedidas para a utilização do aplicativo

Partindo-se mais detidamente à análise das permissões relevantes de acesso concedidas aos aplicativos móveis, é de se registrar, desde já, o dever legal de retenção da menor quantidade de dados pessoais possível. Trata-se aqui de norma inserta no Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet[361], e reproduzida no bojo da LGPD à luz de seus princípios da necessidade e finalidade, que tornam palpável o critério do menor privilégio no acesso aos dados pessoais dos usuários.

Nesse tópico, também é relevante fazer uma diferenciação entre permissões para acesso e melhor utilização do *hardware* do telefone celular e permissões para acesso a *informações do usuário*. De modo natural, as permissões que merecem análise mais cautelosa neste trabalho são aquelas de acesso às informações pessoais.

É importante ter em mente, desde já, que as permissões concedidas são válidas durante a execução em primeiro plano do aplicativo – quanto se está utilizando efetivamente o *software* – e durante seu funcionamento em segundo plano – ou seja, quando o aplicativo está fechado, mas mantendo rotina de execução interna.

Nesse ponto, três princípios deveriam conduzir a solicitação de permissões pelas aplicações: o do menor privilégio, o da transparência e o da confiança[362]. O primeiro indica que o aplicativo deve operar utilizando o mínimo de permissões possíveis para que seu

---

[361] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: (...)
§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
I - tão logo atingida a finalidade de seu uso; ou
II - se encerrado o prazo determinado por obrigação legal.

[362] ABREU, Jacqueline de Souza. *ESPECIAL: As "permissões" de acesso a dados em apps do governo.* Disponível em: <http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-as-permissoes-de-acesso-dados-em-apps-do-governo/>.

funcionamento seja adequado – trata-se de uma preocupação com sua maior estabilidade e menor vulnerabilidade, com vistas a não expor o usuário a riscos desnecessários[363].

O segundo, por sua vez, reflete a preocupação de o usuário ter acesso a o que o aplicativo faz com as permissões, na medida em que, do ponto de vista técnico, após a concessão da permissão, o *software* poderia fazer o que bem entendesse. Isso é especificamente aplicável quando se cogita de permissões abrangentes, que, *per se*, implicam algum grau de desrespeito ao critério da minoração do privilégio de acesso aos dados pessoais da LGPD.

Por sua vez, a confiança indica que o usuário, mesmo que tenha dado permissão geral e abrangente, tem a legítima expectativa de que ela só seja utilizada para fins tecnicamente relevantes, pois, caso se quebre a confiança, o usuário pode ser exposto a riscos e abusos[364]. Trata-se de uma leitura expandida do princípio da privacidade contextual: se o usuário deu a permissão para que o *Facebook* acesse sua galeria, por exemplo, ele deve esperar, de boa-fé, que o aplicativo apenas acesse *efetivamente* as imagens dali quando o usuário quiser fazer o uso delas no bojo da aplicação, para fazer uma postagem, por exemplo. O usuário não espera que o aplicativo fique fazendo, em segundo plano, uma devassa em suas imagens, para qualquer finalidade que seja. Na verdade, ele *confia* que isso não será feito.

As permissões foram, assim, divididas em duas categorias: (i) aquelas que permitem que o aplicativo acesse funcionalidades do *hardware* do aparelho celular – por exemplo, ajuste de volume do celular – e (ii) aquelas que potencialmente concedem ao aplicativo acesso a quaisquer informações do usuário, inclusive as pessoais – por exemplo, acesso à lista de contatos.

De modo geral, foi possível perceber que quase nenhum aplicativo – a única exceção foi o *FGTS* – informa as permissões necessárias ao funcionamento da plataforma quando do *download*. Parece que se parte do pressuposto de que, ao baixar a ferramenta, o usuário concorda com tudo o que ali está "embutido".

É essa espécie de consentimento implícito, avesso às normas da LGPD, na medida em que isso significa uma clara violação à transparência, pois, apesar de terem acesso a informações verdadeiramente sensíveis – gravação de voz, localização, câmera, dados sensíveis e outras –, os aplicativos não informam isso previamente, confiando no suposto consentimento dado com o mero *download*.

---

[363] SALTZER, Jerome H. Protection and the Control of Information Sharing in Multics. Commun. ACM, 17(7), 388–402, 1974. Disponível em: https://doi.org/10.1145/361011.361067.

[364] RICHARDS, Neil; HARTZOG, Woodrow. Taking Trust Seriously in Privacy Law. Stanford Technology Law Review, vol. 19, p. 431-472, 2016.

Em quase todos os segmentos avaliados, há algumas permissões que podem ser consideradas *padrão* – ou seja, estão presentes em quase todos os aplicativos; e, naqueles onde não há a informação relativa ao permissivo específico, é de se desconfiar se não é um caso de falta de transparência, na medida em que há grandes chances de aquela permissão existir na prática.

Dentre elas, algumas são destaque: (i) acesso à internet; (ii) manutenção do aparelho ativo durante a execução; (iii) funcionamento ao ligar o dispositivo; (iv) leitura e edição de fotos, áudio, arquivos e memória externa USB; (v) recebimento de dados da internet; e visualização de conexões à internet e Wi-Fi.

Dentre essas, parece ser particularmente desalinhada com a dinâmica de transparência e de efetiva necessidade do acesso ao dado a (iv), que não é muito intuitiva. *A priori*, ela indica que o aplicativo pode ler e editar todo o sistema de armazenamento do dispositivo. Isso não faria muito sentido e seria contrário às boas políticas de proteção à privacidade do usuário.

É possível, contudo, que essa permissão indique que o aplicativo pode acessar o armazenamento para conseguir ser instalado – afinal, o *software* precisa de um espaço físico no *hardware* – e para conseguir instalar quaisquer outros documentos ou arquivos decorrentes de seu uso direto. Como exemplo, pode-se pensar que um navegador utiliza essa permissão para gravar um arquivo de *download* no dispositivo no usuário. Esse tipo de permissão mais específica faria mais sentido, mas o nome não é bom e a falta de transparência acaba implicando essas lacunas de entendimento, de modo que não há como ter certeza acerca de uma ou outra hipótese ser a correta.

Uma observação é, desde já, relevante: mesmo fora do ambiente do aplicativo específico, o usuário consegue, por meio do menu de configurações do seu celular (ao menos, aqueles com sistema operacional *Android*), restringir as permissões de acesso de seus aplicativos. Basta seguir a sequência "Configurações" – "Aplicativos" – clicar no aplicativo específico – "Permissões" – revogar as concessões previamente definidas. Ao acessar esse tipo de menu, o usuário pode, por experimentalismo, tentar revogar algumas permissões que lhe parecerem excessivas, resguardando os acessos estritamente necessários. Nesse sentido, veja-se a seguinte imagem, que aglomera as telas de alguns aplicativos aqui analisados:

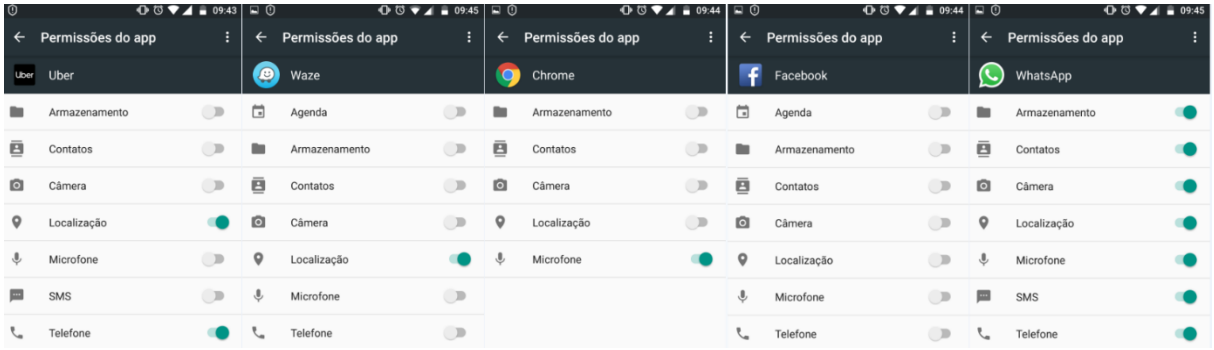

Figura 6 – Possibilidade de revogação de permissões concedidas no menu de configurações do celular, para alguns aplicativos analisados

Embora haja essa possibilidade, a análise feita é mais relevante, na medida em que avalia como os aplicativos, em seus menus próprios, explicam a necessidade das permissões. Ademais, pela leitura das telas apresentadas na imagem retro, é possível perceber que as opções ali dispostas são praticamente pré-definidas e iguais para quaisquer segmentos de aplicativos, ou seja, não há uma disposição específica do *Android* – e nem seria razoavelmente esperado que existisse, na medida em que essa é uma atribuição do aplicativo específico.

Assim, partindo-se dessas premissas, passa-se à análise das permissões mais relevantes solicitadas por cada aplicativo analisado. Salienta-se, desde logo, que todas as tabelas construídas para a presente análise estão dispostas no Apêndice B do trabalho, para que o texto ora construído não ficasse excessivamente poluído com informações menos densas. Assim, esta seção é composta apenas de comentários pontuais e críticos acerca dos resultados ali dispostos, tentando fazer uma análise comparativa entre aplicativos do mesmo ramo, à semelhança da seção anterior.

3.2.1 Comunicação e redes sociais

A partir da tabela, vê-se que há 66 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 33 são referentes a funcionalidades do *hardware* e 33 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Facebook* – acessa 47 informações diferentes.

Por sua vez, os aplicativos que menos têm permissões – *Tinder* e *Pinterest* – acessam 17 informações diferentes. Do universo analisado, a média de permissões foi de 31. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular preocupação: gravar e modificar áudio, fazer transmissão, modificar configurações do sistema, acesso à localização precisa, *download* de arquivos sem o conhecimento do usuário, acesso a sensores corporais (como monitor cardíaco), edição de agenda e envio de e-mails sem conhecimento do usuário, leitura e edição de fluxo social, leitura de agenda e de informações confidenciais. Quase todas essas permissões sensíveis estavam presentes no aplicativo *Facebook*.

No que tange às permissões menos intuitivas, supõe-se que a permissão de acesso a sensores corporais esteja diretamente relacionada a alguma função muito específica do *WeChat*, que inclusive deve usar isso como parâmetro de vantagem competitiva no mercado. No mesmo sentido, a edição de um fluxo social deve indicar função bastante específica do *Viber*, que não se conseguiu investigar detalhadamente na presente análise.

Nesse ponto, supõe-se que essa não seja exatamente uma vantagem competitiva, mas uma transparência maior do aplicativo, porque todos os demais concorrentes também parecem capazes de interpretar o fluxo social do usuário – sugerindo amigos, usando *cookies* e histórico de preferências; trata-se, pela sugestão do nome, da própria ideia por trás da publicidade comportamental, que é a regra em quase todos os aplicativos –, apesar de não usarem essa nomenclatura mais intuitiva e tentarem ocultar a permissão.

3.2.2 Navegadores e e-mails

A partir da tabela, vê-se que há 63 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 30 são referentes a funcionalidades do *hardware* e 33 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *UC Browser* – acessa 48 informações diferentes.

Por sua vez, os aplicativos que menos têm permissões – *Yahoo* e *Outlook* – acessam 23 informações diferentes. Do universo analisado, a média de permissões foi de 31. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular preocupação: gravar e modificar áudio, modificar configurações do sistema, acesso à localização precisa, *download* de arquivos sem o conhecimento do usuário, edição de agenda e envio de e-mails sem conhecimento do usuário, leitura de agenda e de informações confidenciais. Quase todas essas permissões sensíveis estavam presentes no aplicativo *UC Browser*.

Para esta categoria, não parece fazer muito sentido que os *softwares* tenham acesso à localização do dispositivo, sobretudo a localização precisa. Quase *nadando contra a corrente*, apenas o *Gmail* informa não precisar dessa permissão. Se alguns dos aplicativos efetivamente precisar do acesso à localização para operar adequadamente sua plataforma, é melhor que esse pedido de acesso seja específico no momento necessário, do modo mais transparente possível.

Como exemplo caricato, poder-se-ia cogitar de uma mensagem como: "Sr. Usuário, para que você consiga procurar farmácias efetivamente perto de você no buscador, eu, aplicativo, preciso saber se você está em Brasília ou em São Paulo. Você pode me informar manualmente ou permitir que eu acesse a sua localização".

Ao revés, o *Gmail* informa fazer a leitura e edição de *feed* assinado, o que deve ser uma ferramenta bastante específica do aplicativo, que, pelo conceito, acaba aumentando o grau de interação do usuário e, consequentemente, causando mais riscos à sua privacidade. Por sua vez, a leitura de registro sensível de dados, feita pelo *UC Browser*, não parece ser uma coisa positiva – inclusive pela sugestão dada nominalmente –, sobretudo pela falta de clareza do significado de "sensível". Se o aplicativo ao menos explicasse o que considera como sensível, poderia haver maior chance de aceitabilidade à luz dos parâmetros da LGPD.

3.2.3 Entretenimento, vídeos e músicas

A partir da tabela, vê-se que há 55 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 24 são referentes a funcionalidades do *hardware* e 31 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Google Music* – acessa 34 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Band* – acessa 10 informações diferentes. Do universo analisado, a média de permissões foi de 21. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular preocupação: gravar e modificar áudio, acesso à localização precisa, *download* de arquivos sem o conhecimento do usuário, fechamento de outros aplicativos, operação de desligar o celular e leitura de registro de dados sensíveis.

Outra hipótese de pesquisa avaliada aqui diz respeito à comparação entre a versão normal do aplicativo *YouTube* e a sua versão *Kids*. Em uma sucinta comparação, é possível perceber que a versão infantil concede menos permissões do que a versão adulta da aplicação,

o que está alinhado à preocupação de acesso às informações pessoais de crianças. Contudo, é verdade que o aplicativo infantil poderia ter menos acessos ainda, dado que o tratamento de dados de crianças e adolescentes é particularmente pernicioso.

Para esta categoria, também não parece fazer muito sentido que os *softwares* tenham acesso à localização do dispositivo, sobretudo a localização precisa. Nos aplicativos de canais de televisão, isso é ainda menos justificável, na medida em que a programação tende a ser, em sua maioria, nacionalizada (salvo regionalismos específicos).

Em tese, isso parece demonstrar quase uma banalização da privacidade do usuário. Afinal, não seria nada dificultoso que o usuário simplesmente tivesse uma opção de selecionar o seu estado ou a sua cidade a nível macro, sem entrar no mérito da precisão da sua localidade informada por satélite.

O *Google Music*, por sua vez, tem uma permissão peculiar: "agir como Serviço de Gerente de Conta". Imagina-se que ela seja simplesmente decorrente de ser um produto da *Google*, que consegue comunicação fácil com o sistema operacional *Android*, mas falta transparência, como de regra.

3.2.4 Comer e beber

A partir da tabela, vê-se que há 31 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 13 são referentes a funcionalidades do *hardware* e 18 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Rappi* – acessa 25 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Uber Eats* – acessa 16 informações diferentes. Do universo analisado, a média de permissões foi de 19. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular preocupação: gravar e modificar áudio e acesso à localização precisa, mesmo em aplicativo que, *a priori*, não precisa de tal dado para seu correto funcionamento – *Tudo Gostoso*. Afinal, não faz sentido que se acesse a localização do usuário para dispor, eminentemente, sobre receitas culinárias na plataforma, a menos que se tenha a pretensão de fazer, por exemplo, publicidade dos restaurantes mais próximos ao usuário.

Também não parece pertinente a permissão de tirar fotos e gravar vídeos, existente em quase todos os aplicativos analisados. Ao menos, pensa-se que seria mais prudente que a

permissão fosse específica no exato momento em que se tirasse a foto – de uma nota fiscal ou de um produto estragado, por exemplo –, e não algo genérico e abrangente, que chancelaria a manutenção da câmera sempre em *stand-by*; como o consumidor/usuário é vulnerável tecnicamente, e não entende o que é feito, do ponto de vista da tecnologia da informação, com essa permissão – e não há explicações para ele entender –, é razoável supor que a manutenção da câmera *always on* (sempre ativa) é, sim, uma possibilidade.

Por fim, a última permissão interessante é a de "verificar licença da *Google Play*", existente no aplicativo *Tudo Gostoso*. Ora, se o usuário já conseguiu fazer o *download* da aplicação pela loja online, em tese a sua conta seria válida e ativa; assim, a única razão para essa permissão é chancelar que o aplicativo busque os dados do usuário em sua respectiva conta *Google*, que tipicamente contém muitos dados pessoais.

Apesar de essa permissão possivelmente ser inócua – na medida em que precisaria de uma concordância da própria *Google Play*, o que se imagina inexistente –, a mera tentativa não deixa de ser contrária ao princípio do mínimo privilégio. Esse mesmo comentário se aplica a muitos *softwares* de diversas outras categorias, que parecem projetados para a indevida intromissão na privacidade, e não para sua proteção por projeto e por padrão. É, com efeito, fora do atual padrão do mercado encontrar algum aplicativo que efetivamente explane as permissões para seu usuário e que busque avançar apenas naquilo que é estritamente necessário para o funcionamento da ferramenta.

3.2.5 Infantis e jogos

A partir da tabela, vê-se que há 31 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 16 são referentes a funcionalidades do *hardware* e 15 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Garena* – acessa 23 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Candy Crush* – acessa 5 informações diferentes. Do universo analisado, a média de permissões foi de 11. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular preocupação: gravar e modificar áudio, fazer transmissão, modificar configurações do sistema e acesso à localização precisa. Nada muito diferente das demais categorias analisadas até o momento, salvo a

possibilidade de fazimento de transmissões em tempo real, que é comum em alguns jogos atuais e, portanto, aceitável sob o paradigma da proporcionalidade.

Na comparação entre o demonstrativo gratuito do jogo e a sua versão completa e paga – caso de *Minecraft* –, não foram verificadas distinções nas permissões concedidas. Ou seja, aqui a hipótese de pesquisa de que possivelmente haveria diferenças entre os acessos dados às versões gratuitas e pagas foi afastada. Confirma-se, ao revés, a percepção de que muitos aplicativos são construídos sob a metodologia *freemium*, que acaba não fazendo real diferenciação, do ponto de vista da proteção de dados, entre o aplicativo em suas versões paga e gratuita.

No mesmo sentido, foi visto na seção anterior que diversos jogos possibilitam a ascensão para uma versão paga e supostamente livre de publicidade. Contudo, nesse anúncio de *evolução para a privacidade*, os aplicativos não informam exatamente quais permissões originais serão revogadas. Ou seja, falta um pouco de transparência, requisito legal.

Nessa esteira de falta de transparência, a permissão para "manter o aparelho ativo" parece ser mais um típico caso desse comportamento omissivo de alguns desenvolvedores – ou, ao menos, um comportamento despreocupado com a fidedignidade das informações prestadas –, na medida em que é pouco crível que *Minecraft* e *Hopping Ball* não consigam manter o dispositivo em funcionamento enquanto o usuário está jogando. Esse tipo de constatação acaba minando a confiabilidade das listas de permissões existentes na página de *download* de cada aplicativo, na medida em que se trata, provavelmente, de um erro claro.

Na mesma linha, também é pouco aceitável, sob a ótica do menor privilégio, que o *Paint Pop 3D* precise de acesso à localização precisa do dispositivo para o seu correto funcionamento. Talvez seja mais um exemplo do atual cenário de banalização da privacidade. Por outro lado, os demais aplicativos parecem, nesse ponto, aderentes à tutela da privacidade que se entende como adequada, pois nenhum acessa a localização do usuário, já que esse dado tende a ser desnecessário ao funcionamento da ferramenta.

3.2.6 Finanças e crédito

A partir da tabela, vê-se que há 44 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 16 são referentes a funcionalidades do *hardware* e 28 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Bradesco* – acessa 29 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Investing* – acessa 13 informações diferentes. Do universo analisado, a média de permissões foi de 20. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular preocupação: gravar e modificar áudio, acesso à localização precisa, leitura de registro de dados sensíveis e leitura da agenda e informações confidenciais. Não há, contudo, maior detalhamento sobre o que se entende por *informações confidenciais*, mas, como se trata de instituições financeiras, é razoável supor que a confidencialidade remete aos próprios dados bancários em si – mas, como de praxe, seria mais adequado à legislação que a explanação fosse mais clara.

Na comparação entre as versões europeia, britânica e brasileira do aplicativo *Santander*, é perceptível que a versão brasileira é aquela que menos se preocupa com a privacidade dos usuários. Muito provavelmente, isso ocorre por causa da legislação mais apertada na Europa, com o RGPD tendo mais tempo de *enforcement*: apesar de a LGPD ser restritiva e preocupada com a proteção dos dados pessoais, é provável que a cultura da privacidade ainda não tenha irradiado verdadeiramente em todas as empresas até o momento. Não à toa, o *Itaú* começou a fazer as propagandas remetendo ao necessário respeito à privacidade no final do primeiro trimestre de 2021, cerca de meio ano, portanto, após a vigência formal da LGPD.

Nesse sentido, por exemplo, o *Santander UK* é o único que não acessa a localização do dispositivo, o que também parece ser um recurso inócuo para a categoria de aplicativos de banco. Com efeito, se o usuário quiser localizar alguma agência física próxima a seu local, ele poderia dar a permissão específica para aquele momento.

E, no mesmo sentido, não parece haver qualquer pertinência da informação de geolocalização para alguma conferência de segurança do aplicativo. Mas, se houver necessidade dessa verificação geográfica – para movimentações de maior valor, por exemplo – , é mais adequado às normas da LGPD que esse acesso seja restrito ao momento em que necessário. Se o banco precisar confirmar a localização de um usuário para permitir uma transação online que esteja fora do padrão financeiro de determinado cliente – para aferir se não está sendo vítima de um sequestro, por exemplo –, que o acesso se dê apenas nesse escopo.

Também não faz muito sentido que os aplicativos de bancos acessem e, ainda menos, modifiquem os contatos do seu usuário, a menos que se enxergue isso como uma oportunidade para buscar novos clientes à instituição financeira. Contudo, essa verdadeira

fishing expedition (“expedição de pesca”) é vedada pelas normas de proteção de dados e de respeito à privacidade, na medida em que seria lastreada em verdadeiro abuso de confiança.

Por sua vez, a possibilidade de o *PayPal* modificar configurações do sistema também chama atenção: qual a finalidade de a ferramenta editá-las? Não parece haver muita congruência entre a funcionalidade nuclear do aplicativo e a permissão, que deve ser o requisito básico para se aferir a validade da concessão.

Ou seja, a ideia é que se promova um verdadeiro teste de proporcionalidade: a permissão deve ser necessária e adequada à finalidade pretendida pelo serviço desempenhado pelo aplicativo, ou não será proporcional e, portanto, incapaz de gerar a restrição à privacidade do usuário. Esse deve ser o prisma para todas as análises. O que não passar no teste de proporcionalidade não justifica a compressão da amplitude da privacidade do usuário para eventuais finalidades meramente comerciais do provedor.

3.2.7 Compras

A partir da tabela, vê-se que há 37 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 15 são referentes a funcionalidades do *hardware* e 22 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Amazon* – acessa 26 informações diferentes.

Por sua vez, os aplicativos que menos têm permissões – *OLX*, *Magazine Luiza* e *Ebay* – acessam 14 informações diferentes. Do universo analisado, a média de permissões foi de 18. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular preocupação: gravar e modificar áudio, acesso à localização precisa, operação de desligar o celular. Aliás, não parece haver muito sentido em o *Mercado Livre* e o *Magazine Luiza* permitirem a realização de ligações, a menos que se trate de uma permissão para meramente facilitar alguma operação durante o funcionamento da plataforma, o que deveria ser requerido ao titular dos dados apenas no momento efetivo dessa necessidade.

Da mesma forma, é desnecessário o acesso à localização precisa do usuário, na medida em que, quando da efetivação de pretensa compra, o consumidor informará o endereço de entrega – que, muitas vezes, não é aquele onde está situado. Similarmente, o acesso aos contatos também não parece justificável, a menos que se queira criar uma rede de publicidade comportamental, à semelhança das instituições financeiras na seção anterior.

3.2.8 Notícias e revistas

A partir da tabela, vê-se que há 33 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 11 são referentes a funcionalidades do *hardware* e 22 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *G1* – acessa 18 informações diferentes.

Por sua vez, os aplicativos que menos têm permissões – *Der Spiegel*, *Folha de São Paulo* e *NY Times* – acessam 9 informações diferentes. Do universo analisado, a média de permissões foi de 13. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, a transmissão via infravermelho deve fazer alusão a uma funcionalidade bastante específica do *CNN*, da mesma forma que a permissão para tirar fotos e gravar vídeos no *NY Times* – já que não há, em abstrato, qualquer relação lógica entre a câmera e um aplicativo de leitura de notícias. O acesso e a edição de contas e contatos também parece desalinhado com o princípio do menor privilégio no acesso às informações puramente necessárias à finalidade da ferramenta.

Um dado chama particularmente a atenção: ao passo que os aplicativos de noticiários brasileiros parecem não atentos exatamente com a privacidade de seus usuários, aqueles voltados ao público europeu são diferentes, tanto em número de permissões solicitadas, como na qualidade das permissões.

Com efeito, nenhum jornal europeu analisado solicita acesso à localização exata do dispositivo, ao passo que os brasileiros o fazem em sua maioria, sem que haja, *a priori*, qualquer relevância na referida informação. Ainda melhores do que os europeus, estão os jornais dos Estados Unidos, que, como visto na seção anterior, permitem inclusive a revogação do consentimento de modo específico.

3.2.9 Turismo, locais, mapas e navegação

A partir da tabela, vê-se que há 57 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 28 são referentes a funcionalidades do *hardware* e 29 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Google Maps* – acessa 38 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Skyscanner* – acessa 8 informações diferentes. Do universo analisado, a média de permissões foi de 22. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias, ao acesso às conexões à internet, e ao acesso às localizações precisa e aproximada do dispositivo.

Dentre todas as permissões, algumas despertam particular preocupação: *download* de arquivos sem conhecimento, realizar ligações SIP, gravar e modificar áudio, acesso à localização precisa, leitura de registro de dados sensíveis, leitura de agenda e informações confidenciais e modificação de configurações do sistema.

A realização de ligações pelo *Uber* e, principalmente, pelo *Google Maps* é peculiar. No que tange àquele, é fato que é possível ligar aos motoristas. O que chama atenção, contudo, é que essa funcionalidade também existe no *99* e no *Cabify*, embora não haja transparência sobre a permissão. Quanto à ligação SIP, não parece haver pertinência lógica entre uma chamada sem rastros de IP e as funcionalidades disponibilizadas pelo *Decolar*. A menos que exista alguma função absolutamente desconhecida do grande público, o que continuaria desalinhado com o ordenamento jurídico, por incentivar o anonimato na internet, o que é vedado por lei.

O acesso à localização parece pertinente a todos os aplicativos de mapas e navegação, mas não parece muito relevante, *a priori*, aos aplicativos de mero turismo, como *Decolar*, *Booking*, *Skyscanner* e *Airbnb*. Talvez seja mais um dos exemplos de banalização dos dados pessoais e da vida privada. De modo ainda mais específico, o *Waze* solicita acesso aos "comandos adicionais de provedores de localização", o que é obscuro e pouco intuitivo, embora parece aceitável à luz do fato de que o *Waze* é um mapa/GPS, o que demanda toda a acurácia possível para o bom desempenho de suas funções.

Por fim, não parece haver qualquer relação entre leitura e edição de contas e contatos e a funcionalidade típica do segmento ora analisado, o que denota a falta de pertinência lógica, de modo a vulnerar o princípio da necessidade e, por consectário, a lógica do menor privilégio. Da mesma forma, o porquê de o *99* "ler o registro sensível de dados" também é desconhecido e, *a prori*, parece injustificável à luz da LGPD. Uma coisa é a instituição financeira ter acesso ao registro sensível de dados – seja lá o que isso significar –; outra, substancialmente diversa, é um aplicativo de transporte ter o mesmo acesso, sendo que sua finalidade deveria ser a de meramente fazer o adequado transporte de seus passageiros.

Nessa categoria, portanto, há fartos exemplos de aplicativos que são pouco transparentes ao exibir a sua lista de permissões concedidas na página do *download* e de outras

aplicações que excedem a razoabilidade na coleta e tratamento de dados pessoais, o que demonstra que a cultura da privacidade, o *privacy by design* e *by default*, ainda está longe de ser uma realidade efetiva no Brasil.

3.2.10 Educação

A partir da tabela, vê-se que há 28 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 12 são referentes a funcionalidades do *hardware* e 16 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *Google Tradutor* – acessa 22 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Khan Academy Kids* – acessa 6 informações diferentes. Do universo analisado, a média de permissões foi de 14. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, a gravação e modificação de áudio parece particularmente desalinhada com a lógica da LGPD de menor acesso, mas, aparentemente, ela está restrita àqueles aplicativos que realmente têm funcionalidades específicas nesse sentido (aplicativos de aprendizado de idiomas).

Quanto ao acesso e à edição de contas e contatos, parece não haver muita pertinência lógica com a funcionalidade principal desses aplicativos, razão por que a permissão não deveria existir. O mesmo se pode falar em relação à permissão de o *Google Tradutor* poder ler SMS: qual a relevância disso para o funcionamento do *software*? Salvo melhor juízo – ou a existência de alguma função muito específica –, nenhuma.

Noutro giro, vale aqui o registro de que nenhuma dessas aplicações informa acessar os dados de localização, o que é muito positivo, na medida em que realmente não fariam sentido para a correta operação do *software* em sua forma padrão. Seria mais adequado à LGPD que todos os demais aplicativos que não necessitam desse tipo de acesso também tivessem a mesma abordagem, mas essa realidade parece distante.

Outra hipótese de pesquisa avaliada aqui diz respeito à comparação entre a versão normal do aplicativo *Khan Academy* e a sua versão *Kids*. Em uma sucinta comparação, é possível perceber que a versão infantil concede menos permissões do que a versão adulta da aplicação, o que está alinhado à preocupação de acesso às informações pessoais de crianças e adolescentes estabelecida pela própria LGPD.

3.2.11 Produtividade e antivírus

A partir da tabela, vê-se que há 83 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 38 são referentes a funcionalidades do *hardware* e 45 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, os aplicativos que mais têm permissões – *AVG* e *McAfee* – acessam 49 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Adobe Reader* – acessa 17 informações diferentes. Do universo analisado, a média de permissões foi de 32. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias, ao acesso às conexões à internet e o acesso às contas e aos contatos do dispositivo.

Apesar de os números aqui serem expressivos, é evidente que a média foi puxada para cima por causa dos antivírus, que, por próprio conceito, precisam de amplo acesso – ou não fariam a varredura completa dos *malwares*. Na comparação específica entre os aplicativos de compartilhamento, o *Share It* parece menos adequado às normas da LGPD do que os seus concorrentes diretos. Quanto aos leitores e editores de documentos, o *Google Docs* também é o aplicativo que mais tem permissões de acesso aos dados pessoais dos usuários em comparação aos seus concorrentes.

Dentre todas as permissões, algumas despertam particular atenção: (i) alterar ou interceptar configurações de rede e tráfego, especificamente no *Kaspersky*. Essa permissão, contudo, parece pertinente ao funcionamento de um bom antivírus; (ii) definição de aplicativos favoritos, também no *Kaspersky*, mas agora sem haver pertinência lógica *prima facie* entre a permissão e a funcionalidade principal do aplicativo; (iii) *download* de arquivos sem conhecimento, no âmbito de alguns aplicativos de compartilhamento de documentos e *Google Docs*, o que parece pernicioso, sobretudo à luz de que não necessariamente esses aplicativos de compartilhamento são isentos de riscos à segurança lógica dos dados do usuário; (iv) envio de SMS, que também não parece guardar pertinência com a função principal do *Kaspersky*.

Além disso, fala-se de (v) fechamento de outros aplicativos, que, apesar de relevante, também parece guardar relação com as funcionalidades de um antivírus. Ao revés, contudo, não parece pertinente com as funções pretensamente desempenhadas pelo *Share It*; (vi) acesso à localização, que, apesar de necessário aos antivírus – para os mecanismos antifurto –, não parece estritamente necessário ao *4Shared* e ao *Share It*, o que denota nova despreocupação com a privacidade dos usuários; (vii) acesso às contas e aos contatos, bem como a sua edição, que não parece ser relevante às funções principais dos aplicativos

responsáveis tão somente pela leitura de arquivos; (viii) acesso a todos os *downloads* do sistema, sendo que o *4Shared* poderia ter sua operação restrita apenas àqueles *downloads* que efetuou em sua operacionalização.

E ainda, há que se mencionar (ix) a possibilidade de se editar agenda e enviar e-mails sem conhecimento, o que também não parece alinhado às funcionalidades principais dos antivírus – tanto é assim, que o *McAfee* não tem essas permissões; (x) a leitura e edição de SMS e registros de chamada, bem como a leitura da agenda e de informações confidenciais, que também não parece pertinente às funções principais do *Kaspersky*; (xi) que, embora a leitura do registro sensível de dados possa fazer sentido para os antivírus, parece desnecessária para o *Share It*, sobretudo porque este aplicativo trabalha justamente com o compartilhamento de arquivos – um dos quais pode ser o sensível do usuário –; (xii) que, conquanto também possa fazer sentido aos antivírus e aos aplicativos da *Google*, a leitura da configuração dos serviços da empresa não é pertinente ao *WPS Office* e ao *4Shared*; e, por fim, (xiii) que o gerenciamento de usuários parece muito desnecessário ao *Polaris Office*, dadas as suas funcionalidades padronizadas. Ou seja, há uma sucessão de aparentes excesso nos acessos.

3.2.12 Governamentais

A partir da tabela, vê-se que há 26 tipos diferentes de permissões concedidas nos aplicativos analisados, das quais 10 são referentes a funcionalidades do *hardware* e 17 se referem, potencialmente, ao acesso de informações pessoais do usuário. Desses, o aplicativo que mais tem permissões – *DigiSUS* – acessa 17 informações diferentes.

Por sua vez, o aplicativo que menos tem permissões – *Caixa Auxílio Emergencial* – acessa 1 informações diferente: apenas a conexão à internet, o que naturalmente parece inverídico, na medida em que o aplicativo deve, ao menos, receber dados da internet também. Do universo analisado, a média de permissões foi de 12. As permissões de acesso a potenciais informações pessoais mais relevantes dizem respeito à leitura e edição de fotos, arquivos e mídias e ao acesso às conexões à internet.

Dentre todas as permissões, algumas despertam particular atenção: *download* de arquivos sem notificação, licença completa para interagir entre usuários, modificação de contatos, acesso à localização precisa, leitura da agenda e de informações confidenciais e edição de agenda e envio de e-mails sem o conhecimento direto do usuário.

Em específico: não faz sentido, do ponto de vista da necessidade para sua operação, que o *Sisu* possa fazer *download* de arquivos sem notificação do usuário; é indevidamente

obscura e pouco transparente a permissão para que o *SNE Denatran* possa interagir completamente entre os usuários; embora possa haver alguma justificativa para que os aplicativos *Caesb* e *Novacap Buraco* – denúncias de problemas, por exemplo – tenham acesso à localização do usuário, parece ser uma permissão muito ampla para uma funcionalidade muito específica e pontual. Seria mais adequado à LGPD que a autorização de acesso ao dado fosse pedida só no momento específico em que necessário.

Ainda: a permissão para tirar fotos e gravar vídeos parece compatível com os aplicativos que solicitam essa permissão. Nesse ponto, contudo, seria útil se cogitar de uma separação dessas permissões – isto é, uma para "tirar fotos" e outra, autônoma, para "gravar vídeos" –, na medida em que a gravação de vídeos é muito mais compressiva dos direitos de personalidade do que o acesso puro e simples à câmera estática. Em noutro giro, o acesso à ferramenta de gravação dinâmica de imagens parece desnecessário aos aplicativos governamentais aqui analisados.

Por sua vez, conquanto a permissão de acesso à localização do dispositivo possa fazer sentido para os aplicativos *Caesb* e *Novacap* – justamente pelas mesmas razões retro –, não parece guardar muita relação com as funcionalidades principais dos aplicativos da *Caixa*, *e-Título*, *DigiSUS*, *Meu INSS* e *SNE Denatran*. Sendo o tratamento desses dados baseado no fazimento de políticas públicas, parece haver, em verdade, um desvirtuamento das próprias finalidades dessa gestão governamental.

Noutro giro, o acesso e a edição das contas e contatos também não parece fazer muito sentido no âmbito dos aplicativos governamentais; A seu turno, a permissão dos aplicativos *Caixa Trabalhador* e *Bolsa Família* para ler e editar agenda, enviar e-mails sem conhecimento e acessar informações confidenciais parece ser a mais sensível. O não conhecimento desses envios já seria capaz de implicar o desrespeito à lógica da LGPD para quaisquer aplicativos, mas parece ainda mais desrespeitoso no bojo dos aplicativos governamentais, que deveriam se basear pela estrita legalidade. O mesmo se fala do acesso a informações sensíveis.

E, por fim, embora a permissão de leitura e edição de fotos, mídia, arquivos e memória USB tenha sido uma regra em quase todos os aplicativos, a depender de seu real significado – desconhecido –, pode ser particularmente perniciosa neste contexto de aplicativos governamentais. Aliás, também chama atenção o fato de que o *CNH Digital* informa não precisar de tais permissões, o que, provavelmente, denota falta de transparência do *software* quando de seu *download* pelos usuários, na medida em que, provavelmente, a permissão é requerida na prática da operação da ferramenta.

3.3 Aspectos mais relevantes da política de privacidade do aplicativo

De modo mais abstrato, a LGPD afirma que a atividade de tratamento de dados pessoais, gênero de atividades cuja definição também consta na lei, deverá observar, além da boa-fé, alguns princípios (art. 6º da referida Lei): finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

De modo mais concreto, fala-se da previsão de inúmeros direitos ao usuário/consumidor e de balizas para o tratamento legítimo – consentimento, legítimo interesse, dentre outros, tratamento de dados sensíveis, tratamento de dados de crianças, tratamento de dados pela Administração, transferência internacional de dados, prescrições de segurança e de boas práticas e responsabilidades dos agentes de tratamento.

Assim, procedeu-se à análise pormenorizada de todos os termos da política de privacidade de cada aplicativo selecionado – conforme lista já enunciada –, para fins de se chegar àquelas cláusulas que despertam maior interesse do jurista. Como, naturalmente, muitas cláusulas se repetem nos diversos aplicativos analisados, as menções aqui feitas são pontuais àquelas que parecem distinguir o modo de confecção de uma política em relação às demais, para que a leitura não fique tão cansativa.

3.3.1 Comunicação e redes sociais

Em relação ao *WhatsApp*[365], dois pontos pareceram particularmente desalinhados com a lógica da LGPD. O primeiro ponto[366] merece atenção porque implica dizer que os dados são compartilhados irrestritamente entre todas as empresas do mesmo grupo econômico. Ou seja, mesmo que você não seja cadastrado no aplicativo *Facebook*, por exemplo, alguns de seus dados podem chegar ao conhecimento dessa plataforma pelo simples fato de você possuir *WhatsApp*. Isso parece intrinsecamente violar as decisões eminentemente pessoais de cada usuário, na medida em que não deve desejar que seus dados sejam compartilhados entre quaisquer empresas pelo simples fato de pertencerem ao mesmo grupo empresarial.

---

[365] WHATSAPP. *WhatsApp Privacy Policy*. Disponível em: <https://www.whatsapp.com/legal?eea=1#privacy-policy>. Acesso em: 26 mar. 2021.

[366] "O Facebook e outras empresas do mesmo grupo também podem usar dados do WhatsApp para fazer sugestões (por exemplo, de amigos, de contatos ou de conteúdo interessante) e mostrar ofertas e anúncios relevantes".

O segundo ponto[367] merece atenção por possuir conceitos de textura extremamente aberta, hábeis a justificar qualquer espécie de compartilhamento de dados. Basta, por exemplo, que se utilize o pretexto de proteção de direitos, que qualquer espécie de coleta e fornecimento de dados é automaticamente chancelada.

No que toca ao *Google Meet*, seus termos de privacidade são genericamente aplicáveis a todos os produtos da *Google*, razão por que são avaliados em outra seção do trabalho. Registra-se, desde já, que, embora o documento pareça transparente e elucidativo – pelos recursos visuais utilizados em aparente substituição ao excesso de texto –, é criticável a adoção de única política de privacidade para praticamente todos os produtos da empresa, na medida em que cada aplicação guarda particularidades que deveriam merecer tutela específica.

A política de privacidade do *Signal*[368] é enxuta e, basicamente, se limita a tentar tranquilizar o usuário do aplicativo no sentido de que nenhuma informação pessoal é repassada a terceiros ou acessada indevidamente pela aplicação, em virtude da criptografia de ponta a ponta na troca de mensagens. Embora seja certo que o excesso de informações prejudica a transparência, parece que o *Signal* deveria ter sido ligeiramente mais analítico em suas explanações, na medida em que a singeleza dos termos pode transparecer que *algo não está sendo dito ali*. Mas, de modo geral, a simplicidade é o que se entende por mais aderente à lógica de boa-fé objetiva da LGPD.

Em relação ao *Facebook/Messenger/Instagram*[369], diversos aspectos parecem desalinhados com a lógica da LGPD em uma análise mais detida. Aliás, é relevante pontuar que, mesmo sendo empresas do mesmo grupo econômico, as políticas de privacidade do *WhatsApp* têm uma lógica diversa daquelas do *Facebook*: enquanto aquele aplicativo parece se preocupar mais com o paradigma da proteção de dados – salvo pelos compartilhamentos já mencionados –, este aplicativo não parece devidamente alinhado à dinâmica da LGPD, por algumas razões.

O primeiro ponto[370] indica que o *monitoramento* realizado pelo aplicativo é integral, inclusive de modo cooperado entre todos os *hardwares* porventura conectados. O

---

[367] "Podemos coletar, usar, reter e compartilhar dados quando acreditarmos em boa fé que isso se faz necessário para: (a) atuar conforme exigido pela legislação aplicável ou em processos judiciais ou administrativos; (b) impor nossos Termos e outros termos e políticas aplicáveis, inclusive investigações sobre possíveis violações; (c) detectar, investigar, prevenir e resolver atividades fraudulentas e ilícitas ou questões de segurança ou técnicas; ou (d) proteger os direitos, a propriedade e a segurança de nossos usuários, do WhatsApp, da família de empresas do Facebook ou de terceiros".

[368] SIGNAL. Signal Terms & Privacy Policy. Disponível em: <https://signal.org/legal/#terms-of-service>. Acesso em 13 abr. 2021.

[369] FACEBOOK. *Política de Dados*. Disponível em: <https://m.facebook.com/policy.php>. Acesso em: 26 mar. 2021.

[370] "Coletamos informações de e sobre os computadores, telefones, TVs conectadas e outros dispositivos

segundo ponto[371] versa de modo específico sobre a publicidade comportamental de modo amplo.

Com efeito, o aplicativo fornece a terceiros não identificados todo o histórico de compras e de atividades em geral do usuário, bem como recebe, provavelmente de outros aplicativos ou plataformas que também realizem essa coleta múltipla de dados, todas as informações a respeito do perfil do usuário. Havendo tanta amplitude para o fazimento do perfil digital com vistas à publicidade comportamental, é possível criticar inclusive a sua legalidade, na medida em que parece haver um abuso da confiança do usuário, retirando-lhe o basilar direito de ver seus dados respeitados no bojo do contexto em que consentiu para o tratamento ou em que esse seria legitimamente esperado.

O terceiro ponto[372], além de versar sobre a publicidade comportamental, também abarca todo o pernicioso cenário de "usuário-bolha" já comentado. Com efeito, o aplicativo acaba induzindo o usuário a ser submetido apenas às informações ou funcionalidades a que já esteja acostumado ou que seja de seu interesse passado.

Contudo, não necessariamente a análise do comportamento passado implica dizer que a atuação futura será igual, na medida em que existem circunstâncias tópicas especiais que motivam comportamentos excepcionais. Entretanto, ao deixar o usuário restrito ao ambiente em que cotidianamente navega, o aplicativo contribui sobremaneira para formar a bolha.

---

conectados à web que você usa e que se integram a nossos Produtos, e combinamos essas informações dos diferentes dispositivos que você usa. Por exemplo, usamos as informações coletadas sobre seu uso de nossos Produtos em seu telefone para personalizar melhor o conteúdo (inclusive anúncios) ou os recursos que você vê quando usa nossos Produtos em outro dispositivo, como seu laptop ou tablet, ou para avaliar se você, em resposta a um anúncio que exibimos em seu telefone, realizou uma ação em um dispositivo diferente".

[371] "Informações de parceiros. Os anunciantes, desenvolvedores de aplicativos e publishers podem nos enviar informações por meio das Ferramentas de Negócios do Facebook que eles usam, inclusive nossos plugins sociais (como o botão Curtir), o Login do Facebook, nossas APIs e SDKs e o pixel do Facebook. Esses parceiros fornecem informações sobre suas atividades fora do Facebook, inclusive informações sobre seu dispositivo, os sites que você acessa, as compras que faz, os anúncios que visualiza e sobre o uso que faz dos serviços deles, independentemente de ter ou não uma conta ou de estar conectado ao Facebook". Segue a explicação: "Por exemplo, um desenvolvedor de jogos poderia usar nossa API para nos informar quais jogos você joga, ou uma empresa poderia nos informar sobre uma compra que você fez na loja dela. Além disso, recebemos informações sobre suas ações e compras online e offline de provedores de dados de terceiros que têm autorização para nos fornecer essas informações. Tais parceiros recebem seus dados quando você acessa ou usa os serviços deles ou por meio de terceiros com os quais eles trabalham. Exigimos que cada um desses parceiros tenha autorização legal para coletar, usar e compartilhar seus dados antes de fornecê-los para nós".

[372] "Como usamos essas informações? Usamos as informações que temos para oferecer nossos Produtos, inclusive para personalizar recursos e conteúdo (como seu Feed de Notícias, Feed do Instagram, Instagram Stories e anúncios) e fazer sugestões a você (como grupos ou eventos pelos quais você possa se interessar ou tópicos que você talvez queira seguir) dentro e fora de nossos Produtos". Ao explicar o acesso, o termo de uso afirma que, "Para criar Produtos personalizados que sejam únicos e relevantes para você, usamos suas conexões, preferências, atividades e seus interesses com base nos dados que coletamos e dos quais tomamos conhecimento por seu intermédio e de outras pessoas (inclusive dados com proteções especiais que você opte por fornecer); como você usa e interage com nossos Produtos; e as pessoas, as coisas ou os lugares com os quais você esteja conectado e nos quais tenha interesse, dentro e fora dos nossos Produtos".

Cogita-se, nesse sentido, até mesmo de que o Presidente da República esteja, em suas redes sociais, vivendo dentro de uma bolha de opiniões meramente concordes com a sua visão de mundo, o que certamente é deletério para a democracia, à qual é imprescindível o confronto sadio de ideias e ideais[373].

O quarto ponto[374] merece particular atenção por tratar da transferência internacional de dados. Afirma a política que foi obtido consentimento específico do usuário para esse intercâmbio de informações – o que não se viu na prática – e, também, que o compartilhamento internacional é baseado em cláusulas-padrão, o que, em tese, daria maior segurança ao usuário no sentido de que seus dados pessoais e sua privacidade estariam sendo regularmente resguardados no país de destino dos dados. Contudo, não há, intuitivamente, uma lista dos países destinatários desses dados, de modo que o *accountability* efetivo pelo usuário não é tão pleno quanto poderia em potencial.

Em relação ao *Twitter*[375], os seus termos de privacidade e privacidade parecem mais alinhados à dinâmica da LGPD. Um primeiro aspecto[376], que demonstra a postura de a empresa apenas obter e compartilhar os dados expressamente autorizados pelos usuários, parece aderente à tutela da privacidade que se entende como adequada, na medida em que representa a força do consentimento no caso concreto. Causa certa preocupação, contudo, o *disclaimer*

---

[373] METRÓPOLES. A bolha do Jair: o que o presidente vê quando navega nas redes sociais. Disponível em: <https://www.metropoles.com/brasil/a-bolha-do-jair-o-que-o-presidente-ve-quando-navega-nas-redes-sociais>. Acesso em: 12 abr. 2021.

[374] "Compartilhamos informações globalmente, tanto internamente nas Empresas do Facebook, quanto externamente com nossos parceiros e com aqueles com quem você se conecta e compartilha no mundo todo em conformidade com esta política. Suas informações podem, por exemplo, ser transferidas ou transmitidas para, ou armazenadas e processadas nos Estados Unidos ou outros países fora de onde você mora, para os fins descritos nesta política. (...) Utilizamos cláusulas contratuais padrão, seguimos as decisões de adequação da Comissão Europeia em relação a determinados países, conforme aplicável, e obtemos seu consentimento para essas transferências de dados para os Estados Unidos e outros países".

[375] TWITTER. *Política de Privacidade Twitter*. Disponível em: <https://twitter.com/pt/privacy>. Acesso em: 26 mar. 2021.

[376] "Nós compartilhamos ou divulgamos seus dados pessoais com o seu consentimento ou de acordo com as suas orientações, por exemplo, quando você autoriza que um cliente Web ou aplicativo de terceiros acesse a sua conta, ou quando você nos orienta a compartilhar seu feedback com uma empresa". O aplicativo ainda esclarece: "Se você compartilhou informações como Mensagens Diretas ou Tweets protegidos com outra pessoa que acessar o Twitter utilizando um serviço de terceiros, lembre-se de que as informações poderão ser compartilhadas com o serviço de terceiros. Sujeito às suas configurações, também fornecemos a terceiros determinados dados pessoais para nos ajudar a oferecer ou operar nossos serviços. Por exemplo, compartilhamos com anunciantes os identificadores de dispositivos que visualizaram seus anúncios, para que eles possam avaliar a eficácia do nosso negócio de publicidade". E segue sua explicação ao afirmar que: "Também compartilhamos os identificadores de dispositivo, juntamente com os interesses ou outras características de um dispositivo ou da pessoa que o utiliza, para ajudar parceiros a decidir se veiculam um anúncio nesse dispositivo e para permitir que possam realizar atividade de marketing, análises de marca, publicidade com base em interesses ou atividades similares. (...) As informações que compartilhamos com esses parceiros não incluem seu nome, endereço de e-mail, número de telefone ou nome de usuário do Twitter, mas algumas dessas parcerias permitem que as informações que compartilhamos sejam vinculadas a outras informações pessoais caso o parceiro obtenha seu consentimento primeiro".

utilizado no sentido de que a plataforma pode acessar dados compartilhados por parceiros comerciais, que conseguirão obter os referidos dados segundo seus próprios critérios de privacidade.

Em um mercado global e com teias amplas[377], é relativamente temerário que, eventualmente, a baliza seja pelo aplicativo ou serviço que menos proteja a privacidade de seus usuários. Isso porque, segundo o *disclaimer*, bastaria que o primeiro serviço tivesse coletado o dado segundo seus próprios padrões de privacidade – ainda que de forma ilegítima – para que o *Twitter* pudesse ter acesso aos mesmos dados, por meio de acordos comerciais fora de controle do usuário e proprietário do dado, supostamente de maneira legítima. O corte certamente seria no sentido de proteções mínimas ao usuário das aplicações.

Por sua vez, o segundo ponto merece o mesmo destaque do que aquele feito quando da análise do contrato do *Facebook*: é temerário, para um usuário brasileiro, que seus dados sejam circulados globalmente sem que ele tenha efetivo controle sobre isso, sobretudo se se assumir a dificuldade de as autoridades brasileiras competentes pretenderem um *enforcement* da LGPD a nível internacional, depois que os dados já foram exportados e eventualmente violados em seus princípios basilares de segurança e afins.

Nesse ponto, contudo, o tópico que chama mais atenção é o terceiro[378]. Notadamente, a União Europeia alcançou o patamar mais elevado em relação à regulação sobre o tratamento de dados pessoais com o RGPD, que inspirou a LGPD. Nesse sentido, conforme o próprio *disclaimer* estabelecido pelo *Twitter*, na União Europeia, a proteção aos dados dos usuários merece atenção redobrada, especialmente no que tange ao modelo de negócios estabelecidos pelas empresas transmissoras e receptoras dos respectivos dados trafegados.

Esse ponto basicamente se coaduna com o primeiro aqui discutido, na medida em que não faria sentido utilizar um aplicativo com proteção de dados eficaz se essa ferramenta fosse parceira comercial de outra que não se atentasse detidamente às melhores práticas de proteção de dados e de respeito à privacidade do usuário.

---

[377] "Para oferecer os nossos serviços a você, operamos globalmente. Nos casos em que as leis do seu país permitirem, você nos autoriza a transferir, armazenar e usar seus dados nos Estados Unidos, na Irlanda e em qualquer outro país onde operamos. Em alguns desses países aos quais o Twitter transfere dados pessoais, a privacidade e as leis e regulamentos de proteção de dados com relação a quando as autoridades governamentais podem acessar dados podem variar em relação àquelas no país em que você vive. Saiba mais sobre nossas operações globais e transferência de dados aqui".

[378] "Quando transferimos dados pessoais para fora da União Europeia ou dos países da Associação de Livre Comércio Europeia, garantimos um nível adequado de proteção dos direitos dos titulares dos dados com base na adequação das leis de proteção de dados do país receptor, obrigações contratuais impostas ao receptor dos dados (as cláusulas modelo podem ser solicitadas mediante consulta, conforme descrito abaixo) ou os princípios do Privacy Shield entre UE-EUA e Suíça-EUA".

Em uma abordagem mais pragmática, é interessante ver que o *Twitter* preferiu editar os seus termos de privacidade de modo específico ao contexto europeu a perder aquele mercado pela nova regulamentação imposta. Era de se esperar que, dados o potencial brasileiro para formar vários usuários de internet e a recente vigência da LGPD, com todas as suas novas balizas no tema, o mesmo cenário acontecesse no Brasil.

Contudo, não se encontra uma menção sequer às normas nacionais na política de privacidade do aplicativo, o que demonstra algum grau de despreocupação com as normas nacionais afetas ao tema. É verdade que, se o aplicativo consegue respeitar o paradigma do RGPD, provavelmente também conseguirá fazê-lo em relação à LGPD, mas seria mais interessante que se demonstrasse esse zelo específico com o usuário brasileiro.

O *Skype* não foi aqui analisado, na medida em que utiliza a mesma política de privacidade padronizada para todos os produtos da *Microsoft* – cujo documento é detalhadamente analisado em seção posterior.

O *Viber*[379] estabelece como um dos propósitos do seu tratamento de dados personalizar experiências[380]. No documento, também há referência específica à política de *cookies* do aplicativo, com a indicação de cada ferramenta utilizada, sua finalidade e a respectiva política de privacidade.

Nesse ponto, é de se observar que o *Viber* também aposta na publicidade comportamental de terceiros em sua plataforma a partir dos dados pessoais coletados – em que difere do *WhatsApp*, por exemplo. Desconhecem-se as funcionalidades mais específicas do *Viber* para tecer mais comentários, mas é *prima facie* questionável que um aplicativo de mensagens instantâneas exiba avisos publicitários em sua interface.

Contudo, se a monetização dos dados pessoais coletados pelo aplicativo ficar restrita à exibição dos anúncios em sua plataforma – o que não é simples de se aferir –, essa publicidade pode até ser positiva, na medida em que, de uma ou outra forma, serviria para encerrar o tratamento. Nessa linha, a monetização dos dados pelo *WhatsApp* pode parecer menos transparente, e, nesse sentido, desalinhada com as balizas da boa-fé objetiva estabelecidas pela LGPD.

---

[379] VIBER. Viber Privacy Policy. Disponível em: <https://www.viber.com/terms/viber-privacy-policy/>. Acesso em: 12 abr. 2021.

[380] "Personalizar sua experiência fornecendo conteúdo (como jogos) no Serviço, incluindo publicidade direcionada de serviços Viber e outros serviços de terceiros que acreditamos ser de maior interesse para você; personalização pode incluir decisões automatizadas sobre o que você visualizará e quando, mas assegure-se de que isso não terá efeitos legais sobre você" (tradução livre).

O documento de privacidade do *Tinder*[381] começa com o alerta de utilizar linguagem simples[382]. É exatamente disso que se cuida: muitos aplicativos apostam no *juridiquês* pouco claro e pouco inteligível pelos usuários. A questão, contudo, é que essa frase inicial do aplicativo parece ser desconectada do restante da política de privacidade, que também aposta na pretensa falta de entendimento dos usuários da rede.

Na sequência, chama atenção o fato de o aplicativo dizer que processa os dados de mensagens trocadas por usuários. Embora seja legítima a guarda dos dados de mensagens enviadas – para eventuais demandas judiciais posteriores, por exemplo –, o processamento, nesse sentido genérico do termo – e pouco claro, o que é incompatível com os próprios termos inicialmente prometidos pela empresa –, não parece exatamente justificável; ainda mais quando se considera o contexto de que essas conversas entre usuários do aplicativo geralmente refletem situações amorosas, que naturalmente requerem proteção ainda maior – pode se enquadrar até mesmo no dado pessoal sensível da LGPD, na medida em que geralmente há troca de informações referentes à vida sexual dos usuários.

Quanto à opção "*do not track*" ("não rastrear"), o *Tinder* também informa não ser compatível com a tecnologia, sob a justificativa de que não são todos os dispositivos que têm compatibilidade com a utilidade, que ainda não encontra uma definição consistente. Dentre as finalidades do tratamento dos dados, o aplicativo informa oferecer publicidade comportamental na plataforma. Contudo, a ferramenta mais relevante para a qual o processamento dos dados pessoais é útil é o fazimento do *match* no aplicativo: a plataforma promete encontrar pessoas parecidas com o usuário, justamente a partir de seus *inputs* de dados pessoais.

Ou seja, o tratamento dos dados é o próprio pressuposto para o funcionamento correto da aplicação; nesse caso, não há exatamente muito o que o usuário possa fazer, na medida em que certamente não haverá tanta transparência acerca do funcionamento dessa ferramenta, que é uma vantagem competitiva, verdadeiro segredo empresarial (o porquê de o *Tinder* ser tão famoso nessa aproximação de pessoas e outros aplicativos não serem, por exemplo).

Assim sendo, no bojo do *Tinder*, é possível crer que há maior espaço para a configuração de uma espécie de *consentimento implícito* com o tratamento dos dados pessoais

---

[381] TINDER. Privacy. Disponível em: <https://www.gotinder.com/privacy>. Acesso em: 12 abr. 2021.

[382] "Nós nos esforçamos para ser transparentes na maneira como processamos seus dados. Como usamos muitos dos mesmos serviços on-line que você faz, sabemos que informações insuficientes e linguagem excessivamente complicada são problemas comuns em políticas de privacidade. Adotamos a abordagem exatamente oposta: escrevemos nossa Política de Privacidade e documentos relacionados em linguagem simples. Na verdade, queremos que você leia nossas políticas e entenda nossas práticas de privacidade!" (tradução livre).

quando do *download* da ferramenta, mas desde que isso fique restrito, tanto quanto possível, à finalidade principal da ferramenta de fazer o encontro de usuários semelhantes para relacionamento amoroso. Ao se extravasar esse contexto esperado pelo usuário, está-se diante de uma assimetria do tratamento em relação à tutela adequada da LGPD.

Por sua vez, o *Tumblr*[383] inicia fazendo uma propaganda da plataforma e um *disclaimer*[384], indicando que não se responsabiliza por eventuais coletas excessivas de dados em blogs específicos. Apesar de não ter ficado exatamente claro como um blog específico consegue alterar as configurações da própria plataforma que o hospeda, parece questionável que o aplicativo permita esse tipo de edição, que mais envolveria uma mudança da própria programação do sistema.

Outro ponto relevante do aplicativo diz respeito ao fato de se tratar de um produto da *Oath*, ou seja, também submetido aos termos genéricos da empresa – que são mais bem descritos em seção seguinte. Por fim, também há parte do documento de privacidade que faz expressa referência aos direitos positivados no RGPD e nas normas americanas. Por mais que tenha mais de 3,5 milhões de usuários no Brasil, não há qualquer menção às normas protetivas nacionais.

O *Snapchat*[385] segue a mesma linha inicial do *Tinder*. Uma diferença mais adequada à proteção de dados diz respeito ao fato de o aplicativo disponibilizar uma versão resumida e direta do seu documento de privacidade[386]. Ao falar sobre sua política de *cookies*, o aplicativo salienta que a vedação ao uso dos referidos arquivos de texto que servem ao rastreamento do usuário pode afetar a própria funcionalidade do aplicativo, sem maiores detalhes de como isso se daria – e o texto inicial falava na ausência de "juridiquês" vazio.

Para além de outras ferramentas tradicionais nos aplicativos analisados, o aplicativo também fornece página específica para que o usuário baixe os seus dados armazenados de forma simples, o que é parece aderente à tutela da privacidade que se entende como adequada. De modo geral, os termos de privacidade do *Snapchat* pareceram claros e bem construídos, mas, seguindo a linha de quase todos, estão defasados para os usuários brasileiros – ou, ao menos,

---

[383] TUMBLR. Política de privacidade. Disponível em: <https://www.tumblr.com/privacy/pt>. Acesso em: 12 abr. 2021.

[384] "Uma das excelentes funcionalidades dos produtos do Tumblr é a personalização, sendo que os bloggers têm muita flexibilidade na forma de funcionamento dos seus respetivos blogues. Quando visitas um blogue na nossa rede, esse blogue pode recolher mais informações do que aquelas que nós recolhemos e pode fornecer informações a terceiros com os quais não temos qualquer ligação, incluindo anunciantes"

[385] SNAP. Política de privacidade. Disponível em: <https://www.snap.com/pt-BR/privacy/privacy-policy/>. Acesso em: 12 abr. 2021.

[386] "Tentamos escrevê-la [nossa política de privacidade] sem usar todo aquele 'juridiquês', que muitas vezes ofusca esse tipo de documento".

não estão aproveitando a chance de ganhar notoriedade em uma posição vanguardista de melhor tutela da privacidade, com menções expressas à LGPD, por exemplo.

Há, na verdade, uma pequena seção de listagem de alguns direitos e apontamentos específicos para usuários no Brasil[387]. Dentre eles, o que parece mais relevante é a menção às bases legais para o uso das informações: contrato, legítimo interesse, consentimento (apenas "em alguns casos") ou por obrigação legal, principalmente perante autoridades judiciais. Da leitura dos permissivos apontados na política, é fácil perceber que o legítimo interesse realmente é o que chancela a maior parte do tratamento dos dados no âmbito da aplicação, como era intuitivamente esperando mesmo antes de se iniciar a análise específica.

O *Telegram*[388] começa com dois princípios de privacidade da empresa: (i) não usar os dados pessoais para mostrar anúncios; e (ii) apenas armazenar os dados necessários para o funcionamento do aplicativo "como um serviço de mensagens seguro e rico em recursos" (tradução livre). Atingiu os princípios do menor privilégio no acesso aos dados e do seu uso proporcional em cheio. O aplicativo também informa não usar *cookies* para fins de publicidade.

O ponto negativo fica para o seguinte trecho: "infelizmente, se você não está de acordo com os modestos requisitos do *Telegram*, não será possível para nós fornecer nossos serviços" (tradução livre). Embora não pareça haver muita manobra para a retirada do baixo consentimento exigido – já que, teoricamente, inexiste publicidade comportamental –, seria

---

[387] "Bases para usar suas informações
Seu país só nos permite usar suas informações pessoais quando certas condições se aplicam. Essas condições são chamadas de "bases legais" e, na Snap, normalmente contamos com uma de quatro:
Contrato. Uma das razões pelas quais podemos usar suas informações é porque você já entrou em um acordo conosco. Por exemplo, quando você compra um Filtro Geográfico através de um pedido e aceita nossos Termos de Ferramentas Criativas Personalizadas, precisamos usar algumas de suas informações para coletar pagamentos e nos certificar de que mostramos seu Filtro Geográfico às pessoas certas, no local e horário certos.
Interesse legítimo. Outra razão para usarmos suas informações é porque temos - ou um terceiro tem - um interesse legítimo em fazer isso. Por exemplo, precisamos usar suas informações para fornecer e melhorar nossos serviços, incluindo proteger sua conta, enviar seus Snaps, fornecer suporte ao cliente e ajudar você a encontrar amigos e conteúdo que achamos que irá gostar. Como a maioria dos nossos serviços são gratuitos, também usamos algumas informações sobre você para tentar mostrar anúncios que você vai achar interessantes. Um ponto importante para entender o interesse legítimo é que nossos interesses não superam seu direito à privacidade, então nós só contamos com o interesse legítimo quando pensamos que a maneira como estamos usando seus dados não afeta significativamente sua privacidade ou o que seria esperado por você, ou há uma razão convincente para fazer isso. Explicamos nossas razões comerciais legítimas para usar suas informações em mais detalhes aqui.
Consentimento. Em alguns casos, pediremos consentimento para usar suas informações para fins específicos. Se fizermos isso, nos certificaremos que você possa revogar seu consentimento em nossos serviços ou através de permissões em seu dispositivo. Mesmo que não dependamos de seu consentimento para usar suas informações, podemos pedir permissão para acessar dados como contatos e localização.
Obrigação legal. Podem ser obrigados a usar suas informações pessoais para cumprir a lei, como quando respondemos a um processo judicial válido ou precisamos tomar medidas para proteger nossos usuários".
[388] TELEGRAM. Telegram Privacy Policy. Disponível em: <https://telegram.org/privacy>. Acesso em: 12 abr. 2021.

melhor se o usuário ainda tivesse possibilidade de manifestar sua preferência por algumas revogações. Chancelar o *take ir or leave it* não parece ser a melhor escolha.

Um ponto positivo é para a eliminação automática da conta após 6 meses sem uso, inclusive com a eliminação dos dados porventura armazenados. O único ponto que chamou realmente a atenção é que, lendo a política de privacidade, não foi exatamente possível aferir o modo como o aplicativo aufere lucro; faz-se a ressalva de que não se conhecem exatamente todas as funcionalidades da ferramenta, pois nunca a utilizou de modo explícito.

O *Pinterest*[389] começa de uma forma tradicional para todos os aplicativos, mas diferente do *Telegram*, no sentido de explicitar a personalização do conteúdo[390]. Mais à frente, a informação ainda é mais clara e realista: "Temos um interesse legítimo em veicular anúncios que sejam relevantes, interessantes e pessoais para você, a fim de gerar receita (a prestação deste Serviço custa caro!)".

Afinal, para a empresa conseguir sobreviver com um serviço supostamente gratuito, a contraprestação deve vir indiretamente de outra fonte; no caso, a publicidade comportamental é a fonte legítima mais utilizada pelos aplicativos; há, ainda, aquele compartilhamento para finalidades menos justificáveis, mas isso geralmente aparece nas políticas de privacidade como um mero compartilhamento com parceiros comerciais, um conceito amplo o bastante para abrigar quase qualquer espécie de finalidade no tratamento.

No *Pinterest*, a publicidade comportamental é especialmente relevante, na medida em que, por pressuposto da utilização do aplicativo, o usuário já precisa informar do que gosta ou em que está interessado. Assim, se o usuário gosta de design de interiores, a rotina de programação do *software* mostrará ofertas daquele tipo de serviço ao consumidor, o que, assume-se, atrairá o seu interesse.

No caso do *Pinterest*, portanto, o algoritmo de rastreamento das preferências do usuário nem precisa ser muito sofisticado, na medida em que o próprio usuário já fornece espontaneamente as suas preferências, para a utilização da ferramenta. O grande problema é que se constrói a bolha de relacionamento e interesses: o usuário está interessado em algo e ficará cada vez mais interessado nisso, na medida em que será submetido apenas a anúncios exatamente sobre aquilo.

---

[389] PINTEREST. Política de privacidade. Disponível em: <https://policy.pinterest.com/pt-br/privacy-policy>. Acesso em: 12 abr. 2021.

[390] "Nossa missão é ajudar você a descobrir e fazer o que mais gosta. Para isso, mostramos conteúdo personalizado e anúncios que achamos que serão de seu interesse, com base nas informações que coletamos de você e de terceiros".

Como a aplicação é membro do *Privacy Shield*, só compartilha as informações dos usuários com outras que também tenham o certificado de proteção de dados, sob pena de responsabilidade do próprio aplicativo. Essa constatação é uma segurança extra ao usuário e aderente à tutela da privacidade que se entende como adequada. Além disso, o *Pinterest* é um dos poucos aplicativos analisados compatível com a tecnologia "*do not track*" para os navegadores, o que também é positivo.

O *LinkedIn*[391] exibe de plano um painel de privacidade, com acesso fácil às configurações de privacidade, às perguntas frequentes sobre o assunto e aos aspectos do RGPD. O aplicativo também oferece longa página de explicação sobre sua política de *cookies*, na qual informa não seguir a tecnologia "*do not track*". A política segue de modo transparente e claro, inclusive na sua redação de, a cada seção, colocar exibir um resumo sobre o que será ali discutido. Trata-se de um modo simples de facilitar a compreensão do usuário.

Quanto às cláusulas dispostas no documento, nenhuma chamou particular atenção: a plataforma também aufere renda por meio de publicidade comportamental e processa os dados dos usuários para gerar o encontro entre o empregador e o pretendente a empregado. Assim, não seria factível que a empresa explicasse detalhadamente como ocorre o processamento dos dados nessas circunstâncias, na medida em que se trata de nítida vantagem econômica do *LinkedIn* em face de seus concorrentes. Então, partindo-se dessa premissa, os termos do documento de privacidade do aplicativo realmente pareceram completos, embora sem alusão específica à legislação aplicável.

Por fim, no *WeChat*[392], parece faltar aderência à legislação brasileira. Com efeito, a política de privacidade afirma que o aplicativo retém os dados por até 90 dias da data em que são coletados, mas o Marco Civil da Internet estabelece que o prazo de guarda deve ser de 6 meses. Ou seja, o aplicativo, nesse caso, acaba pecando pela insuficiência do tratamento dos dados, na medida em que os guarda aquém do prazo legal exigido.

Na sequência, o documento apresenta uma relação causal muito clara entre o dado coletado e a respectiva finalidade do processamento, agora inclusive com menções expressas ao RGPD. Ao final, também há tabela clara explicando o prazo de retenção das informações para cada tipo de dado coletado. Tal forma de organização da política de privacidade pareceu a mais transparente dentre todas as analisadas.

---

[391] LINKEDIN. Política de privacidade. Disponível em: <https://www.linkedin.com/legal/privacy-policy>. Acesso em: 12 abr. 2021.

[392] WECHAT. WeChat Privacy Protection Summary. Disponível em: <https://www.wechat.com/mobile/htdocs/en/privacy_policy.html>. Acesso em: 12 abr. 2021.

No mais, os termos de privacidade do aplicativo também pareceram completos, inclusive no tocante à política de *cookies*, o que é aderente à tutela da privacidade que se entende como adequada. Por fim, relevante destacar que a página da política de privacidade também contém o certificado TRUSTe de privacidade, o que indica um filtro a mais no âmbito da proteção adequada dos dados pessoais.

O *Zoom*[393] inicia sua declaração de privacidade indicando os registros das mudanças no documento, na medida em que esse é constantemente atualizado. O aplicativo, cujo uso foi exponencialmente aumentado durante a pandemia de coronavírus, teve suas principais atualizações na política de privacidade justamente durante esse *boom* do uso: em março de 2020, a declaração foi inteiramente revisada "para ser mais legível e transparente"; em julho, adicionaram-se critérios do *TrustArc* e a linguagem do RGPD; em agosto, foram removidas algumas referências à invalidação do *Privacy Shield*. Tal prática, de ser transparente com o usuário acerca das mudanças na política, coaduna com a lógica de transparência da LGPD. E, ao que consta, as mudanças recentemente empreendidas também são mais protetivas aos direitos do usuário.

Na sequência, o documento afirma que a coleta dos dados depende do contexto das interações com o aplicativo, o que parece alinhado à lógica de privacidade contextual e especificamente tutelada à luz do caso concreto. Contudo, chama atenção o fato de que, quando se usa o *Zoom* por meio de titulares de contas – empregador ou escola, por exemplo –, a escolha de como se dá o tratamento dos dados do usuário é remetida ao titular dessas contas. Embora possa fazer sentido, seria melhor que o aplicativo, durante a interface de uso, se comprometesse a informar quais foram as escolhas feitas pelo titular para cada usuário.

Por sua vez, o aplicativo contempla declarações de privacidade específicas para moradores da Califórnia – dada a legislação diversa, embora com lógica semelhante – e para crianças; também há sugestões de links externos para uso do aplicativo por governos. Essas especificidades indicam acertado zelo para com a proteção dos dados pessoais dos usuários, mas o documento voltado para as crianças poderia ser mais transparente e interativo, à luz dos preceitos da LGPD.

Na sequência, há longa tabela esquemática indicando os dados pessoais coletados e os respectivos modos de obtenção, finalidade da coleta e a base legal para tanto. Se todos os aplicativos se utilizassem desse instrumental, a vida dos usuários certamente ficaria mais fácil. Chama atenção o fato de o interesse legítimo ser base legal para todos os tratamentos ali

[393] ZOOM. Zoom Privacy Statement. Disponível em: <https://explore.zoom.us/trust/privacy>. Acesso em: 13 abr. 2021.

elencados (nove), ao passo que o consentimento só é justificativa para dois: ampliação de informações de participantes de evento patrocinado e identificadores persistentes de marketing.

O aplicativo ainda informa que, "como muitas empresas, usamos serviços de publicidade que tentam adaptar os anúncios online aos seus interesses com base nas informações coletadas por meio de cookies e tecnologias semelhantes em nossas páginas de marketing". Contudo, dá a opção de o usuário optar por "não vender minhas informações pessoais" para essa finalidade, o que, pela nomenclatura usada, dá transparência a como é realmente feito o tratamento dos dados.

O documento também elenca os "direitos de privacidade europeus" – quase idênticos aos brasileiros –, que podem ser exercidos pelo usuário com o envio de um e-mail ao provedor. A mesma disposição específica destinada à Europa também existe no bojo da transferência internacional de dados: para países europeus, garante-se que os dados só serão transferidos a outros países que tutelem adequadamente a proteção de dados; para outros casos, os países de destino "podem ter regras de proteção de dados diferentes e menos protetoras do que as de seu país". O Brasil, em tese, deveria guardar semelhança com a regra europeia.

3.3.2 Navegadores e e-mails

Os aplicativos *MS Edge* e *Outlook* não foram aqui analisados, na medida em que utilizam a mesma política de privacidade padronizada para todos os produtos da *Microsoft* – cujo documento é detalhadamente analisado em seção posterior. Isso é, *a priori*, questionável, já que os aplicativos têm funcionalidades diferentes. O mesmo se aplica ao *Gmail* quanto aos termos genéricos da *Google*.

O *Yahoo*[394] tem uma política de privacidade completa e com diversidade de opções intuitivas para que o usuário revogue o consentimento em alguns pontos, inclusive por meio de página específica para painel de controle da privacidade. Como os pontos mais relevantes também são comuns para outros aplicativos, a análise das cláusulas é feita mais adiante no trabalho.

Aqui, porém, vale mencionar que, embora a política de privacidade seja realmente muito completa – o que é aderente à tutela da privacidade que se entende como adequada –, as informações estão um pouco esparsas, o que pode acabar confundindo o usuário nos vários

[394] OATH. Produtos de comunicação. Disponível em: <https://policies.oath.com/br/pt/oath/privacy/products/communications/index.html>. Acesso em: 12 abr. 2021.

hiperlinks exibidos no documento. Seria melhor que as informações de alguns desses links externos estivessem condensados no próprio documento original, para facilitar o entendimento dos consumidores e usuários, dando-lhes transparência mais ativa e efetiva.

Outra crítica é ao fato de que, à semelhança de outras gigantes da tecnologia, a Oath preferiu criar um documento único de privacidade para todos os seus produtos, que não necessariamente guardam estrita semelhança de funcionalidades. Como já se mencionou, o mais correto é que cada software tenha sua política individualizada e alinhada às suas especificidades, com eventuais menções genéricas aos termos compartilhados dentre as demais tecnologias do grupo econômico.

Esse é exatamente o caso do *Mozilla Firefox*[395], que tem uma política própria de privacidade para o navegador, embora haja a indicação de também adotar a política da própria *Mozilla* de forma geral. Seria um bom exemplo a se seguir por aquelas empresas que aderem à ideia de único documento para todos os produtos, pois claramente dá mais transparência e utilidade às informações, o que torna o eventual consentimento pelo usuário certamente mais fiável, além de demonstrar maior adequação à boa-fé objetiva.

A política de privacidade da empresa também pareceu aderente à tutela da privacidade que se entende como adequada – inclusive com explicação sobre o fazimento de telemetria do usuário quando de sua utilização do aplicativo na versão *Android*. Contudo, há muitos links externos no documento, o que acaba retirando a atenção do usuário para aquilo que realmente importa nos termos.

A política de privacidade do *UC Browser*[396] é mais enxuta e incompleta do que as duas anteriores, mas pareceu atender aos requisitos mínimos esperados. Em uma parte relevante, o documento elenca os destinatários dos dados compartilhados para fins de publicidade, bem como as respectivas informações compartilhadas[397]. Na sequência, há indicação expressa das políticas de privacidade de cada respectivo responsável pela publicidade comportamental. Essa transparência em relação a quais são os parceiros comerciais da aplicação

---

[395] MOZILLA. Aviso de privacidade do Firefox. Disponível em: <https://www.mozilla.org/pt-BR/privacy/firefox/>. Acesso em: 12 abr. 2021.

[396] UC BROWSER. Privacy policy. Disponível em: <http://www.ucweb.com/company/privacy/>. Acesso em: 12 abr. 2021.

[397] Veja-se: "O UCWeb Service está conectado a determinadas plataformas de publicidade, incluindo a AdMob pelo Google, a Rede de Público do Facebook e o Intowow ("Terceiros anunciantes"). Informações incluindo tipo e modelo de dispositivo, provedor de rede, tipo de navegador, idioma, nome do pacote, palavras-chave, versão, tipo de sistema operacional, hora e fuso horário, endereço IP do dispositivo, tipo de conexão de rede e localização GPS do dispositivo (somente se você fornecer permissão), e seus identificadores de publicidade para dispositivos móveis, como seu IDFA da Apple ou AAID do Google, serão compartilhados com os anunciantes de terceiros".

para a finalidade do tratamento dos dados coletados, embora seja mais aderente à proteção de dados que se entende como adequada, diverge da média dos aplicativos analisados.

Por fim, o *Google Chrome*[398] também segue a mesma política de privacidade dos demais aplicativos da *Google*. No documento analisado, entretanto, estabelece-se a diferenciação entre modos de navegação comum, anônima e segura. Embora os conceitos possam parecer intuitivos, é de se afirmar que fatos recentes – de a *Google* estar enfrentando um processo bilionário nos Estados Unidos por violação à expectativa de anonimato – demonstram que, no âmbito da tecnologia da informação e de suas naturais dificuldades técnicas de compreensão pela maior parte da população, não há exatamente como se fiar à intuição ou ao aparente significado lógico dos termos[399].

Além disso, há breve explicação sobre extensões e complementos a serem instalados no navegador – e isso é especialmente relevante, pois essas extensões também podem tornar o navegador suscetível a ameaças[400], na medida em que muitas delas não são fornecidas pela própria *Google*, razão por que a empresa diz não se responsabilizar por eventuais falhas na política de privacidade dessas extensões.

É possível concordar com essa justificativa – porque faz sentido –, mas seria melhor que o navegador fizesse uma espécie de filtro de todas as extensões disponíveis para *download* diretamente pelo aplicativo, apenas permitindo a instalação de aquelas que tivessem uma política de privacidade minimamente compatível com a do próprio navegador.

3.3.3 Entretenimento, vídeos e músicas

Inicialmente, importante salientar que não foi possível analisar o aplicativo *RecordTV*, na medida em que o link indicado na loja *Google Play* está inativo e não foram encontradas indicações sobre privacidade na página principal das empresa, o que denota falta de preocupação com o resguardo desse direito fundamental dos usuários.

O *GShow* e o *Globoplay* não foram aqui analisados, na medida em que utilizam a mesma política de privacidade padronizada para todos os produtos da *Globo* – cujo documento é detalhadamente analisado em seção posterior. O mesmo se aplica ao *YouTube*, ao *YouTube*

---

398 GOOGLE. Google Chrome Privacy Notice. Disponível em: <https://www.google.com/intl/en/chrome/privacy/>. Acesso em: 12 abr. 2021.

399 GIZ MODO. Google enfrenta processo nos EUA por rastreamento de dados em navegação anônima. Disponível em: <https://gizmodo.uol.com.br/google-processo-dados-navegacao-anonima/>. Acesso em: 12 abr. 2021.

400 TECHTUDO. Sete riscos de baixar extensões no navegador do PC. Disponível em: <https://www.techtudo.com.br/listas/2020/07/sete-riscos-de-baixar-extensoes-no-navegador-do-pc.ghtml>. Acesso em: 12 abr. 2021.

Kids e ao *Google Music*, quanto aos termos genéricos da *Google*, e ao *Amazon Prime*, quanto aos termos genéricos da *Amazon*.

O aplicativo *Disney+*[401] é submetido à política de privacidade geral da *Disney*, inclusive para seus parques temáticos, navios, hotéis e afins. Seria mais aderente à dinâmica da LGPD que cada escopo de tratamento desses dados contivesse uma política de privacidade específica, mas, nesse caso, o documento pareceu explicativo o suficiente e projetado para efetivamente abarcar todas as plataformas.

Quanto à coleta dos dados, a política informa ser compatível com a tecnologia *do not track*, tendo longa seção para ensinar o usuário a usá-la do modo correto. Além disso, também informa que pode receber informações de "outras fontes confiáveis", embora não haja garantia de que essas fontes iniciais realmente seguem um padrão adequado de privacidade. No tocante ao compartilhamento dos dados, o grande foco é o consentimento do usuário: haverá a disponibilização dos dados a terceiros quando o usuário assim solicitar ou concordar, salvo outras hipóteses legais e de prevenção a fraudes.

Também há seção elucidativa sobre como o usuário pode exercer suas preferências de não tratamento de dados, o que é adequado à lógica de transparência da LGPD. Por fim, para além de conter tópicos apartados para a proteção de dados dos europeus e californianos, há também menção aos brasileiros, que, embora não seja muito explicativa e completa, demonstra algum grau de zelo para com os usuários nacionais[402].

Em relação ao *Twitch*[403], é relevante pontuar que, diferentemente de outras políticas de privacidade, essa informa que o compartilhamento de dados com terceiros é acompanhado de uma notificação ao usuário, que poderá rejeitá-lo. Além disso, o compartilhamento com *terceiros* prestadores de serviço para a plataforma é sujeito aos termos de privacidade gerais do aplicativo, o que é positivo por não terceirizar o risco do tratamento dos dados pessoais.

Quanto às crianças, afirma-se que, "se você tem menos de 13 anos de idade, não use ou acesse os serviços da *Twitch* em nenhum momento e de nenhuma maneira". Sustenta-se que essa verificação, contudo, deveria ser feita logo na tela de abertura do aplicativo, e não somente na política de privacidade, mesmo que colocada, nela, com letras garrafais. Noutro

---

[401] DISNEY. Privacy policy. Disponível em: <https://privacy.thewaltdisneycompany.com/en/current-privacy-policy/>. Acesso em: 13 abr. 2021.
[402] DISNEY. Data protection in Brazil. Disponível em: <https://privacy.thewaltdisneycompany.com/en/current-privacy-policy/data-protection-in-brazil/>. Acesso em: 13 abr. 2021.
[403] TWITCH. Aviso de privacidade. Disponível em: <https://www.twitch.tv/p/pt-br/legal/privacy-notice/>. Acesso em: 13 abr. 2021.

giro, há menção específica a alguns direitos mais gerais de usuários europeus e brasileiros, o que denota zelo com a tutela adequada dos dados pessoais dentro de cada contexto nacional.

Mas, para além disso, o que chama mais atenção nos termos de privacidade é a existência de uma aba de "escolhas de privacidade", em que são dispostas tabelas extremamente explicativas e claras que envolvem relações causais diretas: "se você quiser recusar o processamento de suas informações pessoais, envie o seu pedido aqui", e assim sucessivamente. Nesse aspecto, o aplicativo destoa de praticamente todos os demais analisados no trabalho, na medida em que aposta nas relações diretas e objetivas para dar mais transparência ao usuário sobre o modo de exercer seus direitos, o que é alinhado perfeitamente à lógica da LGPD.

No tocante ao *Likee*[404], há políticas de privacidade diferentes para europeus, estadunidenses e de outras nacionalidades. Embora a LGPD se assemelhe substancialmente ao RGPD, é fato que, na prática, é aplicável a política mais genérica ao Brasil. No primeiro aviso da política, denotando seu caráter adesivo, escreve-se, em letras garrafais, que, "se você não concordar com esta política de privacidade em geral ou com qualquer parte dela, não deve usar serviços do aplicativo".

Para além disso, a política é interessante no aspecto de fazer uma diferenciação entre os dados pessoais coletados com base no consentimento do usuário – perfil, conteúdo gerado por ele, dados faciais, contatos, localização e outros – e aqueles coletados com base nos legítimos interesses do provedor – atividade na rede, provenientes de terceiros, transações, identificadores do dispositivo e de publicidade, metadados, *cookies*. Essa diferenciação é alinhada à transparência esperada, embora os acessos pareçam ser amplos (inclusive dados faciais).

O aplicativo ainda informa não coletar os dados tachados como sensíveis pela lei. Quanto ao compartilhamento de dados com terceiros, a empresa informa que pode proceder a essa espécie de tratamento se obtiver o consentimento implícito do usuário, o que é contrário à LGPD, que exige o consentimento livre, expresso, inequívoco e informado. A mesma previsão existe no bojo dos termos destinados aos europeus, sendo que o RGPD, há bastante tempo, qualifica o consentimento como necessariamente expresso.

Quanto ao aplicativo *Band*[405], também não há maiores comentários, já que os termos de privacidade são muito resumidos e genéricos. Duas cláusulas chamam atenção,

---

[404] LIKEE. Privacy policy. Disponível em: <https://mobile.like.video/live/page-about/policy.html#common>. Acesso em: 13 abr. 2021.

[405] BAND. Termos de Uso de Aplicativo e Política de Privacidade. Disponível em: <https://www.band.uol.com.br/segundatela/politicas.html>. Acesso em: 12 abr. 2021.

contudo: (i) a informação de que a empresa pode usar os dados do usuário coletados por prazo indeterminado, o que parece violar o direito básico de retenção pelo mínimo lapso temporal possível.

E: (ii) a colocação de uma cláusula de não indenizar por eventuais falhas do sistema, inclusive em casos de interceptação, eliminação, alteração, modificação ou manipulação por terceiros. Aqui vale o mesmo comentário feito em outras seções: não é viável que o aplicativo se exima de sua responsabilidade por não ter um sistema eficiente de segurança, transferindo-a inteiramente ao usuário.

O *SBT*[406], por sua vez, inicia afirmando que "acreditamos que você deve estar no controle sobre seus dados pessoais", de modo que a política de privacidade serve "para ajudar você a entender melhor como usamos seus dados pessoais", "demonstrando o nosso compromisso com a boa-fé, segurança, privacidade e transparência". Embora inicie dessa forma interessante, afirma, logo na sequência, se utilizar da metodologia tudo ou nada.

O aplicativo também informa coletar o mínimo necessário de dados para oferecer a melhor experiência dentro da plataforma, para fins publicitários ("a receita oriunda de publicidade permite ao *SBT* continuamente melhorar seus serviços"), de segurança e de personalização dos serviços. Dentro do compartilhamento dos dados com terceiros, afirma-se o respeito à transparência e às finalidades previstas na LGPD. Na sequência, contudo, fala-se serem possíveis outras espécies de compartilhamento desde que se acredite ser razoavelmente necessário para o cumprimento do legítimo interesse da empresa.

No tocante ao consentimento, fala-se que o usuário pode solicitar maiores esclarecimentos sobre o alinhamento de vontades, bem como poderá revogá-lo posteriormente, assumindo o risco de a plataforma deixar de funcionar corretamente. Quanto aos dados de menores de idade, o aplicativo informa ser necessária uma foto do menor para o seu cadastro e alinhamento específico à autorização dos responsáveis para o tratamento ser viável. Parece, contudo, que exigir uma foto exorbita o critério do menor privilégio. Mas, de forma geral, o aplicativo pareceu tutelar adequadamente a privacidade de seus usuários. Afinal, trata-se de uma das poucas ferramentas a fazer menções mais expressas à LGPD.

Os termos do *Now Net e Claro*[407], apesar de enxutos, pareceram bem formulados e alinhados à preocupação com o resguardo da privacidade do usuário[408]. Talvez por se tratar

---

[406] SBT. Política de privacidade. Disponível em: <https://www.sbt.com.br/politica-de-privacidade>. Acesso em: 12 abr. 2021.

[407] NET E CLARO. Política de privacidade. Disponível em: <https://www.net.com.br/static/conteudo/politica-de-privacidade-now-3.pdf>. Acesso em: 12 abr. 2021.

[408] Uma cláusula que demonstra essa política da empresa é a seguinte: "os usuários serão avisados de quais

exatamente de um aplicativo que já recebeu sua remuneração diretamente no passado – quando o usuário assinou a Net ou a Claro –, não haja tanta necessidade de investir em publicidade comportamental, de modo que os dados dos usuários podem ficar mais bem resguardados.

O *Deezer*[409] também faz menção expressa ao RGPD em sua primeira cláusula – embora seja uma empresa brasileira, que teoricamente não precisaria estar preocupada com os usuários europeus –, o que demonstra um mínimo zelo para com os ditames legais de respeito à privacidade dos usuários. Nessa linha de preocupação, há indicação expressa de quem é o controlador dos dados, há cláusula fornecimento de dados para o exterior e há indicação do artigo do Regulamento Europeu que informa os direitos dos usuários.

Em sentido contrário, contudo, também há aquela tradicional cláusula de não responsabilidade por ações de terceiros: "o *Deezer* informa não se responsabilizar pela política de privacidade de rastreadores de *cookies* que permite trabalharem na exibição de anúncios em suas plataformas". Isso parece, como falado em outras seções, um pouco contraditório e pernicioso, na medida em que pode ser o gatilho para que a empresa tenha acesso indevido aos dados do usuário, sem arcar exatamente com o ônus disso, já que o rastreamento de toda a cadeia dos dados pessoais certamente não é simples.

Nesse ponto, o *Deezer* pelo menos indica um link para a página da empresa responsável pelo estudo estatístico de seus anúncios. Outro ponto positivo é o fato de o aplicativo conseguir usar a tecnologia "*do not track*".

O *Spotify*[410] também começa indicando um link para seu centro de privacidade, onde o usuário pode obter maiores esclarecimentos sobre os termos da política de dados. Há expressa menção ao RGPD, o que denota zelo. Também há uma seção que explica o motivo de o aplicativo pretender acesso a algumas informações do dispositivo móvel do usuário[411].

---

informações suas estaremos coletando antes do instante desta coleta, ficando a opção de escolha para fornecimento ou não dessas informações sob responsabilidade do usuário, o qual também terá ciência das consequências de sua decisão".

[409] DEEZER. Política de privacidade e de cookies. Disponível em: <https://www.deezer.com/legal/personal-datas>. Acesso em: 12 abr. 2021.

[410] SPOTIFY. Política de Privacidade do Spotify. Disponível em: <https://www.spotify.com/br/legal/privacy-policy/>. Acesso em: 12 abr. 2021.

[411] Veja-se: "Não iremos aceder a nenhum dos dados pessoais abaixo referidos sem antes obter o consentimento do Utilizador: 1. As fotografias do utilizador – Se o Utilizador nos der autorização para aceder às fotografias ou à câmara do Utilizador, só acedemos às imagens que escolher especificamente partilhar conosco e aos metadados relacionados com essas imagens, tais como o tipo de ficheiro e o tamanho da imagem. Nunca iremos digitalizar ou importar a biblioteca de fotografias ou o rolo de câmara do Utilizador; 2. A localização precisa do dispositivo móvel do Utilizador – Se o Utilizador nos der autorização para aceder à localização precisa, isso vai permitir-nos utilizar o GPS ou Bluetooth do Utilizador para fornecer funcionalidades do serviço Spotify que necessitem de localização. Tenha em atenção que isto não inclui o seu endereço IP. Utilizamos o endereço IP do Utilizador para determinar a localização não precisa como, por exemplo, em que país se encontra, de forma a cumprir os nossos acordos de licenciamento; 3. Dados de voz do Utilizador – Se o Utilizador nos der autorização, podemos aceder aos comandos de voz recolhidos através do microfone do dispositivo do Utilizador, para permitir que este interaja

Os acessos parecem excessivos e desproporcionais em relação aos fins pretendidos ordinariamente pela aplicação. Contudo, desconhecem-se maiores funcionalidades do aplicativo, de modo que não pode fazer uma análise mais crítica. Outra cláusula, também presente em outros aplicativos, que chama atenção é a que prevê a possibilidade de retenção dos dados "necessários" caso o usuário exclua sua conta do aplicativo, mas ainda tenha algum débito com a empresa.

Ora, nada mais legítimo do que a empresa poder cobrar as suas dívidas, mas o conceito de "dados necessários" parece um pouco fluido e mereceria maior detalhamento, isto é, parece realmente necessário que sejam mantidos alguns dados bancários e outros menores que permitam a cobrança, mas não dados de rede social, por exemplo. Contudo, de modo geral, a política de privacidade do *Spotify* pareceu de fácil compreensão, na medida em que organizada sob o formato de várias tabelas esquemáticas.

Quanto ao *Palco MP3*[412], também importante frisar a menção expressa ao Marco Civil da Internet, o que denota especial zelo no contexto brasileiro, em que os provedores de aplicações não parecem muito transparentes quanto ao respeito às orientações legais de privacidade.

Segundo o documento, o aplicativo acessa diversos dados dos usuários[413]. Contudo, não há maiores explicações dos motivos específicos de acesso a cada um desses dados. E, de modo geral, a política de privacidade também é vaga, na medida em que o documento é eminentemente voltado aos demais termos de uso que não a própria privacidade.

O *TikTok*[414] começa direcionando o documento às políticas de privacidade específicas para cada país: Alemanha, Rússia, Índia, outros países da União Europeia, Estados Unidos e o residual. O Brasil se insere nessa última categoria, mas há, ao final, seção destinada a direitos específicos de usuários brasileiros, com menção ao controle parental e com a listagem genérica de todos os direitos da LGPD, em aparente tradução da lei. Não há, contudo, mais informações sobre como o usuário exercitará cada direito seu.

---

com o serviço Spotify através de voz. Tenha em atenção que o Utilizador poderá sempre desligar a funcionalidade de microfone; e, 4. Contatos do Utilizador – Se o Utilizador nos der autorização para acedermos aos contatos, podemos aceder aos contatos individuais armazenados no dispositivo para ajudar o Utilizador a encontrar amigos que utilizem o Spotify".

412 PALCO MP3. Termos de privacidade e política de privacidade. Disponível em: <https://www.palcomp3.com/aviso_legal.htm>. Acesso em: 12 abr. 2021.

413 "A. Identificadores anônimos de publicidade do dispositivo, atributos do dispositivo móvel e aplicativos instalados no respectivo aparelho; B. Dados dos sensores do aparelho; C. Dados anônimos de localização do aparelho por meio de GPS ou rede celular".

414 TIKTOK. Privacy Policy. Disponível em: <https://www.tiktok.com/en/privacy-policy>. Acesso em: 12 abr. 2021.

Um ponto negativo é a afirmação genérica, na seção destinada aos direitos dos usuários, de que "você pode ter direitos em relação a suas informações", sem maiores comentários ou detalhamentos. À exceção desse ponto, contudo, a política de privacidade do aplicativo pareceu detalhada e completa.

O *Vigo*[415] segue exatamente a mesma linha detalhista do *TikTok* – inclusive com cláusulas parecidas[416]. Um ponto relevante é o fato de que o aplicativo considera como crianças os usuários com menos de 16 anos – um patamar elevado em relação aos concorrentes, que costumam fixar a idade de 13 anos. Isso implica dizer que, ao tomar conhecimento de que o usuário tem menos do que 16 anos, o aplicativo automaticamente excluirá as informações da pessoa, bem como encerrará sua conta.

Os termos de privacidade do *Netflix*[417] também dispensam maiores comentários, na medida em que perfeitamente alinhados a todos os aqui analisados. Chama atenção a cláusula que explica o motivo de se ter acesso à localização do dispositivo[418]. Com efeito, mesmo com a explicação, não parece justificável o acesso à localização precisa do *hardware* com a única ideia de se manter a *bolha* do usuário, sobretudo diante da minimização do acesso aos dados pessoais.

Outro ponto peculiar é o *disclaimer* da empresa quando do acesso à plataforma por *hardwares* "pouco convencionais"[419]. É claro que esses dispositivos eletrônicos demandam critérios próprios de privacidade, mas isso não justifica que o aplicativo tente se eximir de qualquer responsabilidade. Por sorte, esses dispositivos têm menor propensão de violação à privacidade dos usuários do que os celulares, mas ainda mereceriam maior cuidado pela empresa. Um aspecto positivo, contudo, é o aplicativo fazer longa explicação sobre o seu uso de *cookies*, inclusive ensinando o usuário a desligar todas as opções previamente definidas de rastreamento na internet.

---

[415] VIGO. Vigo Política de privacidade. Disponível em: <http://www.vigovideo.net/hotsoon/in_app/privacy_policy/>. Acesso em: 12 abr. 2021.

[416] No que tange à publicidade comportamental, há a previsão de que, "com relação a anúncios na tela, anunciantes e redes de publicidade que exigem que os dados selecionem e veiculem anúncios para você e outras pessoas. Não compartilharemos seus detalhes de contato com nossos parceiros de negócios para que eles não entrem em contato diretamente com você, mas compartilharemos outras informações para que eles possam sugerir ofertas adequadas às suas necessidades".

[417] NETFLIX. Declaração de privacidade. Disponível em: <https://help.netflix.com/legal/privacy>. Acesso em: 12 abr. 2021.

[418] "Oferecer conteúdo localizado, oferecer recomendações personalizadas e customizadas de filmes e séries que, na nossa avaliação, poderiam ser do seu interesse, determinar o seu provedor de serviços de Internet e ajudar nossa equipe a responder de forma rápida e eficiente às suas dúvidas e solicitações".

[419] Veja-se: "você pode acessar o serviço Netflix por meio de plataformas como videogames, smart TVs, aparelhos móveis e decodificadores e diversos aparelhos com conexão à Internet. Esses sites e plataformas têm políticas de privacidade e dados, declarações de privacidade, termos e avisos de uso separados e independentes, e recomendamos que você os leia atentamente".

O *Shazam*[420] não possui termos de privacidade próprios, pois o aplicativo está submetido à política de privacidade padronizada dos produtos da *Apple*. Por essa razão, não foram avaliados os termos em detalhes, na medida que não eram exatamente aplicáveis às funcionalidades oferecidas pelo aplicativo. Assim, subsiste a crítica à empresa, para que tente desenvolver uma política de privacidade especificamente projetada para cada de seus produtos, o que é mais alinhado às necessárias especificidade e transparência dos termos.

3.3.4 Comer e beber

A política de privacidade do *Ifood*[421] chama atenção por uma cláusula inicial: "para fins da lei n° 12.965 de 2014 (Marco Civil da Internet), ou qualquer lei que venha substituí-la, a localização fornecida será considerada como dado cadastral". É provável que essa informação esteja ali posta como uma forma de o aplicativo – provedor de aplicações, por conceito – se exonerar do encargo de fornecer essa informação se requerido judicialmente, na medida em que o STJ entende que os provedores de aplicação só são obrigados a fornecer dado de IP para fins de identificação de usuário de internet (art. 15 do Marco Civil)[422].

Por sua vez, falta clareza no conceito de "nível compatível" de proteção mencionado pela política de privacidade para o compartilhamento de dados – e, em verdade, a política de privacidade do *IFood* nem pareceu resguardar a privacidade de seus usuários com tanta rigidez assim[423]. Há uma lista geral das categorias de *cookies* utilizadas, mas também existe o aviso genérico de que algumas funcionalidades do aplicativo podem deixar de funcionar se o usuário optar por revogar alguns dos *cookies*. Seria melhor se houvesse uma relação causal direta: *se você deixar de nos fornecer esse cookie X, a função Y não funcionará*. Essa *ameaça* genérica tende a dissuadir o usuário de manifestar seu consentimento de modo livre, que é um direito básico seu.

Por pressuposto – já que se trata de um aplicativo próprio de vendas –, o documento explicita que a ferramenta não se utiliza de *targeting* no escopo de publicidade comportamental de terceiros, mas indica que as informações pessoais coletadas podem ser relevantes para que

---

[420] APPLE. Apple Customer Privacy Policy. Disponível em: <https://www.apple.com/legal/privacy/br/>. Acesso em: 12 abr. 2021.
[421] IFOOD. Política de privacidade. Disponível em: <https://www.ifood.com.br/privacidade>. Acesso em: 12 abr. 2021.
[422] BRASIL. Superior Tribunal de Justiça, REsp nº 1.342.640/RS, Rel. Min. Nancy Andrighi, DJe 14/02/2017.
[423] O documento também fala que o aplicativo pode "compartilhar as informações com parceiros do iFood, para fins de desenvolver campanhas de marketing mais relevantes para interessados nos produtos do iFood. O iFood somente compartilhará dados com parceiros que possuírem política de privacidade que ofereça níveis compatíveis de proteção àquele oferecido por esta política".

o aplicativo promova propaganda específica sua direcionada ao usuário, com base em suas características previamente mapeadas e analisadas.

Por fim, também peculiar o seguinte trecho do documento: "utilizamos o moderno princípio de *privacy by design*, respeitando a sua privacidade e protegendo seus dados nos nossos processos internos como um todo". Ora, uma afirmação que, embora adequada do ponto de vista conceitual e abstrato, carece de maiores detalhamentos concretos, sendo, por isso, genérica e vazia.

O *Rappi*[424] inicia com uma cláusula de não indenizar abusiva por si só e, por isso, inócua[425]. Ora, nenhum sistema de segurança é intransponível; contudo, as falhas não podem ser imputadas ao titular dos dados, mas ao *software* que não conseguiu geri-los corretamente. Se fosse simples assim, bastaria que qualquer pessoa criasse um banco de dados simples e sem preocupações adequadas, com a proteção mínima possível, e colocasse a observação de que não se responsabilizaria por falhas. Se esse tipo de pretensão de limitação da responsabilidade fosse válido, ninguém investiria em sistemas de segurança da informação, mas tão somente em cláusulas de não indenizar.

Outro ponto relevante é o fato de o aplicativo requerer o consentimento do usuário para que seus dados sejam transferidos "a qualquer país ou servidor em outro país", sem nenhuma preocupação aparente com a segurança dos dados dos usuários nesses destinos. Nessa linha, há descompasso com o requisito de paridade internacional na tutela dos dados pessoais insculpido na LGPD.

Quanto ao *Zé Delivery*[426], é de se destacar a exibição inicial de um quadro-resumo com os principais aspectos da política: identificação do controlador dos dados, quais dados são coletados e para que são utilizados, com quem são compartilhados e o que os receptores fazem com eles, como são protegidos, por quanto tempo são mantidos e os principais direitos dos titulares. Para além disso, há menções expressas aos direitos da LGPD, embora sem clareza sobre como exercê-los, e também menções à lógica de segurança insculpida no Decreto nº 8.771/2016. Nessa esteira, o aplicativo, principalmente pela disponibilização de um quadro-

---

[424] RAPPI. Aviso de Privacidade e Políticas de uso das Informação utilizadas pela Rappi. Disponível em: <https://legal.rappi.com/brazil/aviso-de-privacidade-e-politicas-de-uso-das-informacao-utilizadas-pela-rappi/?_ga=2.167336379.427143798.1555076488-278939625.1555076488&_gac=1.195807640.1555076488.EAIaIQobChMI5Ib7qNfK4QIVEoSRCh3KDAUUEAAYASAAEgKlevD_BwE>. Acesso em: 12 abr. 2021.

[425] "Considerando que nenhum sistema de segurança é absolutamente seguro, a RAPPI se exime de quaisquer responsabilidades por eventuais danos e/ou prejuízos decorrentes de falhas, vírus ou invasões do BANCO DE DADOS na PLATAFORMA".

[426] ZÉ DELIVERY. Política de Privacidade. Disponível em: <https://www.ze.delivery/privacy>. Acesso em: 13 abr. 2021.

resumo no começo da política, acaba ganhando notoriedade no tocante à proteção dos dados pessoais de seus usuários, ao menos quanto ao requisito de necessária transparência.

O *Ifood*, por exemplo, afirma que só transfere dados a outros países – já delimitados entre Europa, Estados Unidos e América Latina – se houver compatibilidade com o nível de proteção de dados brasileiro, o que é o requisito legal. Embora seja difícil aferir essa compatibilidade na prática, ao menos a pretensão é boa e mais adequada do que a do *Rappi*, que não parece se preocupar com os direitos de seus usuários.

O *McDonalds*[427] segue a mesma linha de inserir uma cláusula de não indenização por falhas em seus sistemas informáticos[428]. Outra cláusula interessante versa sobre a proteção a direitos autorais[429]. No ponto que reverbera no cerne do presente trabalho, é particularmente desalinhado com a lógica da LGPD o fato de a empresa considerar que informações voluntariamente fornecidas, só por assim o serem, não merecem tutela mais estrita.

Também é inadequada a cláusula de eleição da lei mexicana como a aplicável a eventuais conflitos judiciais. Certamente é aquela cujo direito material é o mais benéfico à empresa. Esse tipo de cláusula também não merece maior destaque, pois é considerada absolutamente inválida no Brasil, na medida em que não teve o consentimento expresso do usuário, como exige a LINDB.

O *Tudo Gostoso*[430] não merece comentários adicionais, à única exceção do fato de que é outro aplicativo que promove o acesso à localização do aparelho. Ou seja, ao dar o consentimento para essa permissão específica, o usuário está consentindo com os termos de privacidade de outra empresa também, o que pode não ser exatamente o mais adequado aos ditames da LGPD.

O *Uber Eats*[431] utiliza o mesmo documento de privacidade do que o *Uber* para transporte de passageiros. Nesse caso, até parece aceitável, na medida em que as funcionalidades são, de certa forma, compatíveis. Também há referência há um documento

---

[427] MCDONALD'S. Política de Privacidad. Disponível em: <https://api-discover-mcd.gigigoapps.com/app/terms?country=MX&language=en>. Acesso em: 12 abr. 2021.

[428] Com a ressalva de que "a limitação ou exclusão não se aplicará na medida em que as leis aplicáveis não permitam tal limitação ou exclusão de responsabilidade por danos incidentais ou consequenciais".

[429] "A Arcos não é obrigada a tratar qualquer informação voluntária como confidencial, e não será responsável por quaisquer ideias livremente sugeridas para o seu negócio (incluindo, sem limitação de ideias, produtos ou publicidade) e não assumirá qualquer responsabilidade ou ônus por causa de quaisquer semelhanças que possam surgir".

[430] TUDO GOSTOSO. Terms. Disponível em: <https://www.tudogostoso.com.br/mobile/pages/terms.html>. Acesso em: 12 abr. 2021.

[431] UBER. Política de Privacidade. Disponível em: <https://privacy.uber.com/policy/>. Acesso em: 12 abr. 2021.

específico de política de *cookies*[432], em que há detalhada explicação sobre o funcionamento desses arquivos e lista de todos os tipos de *cookies* utilizados pelo aplicativo.

Em específico – e diferente dos outros termos analisados –, há uma lista específica de *cookies* para celulares, que "usam várias tecnologias para fornecer anúncios para celular relevantes, acompanhar o desempenho e a eficiência das campanhas de marketing para celular ou de anúncios para celular": *Google, Adobe* e *Tune*. Outro ponto que chama a atenção é o alargado prazo de armazenamento dos dados: 7 anos. Isso não parece exatamente adequado à tutela que visa à minimização do privilégio e do tratamento.

Também há seção especificamente destinada aos usuários da União Europeia, mas sem nenhuma previsão realmente diferente e relevante. De um modo geral, os aplicativos parecem não se envolver com publicidade de terceiros, o que até mesmo é natural, na medida em que já possuem intrínseca natureza econômica – transporte de passageiros, do qual a *Uber* angaria porcentagem para si, e transporte de alimentos de restaurantes específicos, dos quais a *Uber* também angaria porcentagem e ainda cobra a taxa de entrega.

Ou seja, os interesses econômicos da empresa estão plenamente satisfeitos, razão por que não haveria real necessidade de se empreender publicidade comportamental para fins de manutenção de um serviço gratuito. O que há, no *Eats*, é a publicidade dentro da própria plataforma, a partir de gostos já manifestados anteriormente pelo usuário: quem costuma pedir pizza de uma loja especificamente receberá avisos de que aquele determinado estabelecimento tem *promoções* no dia.

Por fim, o *Foursquare*[433] não estabelece regras muito diferentes das aqui já analisadas. De mais relevante, o aplicativo informa que: "cumprimos os *Self-Regulatory Principles for Online Behavioral Advertising da Digital Advertising Alliance* ('DAA'). Atualmente, no entanto, não cumprimos sinais *Do Not Track* ('DNT') de navegadores ou de outros mecanismos semelhantes". Também há dicas de como proceder ao efetivo cancelamento da publicidade baseada em interesses, inclusive com o *download* do aplicativo AppChoices.

3.3.5 Infantis e jogos

[432] UBER. Cookie policy global. Disponível em: <https://www.uber.com/legal/privacy/cookies/en/>. Acesso em: 12 abr. 2021.

[433] FOURSQUARE. Foursquare Labs, Inc. Política de Privacidade. Disponível em: <https://pt.foursquare.com/legal/privacy>. Acesso em: 12 abr. 2021.

Quanto à política de privacidade do *Garena*[434], embora se desconheçam todas as características do jogo, *a priori* parece excessivo que um aplicativo de jogos tenha acesso à exata localização do usuário, ainda mais quando isso é posteriormente associado à publicidade comportamental[435]. No mais, não há maiores comentários a serem feitos, mas apenas uma crítica quanto à falta de transparência e de detalhamento dos termos de privacidade. Para um aplicativo que tem mais de 81 milhões de usuários no Brasil, deveria haver mais transparência.

O *Subway Surfers*[436], a seu turno, pareceu preocupado com as obrigações impostas pelo RGPD, na medida em que há diversas referências expressas ao regulamento europeu em cláusulas da política de privacidade. Há, inclusive, uma lista de todas as empresas de publicidade que recebem os dados coletados dos usuários, com indicação do respectivo link da política de privacidade. Como o aplicativo tem o público majoritário formado por crianças, há uma previsão específica sobre o tratamento de dados infantis[437].

No tocante à transferência internacional de dados, a política de privacidade informa que o aplicativo só envia os dados para instituições certificadas pelo *Privacy Shield*, outra espécie de selo de qualidade de empresas da área.

De modo semelhante, o *Meu Talking Tom 2*[438] informa uma lista enorme de fornecedores que fazem o processamento dos dados coletados para fins de publicidade comportamental, com a promessa de que o usuário pode revogar o consentimento específico previamente concedido a qualquer deles. Especificamente, a política informa que o aplicativo não coleta informações pessoais de modo amplo[439].

---

[434] GARENA. 111dots Studio Privacy Policy. Disponível em: <http://ff.garena.com/policy.html>. Acesso em: 12 abr. 2021.

[435] "Nossos aplicativos móveis podem coletar informações precisas sobre a localização de seu dispositivo móvel usando tecnologias como GPS, Wi-Fi, etc. Nós coletamos, usamos, divulgamos e / ou processamos essas informações para um ou mais objetos, incluindo, sem limitação, localização serviços baseados em você solicitados ou para entregar conteúdo relevante para você com base em sua localização ou para permitir que você compartilhe sua localização com outros usuários como parte dos serviços em nossos aplicativos para dispositivos móveis" (tradução livre).

[436] KILOO GAMES. Subway Surfers Privacy Policy. Disponível em: <http://www.kiloogames.com/pdf/subway-surfers-privacy-policy.pdf>. Acesso em: 12 abr. 2021.

[437] "Com base nas informações de idade e nas configurações do dispositivo, a Kiloo não processa dados pessoais de crianças abaixo do limite mínimo de idade que é prescrito pela legislação nas jurisdições individuais para publicidade comportamental. Se esses dados pessoais tiverem sido processados sem o conhecimento da Kiloo, a Kiloo, imediatamente após tomar conhecimento do incidente, tomará imediatamente medidas razoáveis para interromper tal processamento e excluirá prontamente quaisquer dados dos registros da Kiloo" (tradução livre).

[438] OUTFIT7. Política de privacidade para aplicativos. Disponível em: <https://outfit7.com/privacy/pt/>. Acesso em: 12 abr. 2021.

[439] "Quaisquer informações pessoais sobre você por meio de nossos Aplicativos, com exceção apenas dos identificadores persistentes (como IDFA, IDFV, ID de publicidade e endereço IP). Identificadores persistentes são identificadores que não o identificam pessoalmente, mas que podem identificar exclusivamente seu dispositivo. Algumas legislações (tais como a dos EUA) podem tratar como informações pessoais as informações que identifiquem o seu dispositivo exclusivamente".

Um ponto intrigante é a recomendação de que não se coloque o nome verdadeiro da criança como o apelido do animal virtual objeto do jogo – contudo, essa recomendação não está expressa na interface do próprio aplicativo, mas só na política de privacidade, que quase nunca é acessada pelos responsáveis pela criança.

Também há preocupação específica com a publicidade voltada aos "usuários que não passaram no filtro de idade" da plataforma, na medida em que são desativados os recursos que permitem uma possível coleta e compartilhamento de informações pessoais identificáveis de usuários com menos de 13 anos, à exceção daqueles identificadores persistentes. Nesse sentido, o aplicativo informa ter uma "reputação familiar".

Quando o usuário informa ter menos de 13 anos, não lhe é exibida qualquer publicidade comportamental e também não é criado perfil de rastreamento do usuário. Ainda assim, contudo, os termos de privacidade dão a entender que as informações das crianças são compartilhadas com os parceiros de publicidade. Nesse ponto, o documento tenta estabelecer uma cláusula de não indenizar[440].

Um ponto extremamente relevante e positivo é que "a OUTFIT7 é membro do Programa PRIVO Kids Privacy Assured ("o Programa") para a Certificação COPPA Safe Harbor. A PRIVO é uma organização independente e terceirizada, comprometida a proteger as informações pessoais das crianças que são obtidas on-line".

A desenvolvedora do aplicativo também "participa do programa de certificação ePrivacyApp ("o Programa"), que é uma organização independente especializada em proteção de dados digitais". É interessante e, ao mesmo tempo, aderente à tutela da privacidade que se entende como adequada a iniciativa da desenvolvedora do *software*. Sustenta-se que todos os demais desenvolvedores deveriam se espelhar nessas diretrizes, que efetivamente parecem adequadas aos paradigmas de *privacy by design* e *privacy by default*.

Na sequência, outro ponto positivo é haver longa lista de empresas responsáveis pela leitura e processamento dos dados pessoais para fins de publicidade comportamental, com a indicação da respectiva política de privacidade e indicação de que seria possível promover o *opt-out* de todas. A política de privacidade também ensina o usuário a utilizar o seu dispositivo na função "não rastrear", o que impede, por conceito, a leitura de informações com a finalidade de fazer o *profiling* do usuário. Os termos do documento pareceram aderentes à tutela da

[440] "Não podemos ser os responsáveis caso eles violem os compromissos que assumiram conosco em relação à coleta de informações. Em caso de tais violações, você concorda que nossas obrigações se limitam aos valores que formos capazes de receber como indenização pelas violações de nosso parceiro de publicidade".

privacidade que se entende como adequada, embora sem nenhuma alusão direta à legislação aplicável.

O *Pou*[441] segue a mesma linha de recomendar que o apelido do usuário seja diferente de seu nome real, mas essa informação, aparentemente, só consta na política de privacidade, e não na interface do próprio aplicativo – o que dificulta sobremaneira a sua consecução na prática.

O aplicativo também informa não suportar a tecnologia de não rastreamento. Como um dos poucos pontos positivos do documento de privacidade está a listagem específica de todos os provedores utilizados para fins de publicidade, com os respectivos links de política de privacidade: *AdMob* do *Google*, *AdColony* e *Selva*. Outra vantagem é possibilidade de vedação à exibição de publicidade personalizada no aplicativo.

O *Fifa*[442] inicia seu documento de privacidade informando participar do *Privacy Shield* e ser detentor do selo TRUTe de boas práticas para o resguardo da privacidade de seus usuários. Outro ponto interessante é que o aplicativo informa não divulgar intencionalmente a identificação de informações pessoais diretamente de crianças menores de 18 anos para terceiros independentes, mesmo que haja consentimento – ou seja, o critério etário parece diferente daquele usado por outros aplicativos, que normalmente seguem o patamar de 13 anos. Outra observação de relevo é a indicação de uma autoridade específica que cuida da privacidade de usuários brasileiros, que curiosamente é sita no México.

No tocante ao *Angry Birds*[443], parece desalinhada com a lógica da LGPD a cláusula de que "a Rovio não controla que anúncios específicos são mostrados em nossos jogos (isso é controlado pelas redes de anúncio), mas proibimos determinados tipos de anúncios". Nesse aspecto, esse *disclaimer* ganha especial relevância quando se considera que a maior parte do público do jogo é infantil, ou seja, *a priori* não estão estabelecidas restrições claras à publicidade comportamental infantil – "determinados tipos de anúncios" é um conceito vago para um direito tão importante.

Pela sua política de privacidade, o *Candy Crush*[444] segue a mesma linha do *Subway Surfers*, ao também expressar que, enquanto utiliza o jogo, o usuário consente com o tratamento de seus dados. E a revogação só é possível se acompanhada da própria desinstalação do

[441] ZAKEH. Privacy Policy. Disponível em: <http://help.pou.me/privacy-policy.php>. Acesso em: 12 abr. 2021.
[442] ELECTRONIC ARTS. Privacy and Cookie Policy. Disponível em: <https://tos.ea.com/legalapp/WEBPRIVACY/US/en/PC/>. Acesso em: 12 abr. 2021.
[443] ROVIO. Rovio Privacy Notice. Disponível em: <https://www.rovio.com/privacy>. Acesso em: 12 abr. 2021.
[444] KING. Privacy Policy. Disponível em: <https://king.com/privacyPolicy>. Acesso em: 12 abr. 2021.

aplicativo. O aplicativo informa ter sido projetado apenas para a utilização por adultos, em razão do que exibe uma tabela com as classificações indicativas para cada país.

A tabela também serve para explicitar os usuários para os quais o aplicativo não coleta informações pessoais para fins de publicidade. O documento também ensina o usuário a ajustar as suas preferências para publicidade baseada em interesse, inclusive com os aplicativos específicos já aqui mencionados. Nessa linha, há transparência na relação de consentimento informado. Não necessariamente o consentimento tem as outras adjetivações legais, mas parece, no mínimo, ser informado.

Os aplicativos *Demo Minecraft* e *Minecraft* utilizam a mesma política de privacidade dos aplicativos da *Microsoft*, que já fora aqui analisados e, por isso, dispensam maiores comentários. Fica a crítica, contudo, a essa atuação, já que os serviços são absolutamente distintos. E, noutro espeque, é também relevante pontuar que deveria haver uma diferenciação nas políticas de privacidade entre as versões paga e gratuita, na medida em que os critérios de monetização dos dados pessoais são diversos. Apenas não faz sentido haver discriminação se se assumir que a versão gratuita não monetiza dos dados pessoais, provavelmente por auferir seus lucros a partir da própria versão paga da aplicação. Essa informação, contudo, não é clara na política.

Uma das principais funcionalidades do *Pokémon Go*[445] é promover a interação do usuário com uma espécie de realidade aumentada. Por essa razão, é sabido que o aplicativo utiliza dados de geolocalização, havendo uma explicação expressa da política de privacidade para justificar a necessidade de coleta[446]. Não há outros pontos que mereçam destaque.

A desenvolvedora do *Fruit Ninja*[447] utiliza um rótulo de *Child Safe App* para alguns de seus aplicativos, o que indica que ele foi criado com segurança para crianças como uma prioridade, não tendo publicidade, coleta de dados, compras no aplicativo e links para sites ou aplicativos externos.

O documento também contempla longa lista de parceiros de negócios com os quais o aplicativo ativamente compartilha informações de usuários e dados de uso, com a respectiva

---

[445] NIANTIC. Niantic Privacy Policy. Disponível em: <https://nianticlabs.com/privacy/en/>. Acesso em: 12 abr. 2021.

[446] "Nossos serviços incluem jogos baseados em localização cuja característica principal é fornecer uma experiência de jogo ligada à sua localização no mundo real, por isso precisamos saber onde você está para operar esses jogos para você e planejar a localização dos recursos do jogo (por exemplo PokéStops no Pokémon GO). Identificamos sua localização usando uma variedade de tecnologias, incluindo GPS, os pontos WiFi que você está acessando o Serviço e a triangulação de torres móveis / celulares" (tradução livre).

[447] HALFBRICK. Privacy Policy. Disponível em: <https://docs.halfbrick.com/PrivacyPolicy.htm>. Acesso em: 12 abr. 2021.

política de privacidade. Os termos de privacidade do *Paint Pop 3D*[448] não merecem comentário adicionais, na medida em que perfeitamente alinhados a todos os demais aqui avaliados, com a exceção ao fato de conterem poucos detalhes.

O documento de privacidade do *GTA*[449] parece, logo de início, transparente, ao criar seção específica para falar sobre as consequências de se recusar a fornecer informações pessoais: limitar a habilidade para participar de algumas atividades, tais como sorteios, ou uso de certos serviços online.

A política também apresenta uma lista daqueles anunciantes terceirizados que participam da plataforma, bem como direciona para o respectivo link da política de privacidade, também ensinando o usuário a proceder à revogação do consentimento. À exceção disso, não há maiores comentários relevantes.

A política de privacidade do *Hopping Ball*[450] é pouco detalhada e incipiente, razão por que não parede aderente às normas da LGPD. O *Buddy Toss*[451] segue exatamente a mesma linha de generalidade e acesso amplo a dados, ou seja, sem preocupação com o menor privilégio e com o efetivo teste de proporcionalidade para o tratamento dos dados pessoais estritamente necessários e adequados à finalidade pretendida pela aplicação[452].

3.3.6 Finanças e crédito

O *Banco do Brasil*[453] também não investe em uma política de privacidade muito detalhada, limitando-se a dizer que, quando do relacionamento com terceiros, preza pela contratação de empresas que mantenham o mesmo padrão de confidencialidade e privacidade

---

[448] GOOD JOB. Good Job Games Privacy Policy. Disponível em: <https://goodjobgames.com/policy.html>. Acesso em: 12 abr. 2021.

[449] ROCKSTAR GAMES. Política de Privacidade. Disponível em: <https://www.rockstargames.com/privacy?locale=br>. Acesso em: 12 abr. 2021.

[450] ONEPEAR. Política de Privacidade Jogos Globais. Disponível em: <https://superiorzzr.tumblr.com/post/177787450452/privacy-policy9>. Acesso em: 12 abr. 2021.

[451] BIGDOG GAMES. Privacy Policy. Disponível em: <http://www.crystalrover.com/privacy-policy.html>. Acesso em: 12 abr. 2021.

[452] Em específico, o documento deste aplicativo indica que o usuário "reconhece e concorda que as empresas de publicidade que veiculam anúncios para a Bigdog Games podem combinar as informações coletadas com outras informações coletadas independentemente de outros serviços ou produtos. Essas empresas coletam e usam informações sob suas próprias políticas de privacidade. Essas tecnologias de veiculação de anúncios são integradas aos Serviços da empresa; se o usuário não quiser se sujeitar a essa tecnologia, não pode usar nem acessar o aplicativo. Embora a Bigdog Games tome medidas comercialmente razoáveis para instruir essas empresas de publicidade a cumprir os termos e condições desta Política de Privacidade, não tem acesso ou controle de tecnologias de terceiros" (tradução livre).

[453] BANCO DO BRASIL. Política de Privacidade. Disponível em: <https://www.bb.com.br/pbb/pagina-inicial/voce/politicas-de-uso-e-privacidade#/>. Acesso em: 12 abr. 2021.

do que o próprio Banco. Poderia haver mais especificidade na relação causal direta, embora seja positivo o aplicativo se preocupar em explicar as solicitações[454].

O aplicativo da *Caixa* dispensa, por ora, maiores comentários, na medida em que é analisado na seção destinada aos *softwares* governamentais, já que a empresa segue política única e geral para toda sua linha de produtos.

No que tange à política de privacidade do *Itaú*[455], duas finalidades elencadas para o tratamento dos dados chamam a atenção. Isso sem falar do acesso à localização geográfica, que é no mínimo questionável no âmbito das funcionalidades esperadas para o aplicativo, na medida em que os acessos a esse dado deveriam, na maioria dos casos, ser específicos e restritos a situações de aferição de segurança de transações bancárias, por exemplo.

O primeiro ponto[456] é particularmente desalinhado com a lógica da LGPD, pois não há qualquer referência a quem são os parceiros do *Itaú*. E, nesse ponto, não se pode olvidar que as instituições financeiras têm dados realmente confidenciais de seus usuários. Ou seja, o *Itaú* poderia, em tese, repassar os dados absolutamente sigilosos para fins de publicidade via *targeting*, ou para tantas outras finalidades mais ou menos discriminatórias em relação ao usuário a partir de sua análise de crédito, o que não parece ser o espírito da LGPD de privacidade contextual.

O segundo ponto[457] chancela o fato de o aplicativo coletar informações de navegação e outras informações pessoais armazenadas no dispositivo do usuário para fins de posterior análise de crédito. Ou seja, o *Itaú* informa ter acesso aos dados do usuário para posteriormente analisar se ele será um risco à sua política de empréstimos. Parece um verdadeiro abuso da confiança. O aplicativo usa o dado pessoal do cliente – coletado de modo pouco claro e transparente – para recusar-lhe produtos do banco. Em tese, se o usuário troca mensagens ou compartilha publicações em redes sociais fazendo alusão a dificuldades financeiras, por exemplo, o aplicativo poderia acessar esse tipo de dado para segmentar o potencial cliente.

---

[454] Especificamente quanto às permissões solicitadas no aplicativo, a política de privacidade informa que "o Banco do Brasil solicita a concordância dos usuários do aplicativo BB para ter acesso ao número do telefone em que o app está sendo utilizado, localização do dispositivo, autorização para envio de SMS, acesso à câmera do celular e email cadastrado na loja de aplicativos. Estas informações são necessárias para validações de segurança no dispositivo utilizado pelos nossos clientes e gerar mais comodidade no atendimento".

[455] ITAÚ UNIBANCO. Termos de privacidade e política de privacidade. Disponível em: <https://www.itau.com.br/_arquivosestaticos/Tablet/Mobile/termosdeuso.html>. Acesso em: 12 abr. 2021.

[456] "Permitir o desenvolvimento, a oferta e a utilização de produtos, serviços, conteúdos e anúncios do Itaú Unibanco e de parceiros do Itaú Unibanco mais personalizados, de acordo com suas necessidades e interesses".

[457] "Possibilitar análise de potenciais riscos na oferta e contratação de produtos e/ou serviços do Itaú Unibanco".

Os termos de privacidade do *Bradesco*[458] indicam que a ferramenta só funciona se o usuário der o seu consentimento ao uso de *cookies*, o que é particularmente questionável, sobretudo porque o documento dá a entender que esses dados seriam utilizados apenas para oferecer uma navegação mais personalizada na plataforma[459]. Ora, o usuário deveria poder navegar sem o modo personalizado.

Quanto ao *Serasa Consumidor*[460], parece particularmente desalinhado com a lógica da LGPD o elevado lapso temporal pelo qual é feito o tratamento dos dados – nesse ponto, contudo, é de se afirmar que a Lei do cadastro positivo autoriza as informações creditícias por uma validade de 15 anos, o que pode ser a justificativa utilizada pelo aplicativo. Noutro giro, a empresa, ao informar que também utiliza a plataforma *Google Analytics*, informa o link específico da página de privacidade do gigante da tecnologia, diferentemente da *Caixa*, o que parece aderente à tutela da privacidade que se entende como adequada[461].

O aplicativo informa coletar dados eventualmente disponíveis em sites da internet e "os dados do seu dispositivo", além de poder comercializar uma foto do rosto do usuário – inicialmente coletada para fins de biometria facial – para soluções de prevenção a fraudes. Intrigantes a permissão geral para acessar os dados do dispositivo – sem maiores detalhamentos – e a possibilidade de venda da imagem do usuário, ainda que para fins antifraude (também sem maiores explicações, contudo).

O grande problema, sustenta-se, é que os próprios dados do dispositivo podem conter as informações de histórico de crédito do usuário – ainda mais na era do internet banking –, ou seja, o *smartphone* realmente é um ótimo banco de dados para o *Serasa*.

Quanto à revogação do consentimento, o *Serasa* indica que pode existir "quando os seus Dados Pessoais não forem usados para proteção ao crédito, não houver legítimo interesse no seu tratamento, não for necessário para o cumprimento de um dever legal, contratual ou regulatório da *Serasa Experian* e/ou de seus clientes ou não se enquadrar em quaisquer outras hipóteses legais que autorizem o tratamento de Dados Pessoais". Não há menção à possibilidade

---

458 BRADESCO. Diretivas de Privacidade. Disponível em: <https://www.bradescoseguranca.com.br/portal/layout/temas/seguranca-corporativa/pdf/Diretivas-de-Privacidade-Mobile.pdf>. Acesso em: 12 abr. 2021.

459 "Caso o usuário não concorde com a utilização de tecnologias para reconhecimento da origem e último acesso, bem como acompanhar a sua utilização, o usuário deverá interromper o seu acesso ao aplicativo".

460 SERASA CONSUMIDOR. Políticas do site. Disponível em: <https://www.serasaconsumidor.com.br/politicas-do-site>. Acesso em: 11 abr. 2021.

461 Informa-se que, "quando você acessa nossos Sites e/ou nossos aplicativos, você nos autoriza a coletar, a utilizar, a armazenar e a tratar, pelo prazo de 15 (quinze) anos, os dados de identificação de Dispositivos, de endereços IP e aqueles coletados por meio de Cookies em nossos Sites e/ou aplicativos, para as finalidades a seguir apresentadas: (...) melhorar a sua experiência e as suas interações durante a navegação no Site ou no aplicativo; identificar o seu perfil para permitir a oferta de informações e/ou serviços mais adequados às suas necessidades ou interesses".

de revogação do consentimento pela simples dissolução do interesse em utilizar a plataforma. Especificamente sobre a publicidade digital, a revogação do consentimento – por padrão, *opt-in* – pareceu difícil[462].

Os termos do *Santander BR*[463] merecem o destaque por terem sido os mais detalhados da categoria, mas nada muito diferente se comparado ao ambiente macro deste trabalho. O ponto mais interessante é a explicação detalhada das permissões solicitadas aos usuários quando da instalação do aplicativo. Veja-se:

> Para utilização do **app Santander** são obrigatórios três tipos de autorizações, descritas abaixo:
> **1. Localização**
> Necessário para envio de pushs personalizados e funcionamento do localizador de agências. O banco pode usar a sua localização para prevenção a fraudes.
> **2. Telefone (fazer e gerenciar chamadas telefônicas)**
> Necessário para identificação do dispositivo. É o nome do aparelho que aparece na opção "Desbloqueio de Aparelho" no internet banking e também necessário para a realização de ligação telefônica nas funções de "click to call" disponível em Previdência, por exemplo.
> O banco armazena o nome do telefone e seu ID (IMEI), como descrito acima, apenas para conseguir realizar o processo de desbloqueio para a realização de transações financeiras. Essas informações não são compartilhadas com terceiros.
> **3. Acessar fotos, mídias e arquivos do seu dispositivo**
> Necessário para criação dos comprovantes ao final da transação e selecionar foto na galeria para inclusão de foto de perfil. Nenhuma informação do seu celular é lida ou armazenada pelo banco.
> As duas permissões abaixo são facultativas e só são solicitadas caso o cliente necessite atribuir uma foto de perfil, pagar contas ou boletos e realizar uma recarga.
> **Tirar fotos e gravar vídeos**
> Necessário para atribuir uma foto de perfil, pagar boleto/conta pela câmera ou QR Code de outros sites. As fotos retiradas para uso no perfil não são armazenadas pelo banco, assim como as capturas dos códigos de barras ou QR Code capturados.
> **Acessar os contatos**
> Necessário caso queira realizar uma recarga selecionando um contato que está registrado na agenda do aparelho. Nenhuma informação da agenda de contatos é usada e/ou armazenada pelo banco.
> **Touch ID (iOS) / Impressão Digital (Android)**
> Os clientes com a função ativada e com digitais cadastradas no aparelho (iOS a partir do iPhone 5S e Android para dispositivos que possuem sensor biométrico) poderão acessar o app Santander, caso queiram, sem a digitação de sua senha de acesso.
> Qualquer biometria cadastrada no aparelho permitirá acesso ao app Santander. O cliente é o responsável por desabilitar a função em questão.
> Essa funcionalidade permitirá o acesso ao app Santander, porém não substitui a senha do cartão de segurança Santander ou ID Santander para efetivação das transações.
> O Santander não tem acesso às biometrias cadastradas no aparelho, sendo essas restritas à Apple e Google, conforme os termos da Política de Privacidade dessas empresas.

---

[462] O aplicativo informa que "seus Dados Cadastrais e Pessoais podem ser utilizados por nós para manter um relacionamento comercial e institucional com você. Podemos enviar a você comunicações periódicas relacionadas às novidades dos Sites, às informações de seu interesse específico, para fins de marketing, pesquisas de satisfação e campanhas com ofertas promocionais das soluções oferecidas pela empresa e por parceiros".

[463] SANTANDER. Políticas de Privacidade. Disponível em: <https://www.santander.com.br/institucional-santander/seguranca/politica-de-privacidade>. Acesso em: 12 abr. 2021.

Essa posição de explicar detalhadamente a utilidade de cada permissão parece aderente à tutela da privacidade que se entende como adequada. Assim, o usuário se sente mais seguro em dar o seu consentimento de modo informado. Seria interessante que um resumo desse texto também fosse exibido na interface do próprio aplicativo, quando a permissão respectiva fosse efetivamente solicitada, na medida em que são poucos os usuários que terão a disponibilidade de ler detalhadamente os termos antes de usar o aplicativo.

O *Santander ESP*[464] não pareceu muito melhor do que a versão brasileira. Apesar de não ser tão detalhista no tocante à explicação das permissões solicitadas, apresenta longa lista de todos os *cookies* utilizados – bem como links respectivos para suas políticas de privacidade e indicação de como revogar o consentimento para seu funcionamento – e lista de todos os parceiros com os quais o banco compartilha os dados do usuário. Esse segundo ponto parece ser uma realidade um pouco distante dos aplicativos nacionais, cujos termos de privacidade ainda se limitam a indicar genericamente que o banco fará o compartilhamento com terceiros.

O *Santander UK*[465] dispensa maiores comentários, pois segue a mesma linha de outros aplicativos aqui analisados. Um ponto positivo, contudo, é o fato de o documento de privacidade indicar uma detalhada cartilha cujo título é "*Using my personal data: how we use your personal data*" ("Usando meus dados pessoais: como usamos seus dados pessoais"). As informações contidas nesse documento realmente pareceram completas, mas não foram lidas com detalhe durante o trabalho.

É claro, nesse aspecto de análise comparativa entre os aplicativos bancários internacionais, que há naturais diferenças regulatórias para o sistema financeiro em cada país, o que pode, ainda que indiretamente, implicar mudanças no âmbito das políticas de privacidade. Optou-se, mesmo assim, por fazer a análise enxuta aqui empreendida, mesmo que, pudesse ser um pouco enviesada pelas diferenças próprias das normas regulatórias setoriais internacionais.

Quanto ao *PicPay*[466], embora o aplicativo pareça ter pretensões de ser uma plataforma de pagamentos e de conexão social – o que pode ser perigoso do ponto de vista de processamento não contextual dos dados –, fala-se que "você pode mudar as configurações de

---

[464] SANTANDER ESP. Condiciones Generales de Uso. Disponível em: <https://www.bancosantander.es/es/aviso-legal>. Acesso em: 12 abr. 2021.
[465] SANTANDER UK. Legal information. Disponível em: <https://www.santander.co.uk/personal/support/customer-support/legal-information>. Acesso em: 12 abr. 2021.
[466] PICPAY. Privacidade. Disponível em: <https://picpay.com/site/privacidade>. Acesso em: 13 abr. 2021.

privacidade no seu aplicativo a qualquer momento, bloqueando acesso às suas atividades". Ou seja, em tese, o usuário tem o controle, via consentimento, para aferir o que será tratado.

Chama atenção a seguinte afirmação: "pode ser que a gente peça algumas informações a mais, para deixar seu cadastro 100%. Essas informações também podem ser usadas para mostrar a você alguns produtos ou serviços bem legais, então, caso a gente pergunte a sua faixa salarial, peça uma *selfie* ou cópia do seu documento com foto, é normal, beleza? Pode deixar que essas informações ficam protegidas como todas as outras que você compartilhar com a gente".

Embora se tente criar, pela linguagem acessível e quase coloquial, um paradigma de aproximação entre plataforma e usuário – o que é bom –, é fato que há algumas informações relevantes sendo coletadas para a finalidade de exibir "alguns produtos ou serviços bem legais". Inclusive quando se fala da localização para fins de prevenção a fraudes ou para exibir locais próximos que aceitam a modalidade de pagamento.

No que tange ao compartilhamento de dados com terceiros, inclusive a nível internacional, fala-se na manutenção dos níveis adequados e homogêneos de proteção à privacidade dos usuários. Além disso, se o usuário deixar o "perfil aberto", a sua *rede social* poderá saber quando e onde pagou com o aplicativo, embora sem o valor – o que já parece suficientemente excessivo do ponto de vista da necessária minoração dos dados.

A política de privacidade do *Nubank*[467] é muito simples e sem a necessária transparência para que o consumidor consinta de modo informado com o tratamento de dados. Há certo nível de obscuridades nas cláusulas, que são genéricas, inexistindo menção a níveis mínimos de respeito à privacidade dos usuários[468]. Nessa linha, é curioso o fato de o banco se promover como sendo a antítese daqueles maiores do segmento econômico – simplicidade, transparência, dentre outros –, mas sem tutelar de modo adequado a privacidade dos usuários.

O *Digio*[469] também segue o mesmo grau de generalidade, mas informa especificamente que as destinatárias do compartilhamento de dados devem cumprir "nossas diretrizes de segurança e privacidade" e aquelas estabelecidas nas exigências legais.

---

[467] NUBANK. Política de Privacidade Nubank. Disponível em: <https://nu-assets.s3.amazonaws.com/politica-privacidade.pdf>. Acesso em: 12 abr. 2021.

[468] Um exemplo é a seguinte: "para fins operações de crédito e gerenciamento de riscos, poderemos trocar informações sobre nossos clientes com fontes respeitáveis de referência, órgãos reguladores e serviços de compensação". Ora, o que seriam "fontes respeitáveis de referência" e "serviços de compensação"?

[469] DIGIO. O Digio se compromete com a sua privacidade. Disponível em: <https://www.digio.com.br/assets/Politica_de_privacidade.pdf>. Acesso em: 12 abr. 2021.

Os termos de privacidade do *Banco Inter*[470] ganham destaque ao mencionarem expressamente o atendimento aos padrões de segurança mínimos estabelecidos no Decreto nº 8.771/2016, que regulamentou o Marco Civil da Internet em sua parte de guarda de dados. Embora isso possa ser um apontamento inócuo, demonstra o mínimo de zelo para com o usuário, pois se está seguindo o regramento legal. No mais, os termos de privacidade são mais detalhados do que aqueles dos dois bancos digitais retro, mas ainda genéricos.

O *Mercado Pago*[471] apresenta os mesmos termos aplicáveis a todos os produtos do *Mercado Livre*. De modo geral, também não há trechos que justifiquem comentários mais detalhados. O único ponto relevante é o fato de a política de privacidade fazer expressa alusão à legislação argentina – onde é situada a sede da empresa –, não havendo nenhuma referência à lei nacional. Os termos de privacidade presentes no menu de configurações do aplicativo, entretanto, são em português e fazem referência à lei brasileira, o que denota certa contradição.

Os termos de privacidade do *PayPal*[472] são detalhados, explicando todas as opções – ainda que de modo genérico – que o usuário tem em relação aos seus dados pessoais. Outro ponto positivo é o fato de haver direcionamento a uma página específica sobre a política de *cookies*.

Por fim, fala-se da transparência de colocar a comparação entre os termos novos e os antigos de modo esquemático: trechos alterados são sublinhados. Essa certamente é uma forma de melhorar o entendimento dos usuários. Na leitura comparativa, contudo, não foram percebidas alterações muito substanciais com vistas à maior proteção dos dados pessoais dos usuários.

Quanto ao *Investing*[473], uma cláusula chama atenção: a afirmação de que o compartilhamento de informações com terceiros – seja do próprio grupo empresarial ou externos interessados em oferecimento de publicidade dirigida – pode se dar para "países que podem oferecer um nível diferente de proteção de privacidade do que em sua jurisdição" (tradução livre).

Ou seja, o aplicativo não tem preocupação em manter o nível de privacidade em sua rede de compartilhamento. A posição é diferente quando se trata de usuário situado na

---

[470] BANCO INTER. Termos de Uso e Política de Privacidade. Disponível em: <https://www.bancointer.com.br/politica-de-privacidade/>. Acesso em: 12 abr. 2021.
[471] MERCADO LIBRE. Políticas de privacidad y confidencialidad de la información. Disponível em: <https://www.mercadolibre.com.ar/ayuda/Politicas-de-privacidad_993>. Acesso em: 12 abr. 2021.
[472] PAYPAL. Declaração de Privacidade. Disponível em: <https://www.paypal.com/webapps/mpp/ua/privacy-full>. Acesso em: 12 abr. 2021.
[473] FUSION MEDIA. Privacy Policy. Disponível em: <https://www.investing.com/about-us/privacy-policy>. Acesso em: 12 abr. 2021.

União Europeia, em que o próprio documento informa que o compartilhamento se dá apenas para países certificados. O *software*, portanto, tenta claramente reduzir os seus custos, ao só se preocupar com o grau de proteção dos países quando formalmente exigido pela legislação. A LGPD exige essa mesma linearidade no compartilhamento internacional, mas não há menção à lei nacional nos termos.

Outro ponto desalinhado com a lógica da LGPD é a afirmação de que alguns destinatários dos dados pessoais compartilhados pelo *software* podem usá-los para fins de oferecimento de empréstimos, o que parece descolado do contexto da coleta. Um aspecto positivo é o fato de também haver uma política específica de *cookies*, com uma extensa lista de todos aqueles utilizados e o respectivo propósito principal.

3.3.7 Compras

Os termos de privacidade do *Mercado Livre* já foram analisados na seção anterior, razão por que se dispensa a repetição. Quanto ao *Wish*[474], uma cláusula sobre anonimização de dados que também foi observada em outros aplicativos chama atenção[475]. Embora seja claro que informações anonimizadas possam não merecer tanta preocupação pelos usuários dos aplicativos – afinal, se o processo de anonimização tiver sido bem feito, não há como se chegar ao usuário específico –, seria mais transparente se houvesse ao menos alguma indicação a qual termo seria exatamente aplicável a esse caso.

Ao menos, o aplicativo é transparente sobre como exercer as escolhas de publicidade personalizada, indicando três portais que ensinam a promover a revogação dos consentimentos por *opt-out*. Além disso, os termos de privacidade também ensinam o usuário a bloquear, de modo geral no celular – por configuração do próprio *Android* –, a publicidade baseada em interesse. Conduta transparente e, por isso, adequada às normas da LGPD.

O *Enjoei*[476] não destoou do padrão observado nos demais aplicativos, salvo por expressamente informar que "esta política tem natureza de contrato de adesão e passa por revisões periódicas, sem que seja necessária a sua notificação prévia". Nesse ponto, também se

---

[474] WISH. Privacy Policy. Disponível em: <https://www.wish.com/en-privacy-policy>. Acesso em: 12 abr. 2021.
[475] "Podemos combinar as informações coletadas ('agregadas') ou remover informações ('desidentificar') para limitar ou impedir a identificação de qualquer usuário ou dispositivo específico, o que pode ajudar a apoiar nossos esforços de pesquisa e marketing. Esta Política de Privacidade não se aplica ao nosso uso de tais informações agregadas ou desidentificadas" (tradução livre).
[476] ENJOEI. Política de privacidade e confidencialidade da informação. Disponível em: <https://www.enjoei.com.br/ajuda/sobre-o-enjoei/politica-de-privacidade-e-termos-de-uso-do-enjoei/politica-de-privacidade-e-confidencialidade-da-informacao>. Acesso em: 13 abr. 2021.

recomenda que "você consulte o documento para saber se continua concordando com seus termos antes de seguir com a navegação". O mais alinhado à dinâmica da LGPD, contudo, era a notificação ativa ao titular dos dados acerca de eventual modificação relevante na política. Se a plataforma passar a comercializar os dados do usuário com todos os países do mundo, por exemplo, é necessário que isso seja informado ao titular, e não que se presuma que ele vá consultar recorrentemente a política.

Há menções expressas à LGPD e, quando da seção de transferência internacional, ao RGPD e ao paradigma californiano de proteção de dados. A política de privacidade é bem organizada e de fácil inteligibilidade. Chama atenção apenas o fato de que, diferente da maioria, o aplicativo não faz menção ao legítimo interesse como base legal para o tratamento de dados, tampouco aos contratos. Em verdade, não há menção qualquer a quais seriam as bases legais, mas o conjunto do texto dá a entender que se trata apenas da manifestação do consentimento pelo titular dos dados.

O *Shopee*[477], à semelhança de outros aplicativos aqui analisados, também descreve a realidade *take it or leave it* em letras garrafais: "se você não concorda com o processamento de seus dados pessoais como descrito nesta política de privacidade, não use nossos serviços ou acesse nossa plataforma". É prática comum no mercado, embora fosse desejável, à luz da LGPD, uma maior paridade na discussão de tópicos concernentes à política de privacidade, à semelhança de outro ponto do documento: "cancelar a coleta de informações de localização fará com que seus recursos baseados em localização sejam desativados". Isso se alinha perfeitamente à ideia de consentimento granular e de funcionamento do aplicativo em níveis de funcionalidade.

Em outro ponto interessante, a política de privacidade informa que, como os objetivos do tratamento dos dados pessoais podem depender das circunstâncias do caso concreto posto, não há como antever todas as hipóteses na própria política, razão por que "iremos notificá-lo de tal outra finalidade no momento de obter o seu consentimento, a menos que o processamento dos dados aplicáveis sem o seu consentimento seja permitido pelas Leis de Privacidade". Essa previsão de tentativa de buscar a privacidade contextual é aderente à tutela correta dos dados pessoais sob a dinâmica da LGPD. No decorrer do documento, é possível perceber que a empresa também parece apostar mais no consentimento do usuário como base legal do que no legítimo interesse da plataforma, o que é interessante do ponto de

[477] SHOPEE. Política de privacidade. Disponível em: <https://shopee.ph/legaldoc/privacy>. Acesso em: 13 abr. 2021.

vista da proteção dos dados, haja vista um aparente espectro mais ampliado de proteção do direito fundamental quando se fala do consentimento.

O *OLX*[478] foi o primeiro aplicativo analisado a informar claramente uma prática corriqueira no mercado: a utilização de jogos na plataforma para a obtenção de outros dados pessoais. Isso é comum no *Facebook*, por exemplo[479]. Partindo disso, os termos de privacidade do *OLX* prescrevem que "Nós podemos coletar informações pessoais tais como seu nome e informação de contato quando Você participar de jogos, quiz ou outras ações de marketing que Nós patrocinarmos em Nosso site ou em sites de terceiros". Ainda afirma, seguindo a linha de transparência, que "Nós também podemos processar, diretamente ou por meio de terceiros, informações relacionadas à efetividade de Nossas campanhas publicitárias, incluindo quais anúncios foram visualizados e clicados, tanto na Nossa rede como em sites de terceiros".

Há também prescrição específica para o funcionamento da política de privacidade em dispositivos móveis – o que é quase inexistente em quase todos os documentos analisados. Veja-se:

> Quando você utiliza um aplicativo da OLX, podem ser coletados dados, para fins de veiculação publicitária, sobre o dispositivo, incluindo o Identificador de Publicidade do Android, do iOS ou de outros sistemas operacionais análogos, bem como dados de localização recebidos a partir dos sensores do dispositivo. Além desses dados, também há coleta de dados sobre publicidade no dispositivo, incluindo cliques efetuados a partir dele, impressões e tempo de permanência em publicidade. Cumprindo os requisitos de transparência, detalhamos abaixo os dados do seu dispositivo que podem ser coletados se você se utiliza de um dos nossos apps:
> 1. Identificadores anônimos de publicidade do dispositivo, atributos do dispositivo móvel e aplicativos instalados no respectivo aparelho;
> 2. Dados dos sensores do aparelho;
> 3. Dados anônimos de localização do aparelho por meio de GPS ou rede celular.

Fala-se também do fato de haver indicação para a lista dos provedores destinatários dos dados pessoais coletados e que farão a posterior análise para fins de publicidade comportamental, o que parece aderente à tutela da privacidade que se entende como adequada[480]. Lista essa que comporta uma série de provedores também citados nos termos de privacidade de outros aplicativos.

Mas, na contramão dessa transparência grande e alinhada à dinâmica da LGPD, há uma *permissão* para compartilhamento dos dados para quaisquer países, sem restrições a

---

[478] OLX BRASIL. Política de Privacidade Nubank. Disponível em: <https://olxbrasil.zendesk.com/hc/pt-br/articles/211375589>. Acesso em: 13 abr. 2021.
[479] Aquelas tradicionais histórias de "veja como você seria no futuro", "veja qual personagem você é", etc. Foi por meio de um desses jogos que o escândalo da Cambridge Analytica começou.
[480] São eles: Criteo, Google, Facebook, Twitter, Kenshoo, Advantage Media, DoubleClick Floodlight Sales, Bing, Lomadee, Zanox, Yahoo, Navegg, Google Analytics, In Loco Media.

respeito de nível de proteção à privacidade, o que está na contramão das regras da LGPD para o compartilhamento internacional de dados.

O *Magazine Luiza*[481], assim como outros aplicativos analisados, na própria página específica do documento de privacidade, exibe um *banner* perguntando se o usuário concorda com a política de *cookies* do site e se quer receber anúncio personalizado. Isso demonstra, logo no início, que a publicidade comportamental é um dos motes da empresa, mesmo no documento em que elas não deveriam existir.

Outro ponto que chama a atenção é a cláusula de não indenizar[482]. Embora seja uma cláusula também abusiva, parece melhor do que as outras já comentadas neste trabalho, na medida em que não exime a responsabilidade da empresa em caso de culpa sua – e se poderia argumentar pela culpa justamente como uma espécie de negligência por oferecer um sistema com falhas na proteção dos dados. Por fim, o último ponto que também chama atenção é o fato de os termos de privacidade datarem de julho de 2015, o que parece antigo para o dinâmico mundo da tecnologia.

Por sua vez, o documento de privacidade do aplicativo *Americanas*[483] é extremamente enxuto e pouco detalhista, o que indica que a privacidade não parece ser o paradigma mais importante para a empresa.

O aplicativo da *Amazon*[484] também é transparente o suficiente para deixar claro que utiliza os dados da localização do dispositivo e o seu identificador exclusivo para fins de exibição de publicidade via *targeting*. O aplicativo também informa seguir os princípios de autorregulação para publicidade comportamental online ao fornecer anúncios baseados em interesses.

Tais princípios seriam desenvolvidos pela *Digital Advertising Alliance*, uma coalizão de marketing, publicidade online e organizações de defesa do consumidor[485]. Ou seja,

---

[481] MAGAZINE LUIZA. Política de Privacidade. Disponível em: <https://m.magazineluiza.com.br/s/politica-de-privacidade>. Acesso em: 13 abr. 2021.

[482] "Considerando que nenhum sistema de segurança é absolutamente seguro, o Magazine Luiza se exime de quaisquer responsabilidades por eventuais danos e/ou prejuízos decorrentes de falhas, vírus ou invasões do banco de dados do site, salvo nos casos de dolo ou culpa pela mesma".

[483] LOJAS AMERICANAS. Política de Privacidade. Disponível em: <https://www.americanas.com.br/estaticapop/politica-de-privacidade-lightbox>. Acesso em: 13 abr. 2021.

[484] AMAZON. Amazon Privacy Notice. Disponível em: <https://www.amazon.com/gp/help/customer/display.html/?ie=UTF8&nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_467C686A137847768F44B619694D3F7C>. Acesso em: 13 abr. 2021.

[485] Na mesma linha, o aplicativo informa que o usuário "também pode optar por não receber anúncios personalizados de anunciantes e redes de anúncios de terceiros que sejam membros da Network Advertising Initiative (NAI) ou que sigam os Princípios de autorregulamentação da Digital Advertising Alliance para publicidade comportamental on-line visitando a desativação páginas no site da NAI e no site da DAA" (tradução livre).

a *Amazon* segue os acordos mínimos internacionais sobre a proteção da privacidade dos seus usuários. Os termos, embora não muito detalhistas – considerando-se a abrangência e o porte da empresa, poderiam ser melhores –, parecem aderentes à tutela da privacidade que se entende como adequada quando colocados em comparação a outros aqui analisados nessa categoria.

O *Ebay*[486], assim como diversos outros aplicativos aqui avaliados, também informa não vender, alugar ou divulgar os dados pessoais do usuário a terceiros para único fim de marketing e publicidade comportamental sem o expresso consentimento. O problema é que, na maioria das vezes, o consentimento pela política de privacidade via segmentação é automático, apenas existindo – se efetivamente existir de modo livre, inequívoco, consciente e expresso – a chance de *opt-out*. Se a prática realmente refletisse essa realidade pretensa dos termos de privacidade de serem *opt-in*, seria mais aderente à LGPD.

O aplicativo, assim como o *Amazon*, apresenta página específica de explicação acerca de sua política de *cookies*, mas nenhuma ressalva é aqui necessária. Um ponto que parece aderente à tutela da privacidade que se entende como adequada é o fato de afirmar seguir um padrão internacional de privacidade (*Binding Corporate Rules*[487]), para que todas as empresas subsidiárias tenham o mesmo padrão de proteção dos dados. Para tanto, também há página específica e detalhada sobre um centro de privacidade. Parece aderente à tutela da privacidade que se entende como adequada a posição da empresa, que, ao menos *prima facie*, demonstrou um padrão de preocupação com a gestão dos dados pessoas de seus consumidores.

Uma cláusula que remete ao texto do RGPD – "nós usamos seus dados pessoais de acordo com nossos interesses legítimos, contanto que seus direitos e suas liberdades não prevaleçam sobre tais interesses. Nós implementamos controles para contrabalançar nossos interesses e seus direitos" – também se sobressai, sendo relevante esperar que haja garantias de que o teste da proporcionalidade é realmente feito no caso concreto, gerando um passivo documental que permita aferir a validade das escolhas do provedor.

Outra cláusula que merece atenção especial é a que afirma que o acordo comercial é o único meio de estabelecer uma limitação ao uso dos dados pessoais, o que não parece exatamente algo muito seguro[488].

---

[486] EBAY. Aviso de Privacidade do Usuário. Disponível em: <https://www.ebay.com/pages/help/policies/privacy-policy.html>. Acesso em: 13 abr. 2021.

[487] EBAY. User Corporate Rules. Disponível em: <https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf>. Acesso em: 13 abr. 2021.

[488] "Provedores terceirizados de sites, aplicativos, serviços e ferramentas com os quais colaboramos para permitir que eles publiquem ou anunciem seus anúncios e o conteúdo dos seus anúncios nos sites, nos aplicativos, nos serviços e nas ferramentas deles. Se transferirmos dados pessoais junto com o conteúdo dos anúncios para provedores terceirizados, essa transferência será realizada unicamente com base em um acordo que limite o uso de tais dados pessoais ao processamento necessário para o cumprimento do contrato estabelecido entre nós e esses

Por fim, o *AliExpress*[489] segue a linha questionável de fornecer os dados pessoais coletados aos "provedores de avaliação de risco de crédito, para conduzirem a avaliação de risco nos Vendedores para determinar se um Vendedor pode ter permissão para fazer uma retirada de fundo" (tradução livre).

Embora pareça ser um interesse legítimo da empresa, é questionável que se cogite do compartilhamento de informações com as empresas de proteção do crédito. Também há no documento longa lista de *cookies* utilizados na plataforma, bem como seu respectivo link de termos de privacidade. Também há termos específicos para usuários da União Europeia, mas nenhuma cláusula merece algum destaque maior.

3.3.8 Notícias e revistas

O *G1*[490] apresenta política de privacidade geral de todas as ferramentas da rede *Globo*; nesse caso, o caráter genérico do documento não é tão descompassado da lógica de especificidade da LGPD quanto em outros aplicativos, na medida em que a empresa possui pouca diversidade de funcionalidades aos dispositivos móveis[491].

Contudo, o documento também ressalta que o aplicativo não comercializa ou fornece as informações pessoais individualizadas a terceiros, salvo quando do cumprimento de ordem judicial específica. Ou seja, as informações fornecidas aos parceiros, anunciantes e patrocinadores do grupo empresarial são apenas fornecidas em termos de grupos de usuários, por segmentos de mercado. De modo geral, a política de privacidade do *G1* é clara e contém explicação detalhada sobre as possibilidades de revogação do consentimento pelo usuário. Se esses direitos podem ser facilmente executados na experiência concreta do uso da aplicação, não foi possível aferir no trabalho.

O aplicativo *Folha de SP*[492] começa, ao contrário do *G1* – que informa ser opção do usuário a desativação dos *cookies* –, estabelecendo que a navegação em algumas páginas da

---

provedores terceirizados e obrigue o provedor terceirizado a tomar medidas de segurança para proteger os dados. Provedores terceirizados não têm permissão para vender, alugar ou de qualquer outra forma transferir para terceiros os dados pessoais incluídos nos seus anúncios".

[489] ALIBABA. Privacy Policy. Disponível em: <https://rule.alibaba.com/rule/detail/2034.htm>. Acesso em: 13 abr. 2021.

[490] GLOBO. Política de privacidade da Globo. Disponível em: <https://www.globo.com/privacidade.html>. Acesso em: 12 abr. 2021.

[491] Segundo a empresa, as informações dos usuários "poderão ser utilizadas para gerar dados estatísticos gerais com finalidade informativa ou comercial. Informações geográficas, demográficas, psicográficas e de perfil de uso dos usuários da Globo poderão ser fornecidas a parceiros, patrocinadores, anunciantes ou outras empresas externas, sem que sejam revelados nomes ou outros dados de navegação".

[492] FOLHA DE SÃO PAULO. Política de Privacidade - Folha de S.Paulo. Disponível em:

empresa, inclusive com o maior consumo gratuito de reportagens, pressupõe que o usuário se identifique por meio de cadastro e aceite o armazenamento dos *cookies*. E os termos de privacidade também não evoluem, na medida em que são genéricos e resumidos, não sendo transparentes o suficiente para que o usuário dê o seu consentimento livre, informado e consciente no tratamento de dados.

Prima facie, a política de privacidade do *UOL Notícias*[493] parece avançada e atualizada às exigências das novas legislações. Um primeiro ponto interessante é o estabelecimento da divisão entre os tipos de *cookies* pela sua finalidade: (i) os estritamente necessários, que são aqueles sem os quais o aplicativo não funcionaria; (ii) os de performance, que são os dados anônimos que servem para a correção dos erros do próprio aplicativo; (iii) os de funcionalidade, que permitem experiências mais pessoais do usuário em relação à própria plataforma; (iv) os analíticos e de publicidade, que permitem aos anunciantes entregar anúncios e informações mais relevantes ao usuário (a exemplo do *Google Analytics*); e (v) de mídias sociais, que permitem que o usuário se conecte a partir de uma rede social já existente.

Também na vanguarda brasileira, o *UOL Notícias* foi um dos poucos aplicativos nacionais que efetivamente elencou os direitos dos usuários de acessar e excluir os dados, revogar o consentimento para a sua coleta, solicitar a devida portabilidade e revogar especificamente a concordância pré-determinada com o uso para fins de *marketing*. Também há expressa previsão de um encarregado pelos dados (a figura do *Data Protection Officer*, prevista no RGPD). É claro que esse é o mínimo que se espera à luz das normas da LGPD, mas, dada a realidade do mercado, é necessário que se faça a menção.

Ao revés, o *El País*[494] parece razoavelmente atrasado para fins das exigências impostas pelo RGPD e pela LGPD, na medida em que é pouco detalhista em sua política de privacidade. O ponto mais interessante dela é o fato de que a aplicação vincula uma página específica de empresa de gerenciamento de *cookies*, que contém uma explicação detalhada sobre quais arquivos são utilizados e qual a sua finalidade específica. Só não fica exatamente claro se todos os tipos de arquivos são também utilizados no aplicativo analisado[495].

<https://www1.folha.uol.com.br/paineldoleitor/2018/05/politica-de-privacidade-folha-de-spaulo.shtml>. Acesso em: 12 abr. 2021.

[493] UOL. Normas de segurança e privacidade. Disponível em: <https://sobreuol.noticias.uol.com.br/normas-de-seguranca-e-privacidade.html>. Acesso em: 12 abr. 2021.

[494] EL PAÍS. Política de privacidad de los servicios El País. Disponível em: <https://elpais.com/estaticos/politica-privacidad/>. Acesso em: 12 abr. 2021.

[495] PRISA. Política de cookies. Disponível em: <https://www.prisa.com/es/info/politica-de-cookies>. Acesso em: 12 abr. 2021.

Inicialmente, o *CNN*[496], assim como diversos outros aplicativos analisados, chama atenção por informar que um dos mecanismos de coleta de dados dos usuários são as votações e enquetes patrocinadas na página. Aqui, parece temerário que as empresas se utilizem da justificativa de o usuário ter voluntariamente respondido às enquetes – o que, teoricamente, daria o *check* para o requisito de haver consentimento – para coletar os seus dados pessoais, com finalidades quaisquer. Parece ser um *disclaimer* indevido: se não se consegue tutelar a privacidade nesse tipo de ferramenta, seria preferível, à luz da LGPD, que ela inexistisse.

Outro ponto relevante é o fato de o aplicativo informar que o usuário poderá, na maioria dos casos, desativar a coleta das informações de sua localização geográfica precisa para fins de publicidade comportamental específica. Obscuro – e inexplorado no documento – é saber quais são os casos minoritários em que o usuário não pode revogar o consentimento de acesso a um dado tão relevante quanto a localização.

Mais um aspecto relevante é a informação de que, quando o usuário se envolve com o conteúdo da *CNN* por meio de serviços de mídia social ou aplicativos de terceiros, acaba por permitir que a empresa tenha acesso a determinadas informações, como nome, endereço de e-mail, foto, sexo, aniversário, local, outros arquivos da mídia social – fotos e vídeos –, lista de amigos e conexões, lista de pessoas seguidas, postagens ou curtidas.

Ou seja, a coleta dos dados pelo simples acesso da plataforma *CNN* por meio das redes sociais é muito amplo, incompatível com a lógica de minimização da LGPD. Não se sabe se os outros aplicativos também fazem isso, mas simplesmente são pouco transparentes em sua política de privacidade, ou se a aplicação *CNN* é realmente diferente no quesito do acesso. De modo geral, a política do aplicativo *CNN* é direta e transparente, denotando a realidade do mercado de modo claro e sem *juridiquês* indevido.

O *Fox News*[497] também segue a posição de transparência do *CNN*. De mais interessante e relevante, há a informação de que os aplicativos para dispositivos móveis contêm "kits de desenvolvimento de *software*" ou "SDKs" de parceiros de anúncios de terceiros que os parceiros de publicidade terceirizados da empresa usam para coletar IDs de publicidade para dispositivos móveis para publicidade baseada em interesses no aplicativo e em outros aplicativos.

---

[496] CNN. CNN Privacy Policy. Disponível em: <https://edition.cnn.com/privacy0?no-st=9999999999>. Acesso em: 12 abr. 2021.
[497] FOX NEWS. Privacy Policy. Disponível em: <https://www.foxnews.com/privacy-policy>. Acesso em: 12 abr. 2021.

Para evitar essa coleta ampla, contudo, a política de privacidade ensina que o usuário pode fazer o *download* do aplicativo *AppChoices* para desativar a publicidade com base em interesses em aplicativos para dispositivos móveis ou ativar o acompanhamento de anúncios com limite ou configurações semelhantes no dispositivo móvel. Muito interessante.

O *NY Times*[498] também comenta rapidamente sobre a existência do aplicativo específico de controle dos *cookies*, mas não segue a mesma linha de transparência direta. Nos dois aplicativos, também há certo *disclaimer* acerca do compartilhamento voluntário de informações pessoais sensíveis, o que parece questionável.

Diga-se: embora seja aderente à tutela da privacidade que se entende como adequada a posição *standard* de recomendar que o usuário não forneça esse tipo de dados – na medida em que há inerentes riscos à atividade de provedoria de aplicações –, não parece razoável a existência dessa verdadeira cláusula de exclusão de responsabilidade. Ao menos, isso não seria viável no Brasil, pela incidência do CDC e pelas próprias balizas da LGPD.

O *Le Figaro*[499] segue a mesma linha de outros aplicativos, no sentido de que recusar publicidade segmentada significa apenas que os anúncios exibidos neste no aplicativo não serão mais adaptados aos centros de interesse do usuário. Isso não afetará ou impedirá, contudo, a exibição ou o recebimento de outros tipos de publicidade não segmentada. Também segue a linha de informar que o acesso aos dados de localização geográfica é utilizado para a exibição de notícias mais relevantes ao usuário.

Contudo, não faz muito sentido que o aplicativo se utilize deste pretexto para ter franco e contínuo acesso à exata localidade do dispositivo, na medida em que bastaria o usuário colocar a opção da cidade em que está localizado, de modo mais genérico. Apesar de fazer remissão a uma página específica sobre a política de *cookies*, o link não estava funcionando. No mais, a política de privacidade do aplicativo não acrescenta muito à discussão aqui já posta.

Como de praxe em todos os aplicativos analisados, o *Le Monde*[500] estabelece que um dos casos que justifica a utilização dos dados pessoais é a existência de um interesse legítimo por parte da empresa – o que dispensaria o próprio consentimento do usuário. A particularidade nesse ponto diz respeito à descrição de uma justificativa mais elaborada, na

---

[498] NEW YORK TIMES. Privacy policy. Disponível em: <https://help.nytimes.com/hc/en-us/articles/115014892108-Privacy-policy>. Acesso em: 12 abr. 2021.
[499] LE FIGARO. Politique de confidentialité. Disponível em: <http://mentions-legales.lefigaro.fr/page/politique-de-confidentialite>. Acesso em: 12 abr. 2021.
[500] LE MONDE. Politique de confidentialité. Disponível em: <https://www.lemonde.fr/confidentialite/>. Acesso em: 12 abr. 2021.

provável tentativa de convencer o usuário a realmente continuar usando o aplicativo, ou seja, concordando, de certa forma, com o tratamento dos dados[501].

É realmente inegável que a internet trouxe desafios ímpares à mídia, principalmente quando se fala da sua qualidade impressa. Nesse quesito, a tentativa do aplicativo – assim como de outros no mesmo sentido, vide *Khan Academy*, a ser analisado na sequência – de realmente convencer o usuário a manter a publicidade via *targeting* parece aderente à tutela da privacidade que se entende como adequada.

Trata-se do equacionamento discutido em hipótese de pesquisa, entre o legítimo interesse econômico da empresa de manter as suas atividades – o que também implica a manutenção de inúmeros empregos e vasta cadeia produtiva – e a tutela da privacidade dos usuários. A solução não é simples, mas certamente o *Le Monde* ganhou muitos consentimentos livres e conscientes após esse breve trecho introdutório.

O documento parece adequado por exibir uma intuitiva tabela com os períodos de armazenamento de cada dado coletado. O mais interessante para o presente trabalho é o período de 13 meses de armazenamento dos *cookies* com vistas à publicidade comportamental, um período inferior ao estabelecido genericamente em outros documentos de privacidade lidos.

Também merece destaque a longa seção de descrição dos diversos *cookies* utilizados na plataforma, com indicação específica de onde ler suas políticas de privacidade respectivas e como revogar o consentimento previamente estabelecido. O *Le Monde* pareceu, assim, ser suficientemente transparente, o que talvez seja um sintoma da maior maturidade da Europa no tema da proteção de dados pessoais, com o RGPD vigente há mais tempo e tendo sido amplamente discutido no velho continente.

O *Der Spiegel*[502] exibe, logo no início, uma lista de fornecedores de serviços de publicidade aprovados e suas opções de desativação (o que significa desativar o rastreamento) e de informações detalhadas sobre rastreamento de publicidade. Na sequência, também são

---

[501] "Para a Editora Le Monde , esse interesse legítimo é principalmente, em um contexto de mudança na oferta de mídia na França e no mundo, para sustentar o nível de receita comercial necessário para manter sua independência como órgão de imprensa, financiar a produção de conteúdo editorial de qualidade oferecido a seus leitores, manter conteúdo livre em seus sites e aplicativos ou a existência de ofertas de assinatura de tarifa preferencial para certas categorias de assinantes (estudantes, bibliotecas escolares) , etc.). Acreditamos que este interesse legítimo, de natureza comercial, faz parte de um quadro mais amplo para a manutenção de uma imprensa livre e independente, vetor essencial à liberdade de expressão e à liberdade de opinião de uma sociedade democrática. Ao concordar em receber informações de marketing e publicidade de nossas publicações e parceiros, você contribui para manter a viabilidade econômica de nossa atividade de editoras de imprensa. Em qualquer caso, os seus direitos individuais terão sempre precedência sobre o nosso interesse legítimo e nunca utilizaremos os seus dados para fins comerciais contra a sua vontade".

[502] DER SPIEGEL. So gehen wir mit Ihren Daten um. Disponível em: <https://www.spiegel.de/extra/datenschutzerklaerung-so-gehen-wir-mit-ihren-daten-um-a-1207780.html>. Acesso em: 12 abr. 2021.

indicadas diversas ferramentas que conseguem promover o serviço *opt-out*, principalmente no âmbito de computadores.

Aqui é interessante pontuar que não parece haver uma preocupação muito nítida em diferenciar a política de privacidade dos aplicativos móveis e das ferramentas para computador, sendo que as circunstâncias fáticas de utilização e de acessos são absolutamente diversas. Termos mais específicos para cada *hardware* transpareceriam maior zelo para com a tutela da privacidade do usuário e, pelo que se imagina, não seria uma medida exatamente custosa, financeiramente, para os provedores de aplicação – e essa crítica é aplicável de modo geral a todos os documentos analisados.

Seguindo a mesma linha de transparência, a política de privacidade exibe a lista dos parceiros responsáveis pela atividade de rastreio para fins de publicidade comportamental, com a respectiva opção direta de manifestar a revogação do consentimento. Na lista específica de direitos dos usuários, há menção expressa ao artigo respectivo do RGPD.

Isso demonstra preocupação com o estrito cumprimento da lei, o que é positivo. Na mesma linha de zelo, também há demonstração específica de como o usuário pode retirar seu consentimento em cada um dos sistemas operacionais de dispositivos móveis.

O *The Guardian*[503] segue a linha de transparência do *Le Londe*, ao estabelecer como um dos objetivos do recolhimento e tratamento dos dados pessoais a venda de espaço publicitário nos sites[504]. De toda forma, o documento informa que, mesmo com a publicidade comportamental patrocinando o jornalismo, os "jornalistas são livres e muitas vezes desafiam as atividades de empresas e organizações que anunciam e patrocinam conteúdo que aparece nos sites e publicações do Guardian". Trata-se de uma informação muito relevante e preocupada com o grau de confiabilidade das informações dispostas pela aplicação. Um ponto curioso é que esta foi a única política de privacidade que tentou explicar as permissões solicitadas quando a instalação do aplicativo móvel[505].

Embora seja interessante a ideia de justificar o motivo específico da permissão – o que atinge o princípio da finalidade do tratamento do dado –, os termos de privacidade se limitaram à explicação de duas das diversas permissões solicitadas pelo aplicativo, como se viu

---

[503] THE GUARDIAN. Privacy policy. Disponível em: <https://www.theguardian.com/help/privacy-policy>. Acesso em: 12 abr. 2021.

[504] Pois, "desde a publicação da primeira edição do Manchester Guardian em 5 de maio de 1821, nosso jornalismo foi financiado em parte pela publicidade. Hoje, a publicidade digital sustenta grande parte do nosso investimento em jornalismo de alta qualidade" (tradução livre).

[505] Para tanto, o documento informa que se solicita "permissão para acessar seus detalhes de contato / perfil no seu dispositivo móvel, para que possamos adicionar ou encontrar sua conta do Guardian no seu telefone. Também pedimos permissão para acessar o armazenamento em seu dispositivo móvel, para que você possa armazenar conteúdo e ler quando estiver off-line" (tradução livre).

na seção anterior deste trabalho, o que parece apontar na direção correta da proteção dos dados pessoais, mas como um caminho ainda a trafegar.

Outro ponto positivo do aplicativo é oferecer uma página específica de explicação sobre a política de *cookies*[506], com vasta lista de quais são usados, suas respectivas políticas de privacidade e seus meios de manifestação da retirada do consentimento. Também há, ao final, uma lista de todas as principais atualizações da política de privacidade, o que demonstra zelo para com o usuário (quase uma espécie de *histórico legislativo*).

A política de privacidade do *Flipboard*[507] não merece maiores comentários, pois nada acrescenta ao que já foi discutido aqui. Contudo, é de se mencionar que o documento não pareceu muito transparente e detalhado – em comparação com outros desta categoria –, à exceção do estabelecimento do vínculo direto ao site das duas empresas responsáveis pelos *cookies* da plataforma, onde teoricamente o usuário conseguiria manifestar sua opção de revogar o consentimento.

Por fim, o aplicativo da *BBC*[508] também oferece a opção de desativar a navegação personalizada, mas informa que, mesmo com essa opção, ainda coletará informações sobre o uso da *BBC*, agora de forma anônima. Isso significa que conseguiriam ver que alguém analisou uma história específica na *BBC*, mas não se poderia atribuir aquela informação genérica ao usuário específico.

Isso vai um pouco na contramão de outros aplicativos, que informam coletar informações, mesmo que haja o consentimento, de forma pseudoanonimizada, o que tornaria inviável a identificação específica do usuário só com aquele dado: a identificação completa se daria com o confronto de outras informações relativamente anônimas que o banco de dados teria.

O mais interessante do aplicativo *BBC* é que ele informa não realizar qualquer espécie de publicidade via *targeting* de terceiros em sua plataforma. Ou seja, a atividade de *profiling* empreendida é destinada unicamente à prospecção dos serviços da própria *BBC*, e não de terceiros. Talvez isso se deva ao fato de a *BBC* ser uma corporação pública do Reino Unido.

---

[506] THE GUARDIAN. Cookie policy. Disponível em: <https://www.theguardian.com/info/cookies>. Acesso em: 12 abr. 2021.
[507] FLIPBOARD. Flipboard Privacy Policy. Disponível em: <https://about.flipboard.com/privacy/>. Acesso em: 12 abr. 2021.
[508] BBC. The BBC Privacy and Cookies Policy. Disponível em: <http://www.bbc.com/usingthebbc/privacy/privacy-policy/>. Acesso em: 12 abr. 2021.

3.3.9 Turismo, locais, mapas e navegação

Os aplicativos *Uber*, *Google Maps*, *Google Street View* e *Google Earth* são analisados em outras seções deste trabalho, razão por que dispensam maiores comentários neste momento. Por sua vez, o *99*[509] apresenta longa lista de informações obtidas dos usuários[510]. Em tese, qualquer revogação do consentimento por parte do usuário é capaz de implicar o não funcionamento do aplicativo. Outro ponto desalinhado com a lógica da LGPD é a afirmação de que "as informações fornecidas por Terceiros à *99* obedecem à disciplina própria estabelecida por tais Terceiros e poderão estar sujeitos às suas respectivas políticas de privacidade".

Ora, se o *99* recebe e utiliza as informações dos terceiros, não seria mais do que razoável esperar que, a partir desse momento, passasse a tratar os dados referidos sob o prisma de sua política de privacidade. Não entender dessa forma chancelaria a perniciosa situação de que bastaria que empresas fizessem vinculações com empresas mais *despreocupadas* com a política de privacidade para terem acesso a dados pessoais sem haver responsabilização qualquer pelo mau tratamento dos dados.

Ou seja, o *disclaimer*, já visto em outros aplicativos similares, é uma carta em branco para que as empresas cheguem a dados pessoais e potencialmente sensíveis sem cumprirem o rito da proteção da privacidade e dos dados. Um ponto interessante é o ressalto da política de *privacidade* ao fato de que a mera desinstalação do aplicativo não é suficiente para a exclusão das informações do usuário, embora isso seja pouco justificável, *a priori*. Apesar das críticas, a política de privacidade do *99* pareceu detalhada para o padrão de aplicativos nacionais.

O *Cabify*[511] começa indicando os contatos dos responsáveis pelo tratamento dos dados dos usuários, o que já denota alguma preocupação com a legislação vigente. Na seção de realização de ações de marketing, contudo, o aplicativo pareceu inadequado à lógica de menor

---

[509] 99. Política de Privacidade. Disponível em: <https://99app.com/legal/privacidade/>. Acesso em: 12 abr. 2021.

[510] "Conforme você usa o Aplicativo e/ou os Serviços da 99, inclusive durante as suas viagens, informações adicionais relativas a você podem ser obtidas pela 99, como a sua posição geográfica, rota, duração da viagem, endereço IP, navegador utilizado, informações de cookies, tipo e marca do aparelho celular, identificadores de dispositivos móveis, versão do sistema operacional, aplicativos instalados, informações sobre rede, provedor de conexão à Internet utilizado, configuração dos dispositivos, dados de software, locais habituais de embarque e desembarque, itinerários, as avaliações que você faz sobre os Serviços da 99, dados financeiros, as formas de pagamento utilizadas e seus valores, as comunicações realizadas através do Aplicativo da 99 e as comunicações realizadas entre você e a 99 por meio dos nossos canais de atendimento. Caso você não forneça qualquer das informações solicitadas, a 99 não poderá garantir a qualidade e precisão do Aplicativo e dos Serviços da 99. Nesse caso, a 99 terá o direito de excluir você da plataforma 99 imediatamente, inclusive para assegurar o funcionamento regular e seguro do Aplicativo e dos Serviços para os demais usuários".

[511] CABIFY. Política de Privacidade Brasil. Disponível em: <https://cabify.com/brazil/privacy_policy?hidden=true>. Acesso em: 12 abr. 2021.

acesso da LGPD[512]. É traçado um perfil sociológico do usuário para que haja publicidade mais efetiva no aplicativo. Embora essa possa ser a realidade de todos os aplicativos, o termo "perfil sociológico" é muito forte pode causar certa apreensão *a priori*, na medida em que não se sabe exatamente o que configuraria esse perfil. Outro aspecto relevante é o fato de que haverá publicidade por terceiros se for utilizado um serviço específico da plataforma.

Desconhece-se a funcionalidade completa da ferramenta, mas, ao que parece, trata-se de uma vantagem comercial do aplicativo. Contudo, o uso dessa vantagem comercial também implica, ao que consta, maior desrespeito à privacidade do usuário, que só poderá evitá-la com sua manifestação *opt-out*. Um ponto positivo do documento é que, diferentemente de quase todos os demais analisados – que só afirmavam genericamente o compartilhamento de informações com outras empresas do mesmo grupo econômico –, o *Cabify* lista quais são as empresas destinatárias dos dados do usuário.

O *Maps.ME*[513] merece destaque por exibir, de modo esquemático, o tipo de tratamento de dado pessoal e o respectivo fundamento para isso. Algo claro, à semelhança da ideia do quadro-resumo que já se sustentou no presente texto. Contudo, vincula a concessão do consentimento para todo o tipo de tratamento ao próprio funcionamento da plataforma, ou seja, se o usuário revogar alguma permissão previamente definida, não mais conseguirá usar a aplicação. Além disso, a política de privacidade não merece maiores comentários e pareceu pouco alinhada aos apertados requisitos da legislação europeia – ainda mais por se tratar de empresa holandesa.

Os termos de privacidade do *Waze*[514] são muito completos, detalhistas e claros, o que parece aderente à tutela da privacidade que se entende como adequada. Não há, contudo, nenhuma cláusula que chame atenção positivamente para além das já detalhadas neste trabalho.

---

[512] "Utilizaremos os seus Dados Pessoais para enviar notícias, produtos e promoções relacionados com a Cabify e com terceiros relacionados com os setores relativos a produtos e consumos. Para tal finalidade, analisaremos o seu histórico de viagens, os montantes pagos, as viagens promocionais utilizadas, a frequência com que utiliza o Serviço, o seu perfil sociológico e os seus interesses pessoais e criaremos um perfil acerca de si para que as promoções enviadas sejam personalizadas, de maneira que se adaptem, em cada momento, às suas necessidades e preferências pessoais. Considere que, em qualquer momento, poderá pedir deixar de analisar o seu perfil, mesmo que isso implique que não receberá mais notícias, ofertas e promoções. O perfil que criarmos acerca de si não será utilizado para outra finalidade que não seja a da personalização das nossas promoções. Também enviaremos comunicações de terceiros sobre os setores relativos a produtos e consumos que pensamos que possam ser do seu interesse de acordo com o seu perfil se nos dá o seu consentimento de maneira específica. Só enviaremos estas comunicações se, além disso, utiliza o serviço Wi-Fi da Cabify. Tenha em consideração que, poderá utilizar o serviço Wi-Fi sem necessidade de aceitar receber comunicações de terceiros. Em qualquer caso, tenha em mente que poderá cancelar essas comunicações em qualquer momento. Para isso, basta simplesmente fazer clique no link "Cancelar" contido em qualquer uma das comunicações".

[513] MAPS.ME. Maps Me Privacy Policy. Disponível em: <http://legal.my.com/us/maps/privacy/>. Acesso em: 12 abr. 2021.

[514] WAZE. Waze Privacy Policy. Disponível em: <https://www.waze.com/pt-BR/legal/privacy>. Acesso em: 12 abr. 2021.

Nesse caso, contudo, nada mais natural que um aplicativo de navegação tenha acesso à localização precisa do aparelho; mas, daí para utilizar esse dado para fins de publicidade comportamental, há um longo caminho a ser percorrido no âmbito do teste de proporcionalidade[515]. E isso sobretudo porque não faz sentido que o próprio usuário revogue essa permissão de acesso ao local do dispositivo – sob pena de ficar sem funcionalidade o aplicativo –, o que implica sempre haver a referida publicidade de segmentação, sem possibilidade de revogação.

O *Trivago*[516] já começa apresentando referências específicas aos artigos do RGPD. Outro ponto que merece destaque é o fato de o aplicativo utilizar, para tornar viável a inscrição em seu newsletter, "o método *double opt-in*"[517]. Trata-se de um exemplo de destaque – por dar valor ao consentimento prévio mais estreito do usuário – em um universo de ferramentas que, quase indistintamente, utiliza o método *opt-out*.

E o padrão do aplicativo continua elevado, ao informar que os plug-ins da plataforma (*Facebook*, *YouTube*, *Twitter*, *LinkedIn*, *Pinterest* e *Xing* – todos devidamente identificados, aliás) só começam a funcionar se o usuário clicar no respectivo símbolo e lhe der consentimento para que os dados sejam transmitidos ao respectivo fornecedor.

Ou seja, mais uma manifestação da *opt-in*, com expressa referência ao artigo do RGPD aplicável. A política de privacidade também elenca detalhadamente todas as ferramentas que utiliza para empreender análise estatística da plataforma, bem como as respectivas políticas de privacidade. Todos esses fatos demonstram que o *Trivago* parece alinhado à boa tutela dos dados pessoais e da privacidade.

O aplicativo *Decolar*[518] não merece maiores comentários, na medida em que seus termos de privacidade são genéricos. O único ponto interessante e que parece aderente à tutela da privacidade que se entende como adequada é a menção expressa à legislação brasileira[519].

---

[515] Veja-se: "as informações e anúncios que você vê ao acessar os Serviços podem ser segmentados com base em sua atividade atual do Waze, como sua localização atual, seu destino ou informações contextuais com base na sua sessão de unidade atual. Por exemplo: se você pesquisar por "posto de gasolina", poderá ver um anúncio de um posto de gasolina local".

[516] TRIVAGO. Trivago's privacy policy. Disponível em: <https://www.trivago.com/privacy-policy>. Acesso em: 12 abr. 2021.

[517] De acordo com a própria empresa: "Isso significa que depois de se inscrever, enviaremos um e-mail para o endereço de e-mail especificado, no qual pedimos que você confirme que deseja receber o boletim informativo. Se você não confirmar sua inscrição em [24 horas], suas informações serão bloqueadas e excluídas automaticamente após um mês" (tradução livre).

[518] DECOLAR. Política de Privacidade Decolar. Disponível em: <https://comercial.decolar.com/br/confidentiality>. Acesso em: 12 abr. 2021.

[519] Veja-se: "a Decolar resguarda suas Informações Pessoais de acordo com os padrões e procedimentos de segurança e confidencialidade vigentes no Brasil conforme inciso X do artigo 5º da Constituição Federal, artigo 43 da Lei 8078/90, Lei 12.737/2012 e legislação correlata". Na mesma linha, o documento informa que, "no Brasil, os usuários, titulares das Informações Pessoais têm reconhecidos e poderão exercer os direitos de acesso,

Embora haja essas menções expressas, faltaram as remissões ao Marco Civil da Internet e, em posição de vanguarda, à LGPD.

O *Booking*[520] inicia tentando realmente cativar o usuário[521]. Na sequência, demonstrando ser um verdadeiro contrato de adesão, o documento faz a seguinte afirmação: "esta parte é triste, mas necessária: se você discordar desta Política de Privacidade, você deve parar de utilizar nossos serviços. Se você concordar com nossa Política de Privacidade, você está pronto para fazer sua próxima reserva. Deixe a diversão rolar!".

Também chama atenção o fato de o aplicativo se "esforçar" para compartilhar o endereço de e-mail do usuário com terceiros interessados em marketing de forma criptografada, o que evitaria a possibilidade de identificação pessoal. Contudo, o termo "esforçar" é fluido e nada garante ao usuário.

Há seção especificamente destinada aos aplicativos móveis, onde se ressalta o fato de que o rastreamento dos usuários é pré-definido, mas pode ser manifestada a opção de retirada do consentimento pelo consumidor. Quanto aos *cookies* utilizados, também há longa explicação sobre como desativá-los, inclusive com menção expressa aos links dos grupos *Network Advertising Initiative* e *Interactive Advertising Bureau*. De modo geral, a política é transparente e aderente à tutela da privacidade que se entende como adequada.

A política de privacidade do *TripAdvisor*[522] também não merece comentários adicionais, já que perfeitamente alinhada às outras já aqui estudadas. Não pareceu tão completa quanto a do *Booking* e de outros aplicativos aqui avaliados, mas pareceu suficientemente aderente à tutela da privacidade que se entende como adequada.

Há cláusulas que indicam como funciona a publicidade comportamental com base nas pesquisas do usuário – ao perceber que o usuário está pesquisando hotéis em Londres, por exemplo, o aplicativo já automaticamente percebe o interesse e começa a direcionar anúncios

---

cancelamento e atualização das suas Informações Pessoais, bem como a opor-se ao tratamento das mesmas e a ser informados sobre as cessões realizadas, de forma gratuita em intervalos não inferiores a seis meses, salvo que se comprove um interesse legítimo ao efeito conforme o estabelecido artigo 43 da Lei 8078/90". Trata-se quase de uma decorrência do próprio direito fundamental à impetração do habeas data, mas ainda está em patamar inferior aos novos direitos estabelecidos justamente pela LGPD, cuja menção seria ainda mais interessante para a empresa.

[520] BOOKING. Política de Privacidade. Disponível em: <https://www.booking.com/content/privacy.pt-br.html?label=gen173nr-1FCBQoggJCB3ByaXZhY3lIHFgEaCCIAQGYARy4AQbIAQzYAQHoAQH4AQKIAgGoAgO4AtOayuUFwAIB&sid=51b8c4d59804d2478b5ba971f8448cb7&tmpl=docs%2Fprivacy-policy&lang=pt-br&soz=1&lang_click=top;cdl=nl;lang_changed=1>. Acesso em: 12 abr. 2021.

[521] Veja-se: "antes de tudo – sua privacidade é importante para nós. Sabemos que todas as políticas falam isso, mas honestamente, é verdade. Você confiou em nós ao usar os serviços da Booking.com e valorizamos sua confiança. Isso significa que nos comprometemos a proteger os dados que você nos fornecer. Nós agimos de acordo com o interesse de nossos clientes e somos transparentes sobre o processamento dos seus dados pessoais".

[522] TRIPADVISOR. Privacy Policy. Disponível em: <https://tripadvisor.mediaroom.com/us-privacy-policy>. Acesso em: 12 abr. 2021.

de pacotes e outros para a cidade; isso, sustenta-se, é até positivo, pois dá maiores opções ao consumidor, permitindo que ele tenha a comparação de modo fácil – e na sua localização geográfica, mas nada que demande especial atenção.

O *Airbnb*[523] chama atenção pelo tamanho de sua política de privacidade, detalhada – e, até mesmo, excessivamente grande, o que acaba dificultando a correta compreensão pelo usuário. Na sequência, uma cláusula parece contraditória: a ferramenta afirma compartilhar informações pessoais com plataformas de mídias sociais com vistas à promoção dos próprios produtos da *Airbnb* em razão de seu legítimo interesse, mas apresenta uma escusa de responsabilidade pelo tratamento que essas mídias sociais podem dar aos dados pessoais dos usuários.

Ora, se há um legítimo interesse da empresa na origem do compartilhamento do dado, ela também deveria se responsabilizar pelo tratamento dispensado pelas outras empresas da cadeia; do contrário, o legítimo interesse parece ser uma via de mão única, sem quaisquer ônus à empresa da origem e que efetivamente teve a relação de coleta de dados com o usuário. Sustenta-se que o legítimo interesse deve, no mínimo, vir acompanhado do adequado rastreamento dos dados com a aferição de como eles estão sendo tratados e protegidos por qualquer destinatário do compartilhamento.

Também há uma longa lista de empresas do mesmo grupo econômico que são destinatárias dos dados coletados dos usuários, com a respectiva explicação de como se dá esse compartilhamento – o que é interessante e transparente. Em outra cláusula relevante, a plataforma diz "revisar, rastrear ou analisar suas comunicações com outros usuários por meio da Plataforma *Airbnb*", com base em um suposto legítimo interesse de garantir a conformidade com as leis aplicáveis e evitar fraudes.

A justificativa é boa, mas não fica exatamente claro se há o *scan* de todas as mensagens enviadas, independentemente de qualquer suspeita de fraude. Se assim for, o procedimento de análise pode ser amplo demais para o fim pretendido, ainda mais porque pode ser feito manualmente.

Também há longa explicação sobre os direitos dos usuários e como se dá a operação global da plataforma – em nítida preocupação aos limites geográficos do compartilhamento dos dados pessoais, o que foi comentado neste trabalho. Apesar das poucas críticas, os termos do aplicativo pareceram adequados à tutela da privacidade que se entende como adequada.

---

[523] AIRBNB. Política de Privacidade do Airbnb. Disponível em: <https://www.airbnb.com.br/terms/privacy_policy>. Acesso em: 12 abr. 2021.

Por fim, o *Skyscanner*[524] tem uma política de privacidade completa e aderente à tutela da privacidade que se entende como adequada. Como exemplo, diferentemente de outros aplicativos aqui analisados – que se limitam a dizer que nenhum sistema informático é 100% seguro e que, por isso, não responderiam por eventuais falhas –, o documento de privacidade da empresa corrobora a posição, mas não cria o *disclaimer*, preferindo enfatizar as suas ações proativas para minorar os riscos de indevido acesso amplo aos dados pessoais de seus clientes[525].

Outro ponto interessante do documento do *Skyscanner* é a sua linguagem fácil e próxima ao seu típico usuário[526]. Com explicações claras, quase todos os usuários devem concordar em manter o rastreamento e os *cookies* ativos. Aliás, o documento de privacidade também faz remissão à política de *cookies*, novamente aderente à tutela da privacidade que se entende como adequada, inclusive com várias referências a como retirar o consentimento no rastreio de dados.

3.3.10 Educação

O *Duolingo*[527], à semelhança de outros aplicativos aqui analisados, também utiliza a tecnologia *Google Analytics* para aferição do grau de interação do usuário com a plataforma. A vantagem é a possibilidade de manifestar o interesse em não participar da coleta desses dados.

Ao comentar sobre os links de sites de terceiros, o aplicativo informa que não controla esses outros sites e não é responsável por seu conteúdo, suas políticas de privacidade ou seu uso de dados pessoais, incluindo informações pessoais ou financeiras. Ademais, informa

---

[524] SKYSCANNER. Privacy Policy. Disponível em: <https://www.skyscanner.net/media/privacy-policy>. Acesso em: 12 abr. 2021.

[525] Veja-se: “infelizmente, nenhum site ou aplicativo pode garantir segurança completa, mas criamos um programa de segurança para toda a organização, projetado para manter seus dados pessoais o mais seguros possível. Ele usa uma variedade de medidas de segurança técnica, organizacional e administrativa e técnicas de melhores práticas, dependendo do tipo de dados sendo processados”. E, “para garantir que mantemos uma cultura de "Privacidade por design", fornecemos proteção completa de dados e treinamento de privacidade a todos os funcionários do grupo Skyscanner. Desenvolvemos nossos serviços com o objetivo de usar a quantidade mínima de dados pessoais possíveis, incluindo o uso de técnicas de minimização de dados, como anonimização e pseudonimização. Além disso, sempre que desenvolvemos ou atualizamos nossos serviços de maneiras que envolvem a coleta ou o uso de novas formas de dados pessoais, realizamos uma avaliação de impacto sobre a privacidade para entender e reduzir a probabilidade de qualquer impacto indesejado sobre você” (tradução livre).

[526] Veja-se o seguinte trecho, que tenta convencer o usuário acerca da importância de permitir que haja publicidade comportamental na plataforma: “anúncios personalizados para você com base em informações coletadas por nós ou por Soluções de anúncios de terceiros enquanto você usa nossos serviços, como sua localização geral (por cidade ou país) e suas pesquisas no Skyscanner ou histórico de reservas (“Informações relacionadas ao Skyscanner”). Por exemplo, se você reservou um voo para Roma, verá anúncios sobre hotéis em Roma, em vez de hotéis em Paris (Paris é adorável, mas isso pode ser um pouco chato!)”.

[527] DUOLINGO. Privacy Policy. Disponível em: <https://www.duolingo.com/privacy>. Acesso em: 11 abr. 2021.

que a inclusão de tais links pelo *Duolingo* não implica qualquer endosso do conteúdo nesses sites ou de seus proprietários ou operadores. Esse parece ser o padrão dos aplicativos, embora inadequado à boa tutela dos dados pessoais.

Outro ponto interessante é que, à semelhança de outros aplicativos, o *Duolingo* explicita um requisito legal específico dos Estados Unidos. Com efeito, a Seção 1798.83 do Código Civil da Califórnia autoriza os residentes do Estado da Califórnia a solicitarem de uma empresa, com quem esse residente tem uma relação comercial estabelecida, determinadas informações sobre os tipos de dados pessoais que a empresa compartilha com terceiros para fins de marketing direto por tal terceiro e as identidades dos terceiros com quem a empresa compartilhou tais informações durante o ano civil imediatamente anterior.

Quando o usuário é o público infantil, o *Duolingo* afirma que "apenas anúncios amigáveis para a família são exibidos e esses anúncios não fazem rastreamento comportamental". Outro ponto desalinhado com a lógica da LGPD é o fato de o aplicativo informar que não foi projetado para responder a sinais "não rastrear" enviados por alguns navegadores. Dois pontos que merecem o alerta dos usuários, na medida em que os anúncios *amigáveis* são um conceito muito fluido – acabando por incentivar a própria publicidade infantil, que, embora aceita no ordenamento jurídico brasileiro, é submetida a uma série de regras mais estreitas.

Por sua vez, o *Babbel*[528], não muito diferente de todos os outros aplicativos aqui analisados, afirma que utiliza "prestadores de serviços externos com o objetivo de otimizar nossos serviços, realizar atividades de publicidade ou analisar nosso site em busca de erros e em termos de seu desempenho", fornecendo uma lista com cinco prestadores de serviços e suas respectivas políticas de privacidade, o que é interessante.

O *TED*[529] também informa utilizar tecnologias de rastreamento via *cookies*, dentre quais o *Google Analytics* e o equivalente do *Facebook*. Isso porque, de acordo com a política de privacidade, os *cookies* fornecem um mecanismo que entende como o usuário usa o site ao longo do tempo, para que se possa oferecer ao usuário a melhor experiência de acordo com suas preferências expressas.

Informa, contudo, que o aplicativo não vende essas informações a terceiros, mas pode fornecer informações a parceiros que auxiliam na atualização, gerenciamento ou

---

[528] BABBEL. Privacy Statement for Babbel. Disponível em: <https://about.babbel.com/en/privacy/>. Acesso em: 11 abr. 2021.

[529] TED. Privacy Policy. Disponível em: <https://www.ted.com/about/our-organization/our-policies-terms/privacy-policy>. Acesso em: 11 abr. 2021.

manutenção dos sites. Outro ponto relevante é informação de que há coleta de dados de localização por padrão, o que não parece exatamente guardar muita relação com a funcionalidade principal do aplicativo.

O usuário, se desejar, pode fazer a opção de revogar a permissão tácita para a coleta desses dados. Especificamente sobre a publicidade comportamental, o aplicativo informa que os dados coletados e tratados só são utilizados para que se promovam propagandas do próprio aplicativo, incluindo educação gratuita. Na sequência, o documento lista uma série de funcionalidades específicas do programa, que podem coletar e tratar dados determinados, conforme lista detalhada ali colocada.

Outro ponto interessante é que a política de privacidade do *TED* explicita algumas alterações feitas no documento em virtude da entrada em vigor do RGPD. De mais relevante: (i) maior detalhamento da política, especificamente quanto aos dados de como o aplicativo processa, armazena e gerencia seus dados; (ii) acréscimo de opções de consentimento para a coleta dos dados, aparentemente diminuindo o escopo da coleta automatizada; (iii) atualização de contratos com os terceiros processadores dos dados do usuário, para garantir que eles também sigam as regras mais apertadas de proteção à privacidade.

E ainda: (iv) modificação de processos internos para garantir que o usuário tenha rápido conhecimento em casos de violação à integridade de sua tutela privada; e (v) criação de uma maneira de os usuários entrarem em contato com o aplicativo, a fim de que solucionem todas as suas demandas legítimas extrajudicialmente. A explicitação das mudanças é aderente à transparência esperada dos provedores de aplicação.

O primeiro ponto interessante a ser observado sobre a *Khan Academy*[530] é o fato de, logo no topo do site, constar um selo de signatário do juramento pela privacidade dos usuários. Esse tipo de campanha também foi observada quando da análise dos aplicativos *CNN* e *Fox News*. A parte realmente relevante dessa prática é que estimula as empresas a tutelarem ainda mais a privacidade.

No futuro iminente, espera-se que esse selo tenha real valor e consideração pelo usuário, na medida em que significará a diferença entre um aplicativo que oferece risco à sua privacidade e outro que não – hoje, pode-se pensar na diferença entre os protocolos *http* e *https*, por exemplo; certamente o usuário fica muito temerário em fazer uma compra, com a inserção de seus dados pessoais e bancários, em um site que não seja considerado, por protocolo da internet, seguro.

---

[530] KHAN ACADEMY. Khan Academy Privacy Policy. Disponível em: <https://www.khanacademy.org/about/privacy-policy>. Acesso em: 11 abr. 2021.

O documento começa, nessa esteira, informando que o aplicativo não vende as informações do usuário a terceiros, na medida em que se trata de mera organização sem fins lucrativos, cuja missão é a educação, com a melhor experiência de aprendizado, e não a venda de produtos. Isso parece aderente à tutela da privacidade que se entende como adequada.

Porém, não parece fazer muito sentido a coleta de informações de localização, ainda que não se trate da localização exata. Embora comece assim, também se rende à necessária realidade da publicidade comportamental para os aplicativos pretensamente gratuitos. Aqui, contudo, a publicidade parece mais restrita[531].

Entretanto, o documento ensina exatamente o usuário a fazer a opção por não mais permitir o rastreamento para fins de anúncios dirigidos, tanto na plataforma *Android* quanto *iOS*. Um ponto relevante aqui, contudo, diz respeito ao fato de que os vídeos da plataforma são exibidos por meio do *YouTube* e, por isso, o aplicativo afirma não se responsabilizar pela coleta especificamente realizada pela empresa.

De fato, isso até faz certo sentido, mas é impensável que a plataforma tente usar a sua "incapacidade" de ter um meio próprio para chancelar a coleta de dados de acordo com as políticas do próprio *software* de exibição dos vídeos. O *Khan Academy Kids*[532] segue a mesma linha, com a principal diferença de efetivamente vedar taxativamente a existência de publicidade direcionada, na medida em que não se permite que terceiros coletem as informações.

---

[531] Veja-se: "*Conteúdo Patrocinado* A Khan Academy não exibe anúncios de terceiros no Serviço. De tempos em tempos, permitimos que terceiros patrocinem conteúdo exibido em nosso Serviço. Por exemplo, organizações com fins lucrativos podem desejar patrocinar todo o conteúdo relacionado a um tópico educacional específico, como astronomia ou biologia. O conteúdo patrocinado sempre será rotulado (por exemplo, "Patrocinado por ___"). A Khan Academy não compartilha informações pessoais de nossos usuários com esses patrocinadores sem o consentimento explícito, e esses patrocinadores não têm a capacidade de rastrear ou coletar informações sobre os visitantes ou usuários de nosso site. Como uma organização sem fins lucrativos, a Khan Academy depende de nossos patrocinadores, doadores e outros colaboradores para fornecer o financiamento necessário para fornecer o serviço gratuito aos nossos usuários. Por favor note: De tempos em tempos, podemos exibir conteúdo de vídeo do YouTube criado por terceiros e não pela Khan Academy. Embora o conteúdo de vídeo criado pela Khan Academy não exiba anúncios em vídeo, o conteúdo de terceiros pode incluir publicidade que não podemos controlar.
Publicidade Baseada em Interesse A Khan Academy não exibe anúncios direcionados em nosso serviço. No entanto, participamos de publicidade com base em interesses e usamos empresas de publicidade de terceiros para veicular anúncios segmentados em outros sites, aplicativos ou serviços, incluindo no Facebook e em outras redes sociais, ou em outros dispositivos que você possa usar. Essas redes de anúncios de terceiros usam tecnologias de rastreamento para reconhecer seu navegador ou dispositivo e coletar informações sobre sua visita ao nosso Serviço para fornecer conteúdo personalizado, publicidade e mensagens comerciais que podem ser mais relevantes para seus interesses, bem como fornecer publicidade serviços relacionados, como relatórios, atribuição, análise e pesquisa de mercado".

[532] KHAN ACADEMY. Khan Academy Kids Privacy Policy. Disponível em: <https://www.khanacademy.org/kids/privacy-policy>. Acesso em: 11 abr. 2021.

Contudo, o aplicativo informa poder fazer anúncios patrocinados sobre si quando o usuário estiver usando outras ferramentas. O *Google Classroom* e o *Tradutor*[533] dispensam maiores comentários, na medida em que apenas mantêm a orientação padronizada de todos os produtos da *Google*, já explicadas.

O *Kahoot!*[534] possui um *disclaimer* relevante: não se responsabiliza pelo vazamento de eventuais informações sensíveis compartilhadas voluntariamente pelo usuário (número de seguridade social, informações sobre origem racial ou étnica, opiniões políticas, religião, crenças, saúde, biometria, características genéticas, associação a sindicatos ou fundos). Esse pretenso afastamento da responsabilidade é nulo e, em verdade, pode constituir verdadeira cláusula abusiva pelo CDC.

O *Brainly*[535] segue a tradicional segregação de coleta dos dados pessoais entre aqueles voluntariamente fornecidos pelo usuário e os obtidos quando da utilização do serviço. Nas bases jurídicas para o processamento dos dados, há menção aos legítimos interesses do provedor e à necessidade de execução de contratos, além do cumprimento de deveres legais ou regulamentares. Ao final, há uma tabela elucidativa com a categoria de dado pessoal coletado com os respectivos objetivos daquele processamento e a base legal autorizativa, o que caminha alinhado às boas práticas previstas nas normas de proteção de dados, inclusive a LGPD.

Sobre a privacidade das crianças, é interessante observar que a plataforma criou uma espécie de canal de denúncias para ajudá-la a excluir todos os dados pessoais retidos de crianças com menos de 13 anos de idade. Aliás, como o aplicativo é mais voltado ao público infantil – já que é um grande *chat* para dúvidas sobre estudos –, pensa-se que o critério etário para a não coleta dos dados deveria ser até um pouco maior, como os 16 anos vistos em outros aplicativos aqui analisados.

3.3.11 Produtividade e antivírus

O *McAfee*[536] adverte que pode "coletar outras informações de ou sobre você, como informações sobre quais produtos você comprou, seus interesses, informações demográficas, fotografias e vídeos e dados biométricos, como impressões digitais ou impressões de voz", bem

[533] GOOGLE. Privacidade & Termos. Disponível em: <https://policies.google.com/privacy>. Acesso em: 11 abr. 2021.
[534] KAHOOT!. Privacy Policy. Disponível em: <https://kahoot.com/privacy-policy/>. Acesso em: 11 abr. 2021.
[535] BRAINLY. Priavcy policy. Disponível em: <https://brainly.com/pages/privacy_policy>. Acesso em: 13 abr. 2021.
[536] MCAFEE. Aviso de privacidade da McAfee. Disponível em: <https://www.mcafee.com/enterprise/pt-br/about/legal/privacy.html>. Acesso em: 11 abr. 2021.

como coletar automaticamente informações sobre os dispositivos em que o aplicativo está instalado, o que é extensível inclusive a outros dispositivos conectados à mesma rede.

O aplicativo também informa coletar informações de terceiros, inclusive dados atualizados de pagamento, endereço e registros de crédito. Além disso, informa coletar dados de localização geográfica, o que, *a priori*, não parece guardar muita relação com as funcionalidades oferecidas.

Na linha do comentado no presente trabalho – de que o aplicativo gratuito, em verdade, tem um custo embutido –, o *McAfee* torna isso explícito com o seguinte trecho: "Nós disponibilizamos uma variedade de produtos para nossos clientes sem nenhum custo. Para manter esses produtos gratuitos, podemos usar as informações coletadas por meio deles, como os sites que você visita ou os aplicativos para celular que você usa, para permitir que a *McAfee* e outras pessoas mostrem anúncios direcionados a seus interesses".

Como *disclaimer*, entretanto, o aplicativo informa que as informações não identificam pessoalmente o usuário, proibindo que os terceiros façam a mesma coisa por meio de contratos – fica a dúvida, entretanto, de qual é a real confiabilidade desse contrato entre as empresas para o usuário. O aplicativo também informa ser possível a revogação do consentimento específico para esse fim no menu de configurações da plataforma.

Especificamente quanto à privacidade das crianças, o aplicativo informa que só utiliza os seus dados pessoais – após o devido consentimento dos pais – para entregar as funcionalidades do próprio *software*. Ou seja, não há escopo para a publicidade comportamental em dispositivos usados pelo público infantil. Também há trecho especificamente preocupado com a política de privacidade aos usuários europeus – em razão do RGPD –, cujos principais apontamentos são os mecanismos de transferências de dados e de acesso, retificação e apagamento das referidas informações.

Por sua vez, o *Kaspersky*[537] também informa que uma das finalidades da coleta e tratamento de dados dos usuários é "melhorar a interação do usuário e experiência com nossos produtos e serviços, em particular, alterando interfaces e fornecendo os conteúdos e anúncios desejados, em relação ao anúncio com fins de Marketing". A política de privacidade informa que há dados cujo fornecimento é obrigatório – sob pena de não funcionamento da aplicação –, mas que também há aqueles passíveis de revogação de consentimento pelo usuário.

Na sequência, a aplicação informa nunca processar dados pessoais sensíveis, como religião, preferência sexual, opiniões políticas ou outras categorias especiais de dados. No

[537] KASPERSKY LAB. Política de privacidade de produtos e serviços. Disponível em: <https://www.kaspersky.com.br/products-and-services-privacy-policy>. Acesso em: 11 abr. 2021.

mesmo sentido, também afirma que não processa quaisquer dados pessoais de crianças, desde que os pais informem que se trata de um dispositivo infantil. Como é regra no mercado, o aplicativo informa que também compartilha as informações fornecedores[538], elencando alguns direitos do usuário[539].

Na sequência, o documento expressa os princípios que norteiam a tutela da privacidade pela empresa: (i) escolha e consentimento, que deve ser livre, específico e fundamentado; (ii) especificação e legitimidade da finalidade; (iii) limitação e processamento de dados para o que estiver dentro dos limites da legislação aplicável e estritamente necessário para as finalidades especificadas; (iv) limitação do uso, da retenção e divulgação para que o que é necessário para atender específicos, expressos e legítimos; (v) precisão e qualidade; (vi) liberdade, transparência e aviso; e (vii) participação e acesso individuais, dando ao usuário a possibilidade real de acesso aos seus dados e de eventual correção.

Parece aderente à tutela da privacidade que se entende como adequada a posição da empresa: embora todos os princípios sejam mera decorrência legal, é relevante que a empresa os coloque em sua página principal, sobretudo porque denota uma posição de zelo e preocupação. Nesse quesito, as aparências são muito importantes e eloquentes.

Na sequência, o *AVG*[540] (as mesmas ideias se aplicam ao *Avast*[541], na medida em que as empresas são coligadas) inicia afirmando que pensou sua política de privacidade de acordo com os requisitos estabelecidos no RGPD. Assim, informa que, para "determinados produtos para dispositivos móveis, oferecemos anúncios de terceiros"[542].

No que tange ao compartilhamento dos dados pessoais com terceiros para eventuais fins de publicidade comportamental, o documento informa que é viável ao usuário desativar

---

[538] "Fornecedores que prestam serviços para nós, incluindo empresas que fornecem processamento de dados, análise da web, publicidade, distribuição de e-mail, processamento de pagamentos, preenchimento de pedidos, e outros serviços"

[539] "Obter confirmação de que temos dados pessoais sobre você, solicitar acesso e receber informações sobre seus dados pessoais, receber cópias de seus dados pessoais fornecidos a nós, também em formato legível por máquina, e enviá-lo a outro controlador de dados, onde tecnicamente possível, atualizar e fazer correções em seus dados pessoais, se opor ao processamento de seus dados pessoais, e ter as informações bloqueadas, anônimas ou excluídas, conforme apropriado, bem como registrar uma queixa com uma autoridade supervisora".

[540] AVG. Política de Privacidade. Disponível em: <https://www.avg.com/pt-br/privacy>. Acesso em: 11 abr. 2021.

[541] AVAST. Política de Privacidade. Disponível em: < https://www.avast.com/pt-br/privacy-policy>. Acesso em: 11 abr. 2021.

[542] O contrato ainda esclarece que, "Embora não compartilhemos os seus dados pessoais com a rede de publicidade, os dados do seu dispositivo, incluindo o endereço IP, são usados pela rede de publicidade para permitir a exibição dos anúncios. Caso não queira visualizar anúncios de terceiros, você tem a escolha de mudar para uma versão paga do produto. Se você receber um anúncio de terceiros e clicar no anúncio, os seus dados serão regidos pelo terceiro em cujo anúncio você clicou".

esse recurso, mesmo nos produtos gratuitos. Nessa situação, o que deve vigorar é aquela posição não incomum de que continuará havendo publicidade, mas ela não mais será direcionada[543].

Denotando mais transparência ainda, o documento fornece a lista de todos os *cookies* utilizados pelo *software*, com sua respectiva finalidade. Na sequência, a política de privacidade também explicita, para cada funcionalidade do aplicativo, quais são os dados coletados e a respectiva finalidade, o que pareceu alinhado às funções específicas de cada segmento. O conjunto *AVG-Avast* parece ter política de privacidade adequada.

O *Clean Master*[544] informa que uma das opções de *login* do usuário é por meio de sua rede social, da qual a única informação necessária seria o e-mail. Ou seja, todos os demais dados só seriam importados se o usuário consentisse.

Resta saber, contudo, se essa informação é claramente prestada ao usuário quando da utilização do aparelho; se a opção pré-marcada for de fornecimento integral dos dados – sem nenhum aviso da possibilidade de fornecimento só do e-mail –, a previsão da política de privacidade é inócua, na medida em que dificilmente surtirá efeitos práticos.

Na sequência, o aplicativo informa que, com base no consentimento do usuário, pode trabalhar e compartilhar algumas informações pessoais com parceiros de publicidade terceirizados para fornecer anúncios ou outros conteúdos personalizados. Há indicação de links específicos para a política de anúncios e para as políticas específicas dos parceiros publicitários. Também informa compartilhar informações relacionadas aos usuários do serviço com afiliadas ou terceiros não afiliados de forma agregada e não identificada.

Contudo, adverte que, embora essas informações não identifiquem pessoalmente o usuário, em alguns casos, essas partes podem ser capazes de combinar essas informações agregadas e desidentificadas com outros dados que têm sobre o usuário ou que recebem de outras partes, de maneira que lhes permita identificar pessoalmente o próprio usuário.

---

[543] "Para podermos oferecer gratuitamente os nossos serviços, exibimos anúncios de terceiros nos aplicativos para dispositivos móveis por meio de redes de publicidade populares, como a AdMob da Google, o MoPub do Twitter, a InMobi e o Audience Network do Facebook. Exibimos um logotipo do AdChoices em cima de todos os anúncios. Você pode clicar no ícone para saber mais sobre a rede de publicidade e encontrar opções de personalização por meio dessa rede. Para ativar o anúncio, incorporamos um kit de desenvolvimento de software (Software Development Kit, SDK) de terceiros para esses anúncios. O código SDK é oferecido por agências de publicidade ou redes de terceiros. Os dados dos nossos usuários com produtos gratuitos para dispositivos móveis permanecem anônimos, para nós e para as agências de publicidade de terceiros. No entanto, o código SDK das agências de publicidade coletará dados para criar perfis para adaptar os anúncios a você. O SDK poderá coletar informações, como os aplicativos de terceiros que você instalou no dispositivo, o identificador de publicidade do Android, o endereço IP, os detalhes do sistema operacional e o endereço MAC do seu dispositivo, além de outras informações estatísticas e técnicas. Se você não quiser visualizar anúncios de terceiros, poderá desinstalar o produto gratuito para dispositivos móveis e/ou escolher uma versão paga do produto para dispositivos móveis, que não veicule anúncios de terceiros".

[544] CHEETAH MOBILE CLEAN MASTER. Privacy Policy. Disponível em: <https://www.cmcm.com/protocol/site/privacy.html>. Acesso em: 11 abr. 2021.

Essa informação é muito relevante e desalinhada com a lógica da LGPD, na medida em que acaba constituindo verdadeiro *disclaimer* ao dever de anonimização, já que transfere a responsabilidade pela pretensa identificação aos terceiros responsáveis pelo tratamento dos dados. Se é possível que eles identifiquem o usuário a partir da agregação das informações disformes fornecidas, é porque os dados ainda guardavam um pouco de pessoalidade – o que é vedado pela legislação.

O aplicativo, à semelhança do *Kaspersky*, também elenca um rol de direitos básicos do usuário. O único detalhe é que os direitos são ali previstos apenas na seção destinada aos usuários da União Europeia. Dentre eles, destacam-se os direitos: (i) de retirar o consentimento; (ii) de acessar e retificar os dados; (iii) de ser esquecido; (iv) de promover a restrição aos dados; (v) de objetar o processamento; (vi) de solicitar a portabilidade dos dados; (vii) de identificação e notificação de terceiros que tenham sido destinatários dos dados; (viii) de objetar a tomada de decisão automatizada, inclusive a construção de perfil; e (ix) de apresentar queixas. Fica o questionamento acerca do motivo de esses direitos só estarem expressos na seção destinada aos usuários europeus.

Quanto ao *Adobe Reader*[545], não há maiores destaques além daqueles já feitos. O único ponto aqui é que, eminentemente, a empresa afirma compartilhar as informações pessoais dentro da própria família de *softwares*, escopo em que a finalidade também pode ser a publicidade via *targeting*. Parece não ser feito nenhum compartilhamento externo para fins de mera publicidade comportamental, o que é adequado à tutela adequada dos dados pessoais[546].

No que tange ao *MS Word*, a política de privacidade genérica da *Microsoft*[547] é algo que recebe, de modo geral, a primeira crítica. Com efeito, seria no mínimo esperado que a *Microsoft*, empresa do porte que é, tivesse uma política de privacidade específica para cada de suas aplicações; ou, no mínimo, que houvesse um documento diferente para as ferramentas destinadas a computadores e a dispositivos móveis, na medida em que a diferença técnica é notória. Ao revés, optou-se por cláusulas mais genéricas.

Diferente do *Adobe*, o *MS Word* afirma usar os dados pessoais para "anunciar e comercializar, incluindo o envio de comunicações promocionais, o direcionamento de anúncios

---

[545] ADOBE. Política de privacidade da Adobe. Disponível em: <https://www.adobe.com/br/privacy/policy.html>. Acesso em: 11 abr. 2021.

[546] O compartilhamento externo só é feito se a provedora de aplicações "acreditar de boa-fé que o acesso, o uso, a preservação ou a divulgação das informações forem razoavelmente necessários para detectar, prevenir ou, de outra forma, resolver fraudes, problemas técnicos ou de segurança, bem como para proteger-se contra danos aos direitos, à propriedade ou à segurança da Adobe, de seus usuários ou do público, conforme exigido ou permitido por lei".

[547] MICROSOFT. Política de Privacidade da Microsoft. Disponível em: <https://privacy.microsoft.com/pt-br/privacystatement>. Acesso em: 11 abr. 2021.

e a apresentação de ofertas relevantes" especificamente para o usuário. Ou seja, é feita uma publicidade comportamental de amplo espectro. A empresa disponibiliza um Painel de Privacidade, dentro do qual é viável que o usuário tenha um amplo controle sobre os seus dados pessoas que são objeto do tratamento. Especificamente sobre o pacote Office – do qual o *MS Word* faz parte –, não há nenhuma informação relevante adicional. De modo geral, o que se percebe é que os termos deveriam ser mais específicos, transparentes e explicativos, e não genéricos.

Em relação ao *Polaris Office*[548], o mais relevante em detrimento dos outros termos analisados é o fato de listar quais empresas parceiras recebem o fluxo de dados pessoais: *Google*, *Google AdMob*, *Facebook*, *MoPub*, *IronSource*, *Unity*, *YeahMobi*, *InMobi*, *Adfit*, *Mobon* e *Criteo*. Além disso, também estabelece os direitos básicos do usuário. No restante, são mantidas as boas práticas dos demais aplicativos.

O *WPS Office*[549] informa que "seremos transparentes sobre a coleta e uso de suas informações para que você possa tomar decisões informadas. Você não é obrigado a nos fornecer as informações que solicitamos, mas se você optar por não fazê-lo, em muitos casos, não poderemos fornecer nossos Produtos e Serviços ou responder a quaisquer dúvidas que você possa ter", dentre as quais: (i) baixar, instalar ou usar os serviços; (ii) inscrever-se ou fazer *login* nos serviços; e (iii) impossibilidade de atendimento por eventuais problemas no serviço.

Contudo, não é feita uma relação causal direta entre qual não consentimento implicaria determinada consequência, o que seria mais interessante pelo dever de transparência. Ou seja, de início, trata-se daquele aviso padronizado alinhado à ideia de *níveis* de aplicativo.

Mais à frente, o documento explica "se combinarmos dados não pessoais com suas informações, os dados combinados serão tratados como dados pessoais", o que é particularmente relevante. Ou seja, ao fazer a união entre o mais e o menos protegido, a conclusão acaba sendo pelo mais protegido. Para além da preocupação com a transferência internacional de dados – o que é uma realidade em todos os aplicativos analisados desta categoria –, não há mais comentários adicionais a serem feitos a respeito dessa política.

De modo semelhante à *Microsoft*, a *Google*[550] também apresenta uma política de privacidade genérica para todas as suas ferramentas, apesar de haver uma página específica

[548] POLARIS OFFICE. Privacy & Terms. Disponível em: <https://www.polarisoffice.com/en/privacy>. Acesso em: 11 abr. 2021.
[549] WPS OFFICE. Privacy Policy. Disponível em: <https://wps.com/privacy-policy/?lang=ptbr>. Acesso em: 11 abr. 2021.
[550] GOOGLE. Privacidade & Termos. Disponível em: <https://policies.google.com/privacy>. Acesso em: 11 abr. 2021.

intitulada “Guia de privacidade dos produtos do *Google*”, mas que transpareceu insuficiência de informações.

Ou seja, no que toca ao *Google Docs* e ao *Google Drive*, a primeira informação desalinhada com a lógica da LGPD – mas esperada – é o fato de a *Google* coletar todo “o conteúdo que você cria, de que faz upload ou que recebe de outras pessoas ao usar nossos serviços. Isso inclui e-mails enviados e recebidos, fotos e vídeos salvos, documentos e planilhas criados e comentários feitos em vídeos do *YouTube*”.

Assim como todas as empresas analisadas, a *Google* informa coletar os dados para criar serviços melhores, dentre os quais se incluem os anúncios baseados em *profiling* e *targeting*. A empresa, contudo, informa não exibir anúncios personalizados baseados em categorias sensíveis, como raça, religião, orientação sexual ou saúde. Também avisa não compartilhar informações que identifiquem o usuário pessoalmente para anunciantes, como nome ou e-mail, a menos que ele peça. Isso é particularmente interessante, pois indica o atendimento da opção legislativa pelo *opt-in*.

De mais relevante, a *Google* oferece uma página específica para que o usuário faça um “check-up de privacidade”, gerenciando, analisando e atualizando suas informações, inclusive aquelas utilizadas para fins de publicidade comportamental. Nesse ponto, a empresa também ganha pontos. Outro aspecto positivo é a empresa permitir que o usuário exclua ou exporte uma cópia do conteúdo associado à sua conta *Google*, inclusive para fins de migração para outros serviços.

Outro aspecto interessante da *Google* é a disponibilização de curtos vídeos explicando os aspectos principais da política de privacidade. Embora os vídeos sejam em inglês, têm legenda em português, o que facilmente facilita a adequada compreensão da política de privacidade da empresa. Sustenta que essa prática deveria ser adotada em diversas outras ferramentas – senão em todas –, de modo a dar transparência mais ativa e efetiva aos usuários sobre as balizas de sua privacidade.

O *Dropbox*[551], que também foi recentemente integrado aos produtos da *Google*, não apresenta diferenças muito significativas. Nos termos de privacidade mais antigos, contudo, não havia qualquer informação sobre eventual publicidade comportamental efetuada por terceiros destinatários dos dados compartilhados pelo aplicativo, o que era um ponto positivo. A única publicidade lá comentada dizia respeito àquela do próprio aplicativo, para que o usuário de sua versão gratuita tivesse interesse em progredir à versão *premium*.

[551] DROPBOX. Dropbox Privacy Policy. Disponível em: <https://www.dropbox.com/privacy?mobile=1>. Acesso em: 11 abr. 2021.

O *4Shared*[552], por sua vez, já começa com um ponto positivo: o título do documento denota que os termos de privacidade ali descritos foram especificamente projetados para o aplicativo, ou seja, na linha da necessária diferenciação entre computadores e dispositivos móveis.

Contudo, ao fazer referência à publicidade construída por terceiros, o documento explicita que "o uso de *cookies* e *beacons* pelos nossos parceiros não é coberto pela nossa declaração de privacidade. Nós não temos acesso ou controle sobre esses *cookies*". Ou seja, trata-se da corriqueira tentativa de limitação de responsabilidade dos fornecedores das aplicações pela parcela do serviço prestada por suas parceiras de publicidade, o que é inviável, conforme preceitua o CDC.

Além de parceiros de publicidade diretamente contratados, o *4Shared* informa que também pode divulgar alguns dados pessoais, sob a forma pseudonimizada, com provedores de dados de publicidade segmentados por terceiros para facilitar os serviços de publicidade para seus clientes, como redes de anúncios e outros sites e aplicativos de terceiros.

Nesse ponto, há uma lista de quinze empresas com os dados individualmente recebidos. Nessa linha de raciocínio, o *4Shared* parece prezar pela transparência, ainda mais por disponibilizar a política de privacidade de *Adsquare*[553], que parece ser uma plataforma de gerenciamento de todos os provedores de publicidade segmentados. A análise desses termos específicos foge ao escopo do presente trabalho, mas seria passível de trabalho posterior.

Outro ponto positivo é que o documento ensina, de modo específico, o usuário a bloquear a coleta de dados e o seu uso por empresas terceirizadas. Uma possível evolução desse cenário, que já é razoável, perpassaria, por exemplo, pela disponibilização de *prints* indicativos das telas específicas.

Por sua vez, o *Share It*[554] chama atenção por dois pontos que podem indicar um pretenso *disclaimer* sobre a própria segurança da ferramenta: (i) o aplicativo não se responsabiliza por informações voluntariamente transferidas pelo usuário que tenham sido interceptadas por terceiros, o que só poderia ocorrer se houvesse uma falha na segurança da informação.

---

[552] 4SHARED. 4shared App Privacy Statement. Disponível em: <https://www.4shared.com/privacyForApps.jsp>. Acesso em: 11 abr. 2021.
[553] ADSQUARE. Privacy Policy & Opt-Out. Disponível em: <https://www.adsquare.com/privacy/>. Acesso em: 11 abr. 2021.
[554] SHARE IT. Privacy Policy. Disponível em: <http://cdn.ushareit.com/shareit/w/privacy/pr_en/index.html>. Acesso em: 11 abr. 2021.

E (ii) o aplicativo solicita que o usuário não envie e não divulgue nenhuma informação pessoal confidencial (por exemplo, informações relacionadas a origem racial ou étnica, opiniões políticas, religião ou outras crenças, saúde, orientação sexual, antecedentes criminais ou participação em organizações anteriores, inclusive sócios sindicais) por meio do aplicativo. É claro que, ao enviar esse tipo de informação, o usuário está majorando o risco de ser indevidamente exposto, mas não parece ser o caso de a empresa tentar se isentar totalmente de uma possível falha em seu sistema de segurança.

No que tange ao escopo de informações infantis, também chama atenção o fato de que o *Share It* é o aplicativo que menos tutela o público infantil em termos de idade, limitando-se a dizer que não tem interesse nos dados de menores de 13 anos (ao passo que a maioria das aplicações estabelece o limite etário de 18 anos). Como o aplicativo é oferecido no Brasil, o ideal seria que a tutela mais apertada se desse, ao menos, até os 16 anos, em que o adolescente já é considerado relativamente capaz.

3.3.12 Governamentais

Os aplicativos *FGTS*, *Caixa Trabalhador*, *Caixa Auxílio Emergencial* e *Bolsa Família* estão submetidos à política de privacidade geral da *Caixa*[555]. Nesse ponto, vale a crítica de que, para melhor aderência às normas da LGPD, os termos deveriam ser individualizados para cada *software*, e não gerais para um grupo de aplicações sem tanta similaridade.

De toda forma, a *Caixa* inicia sua política informando que os dados mais sensíveis, em tese, não estão sujeitos a qualquer procedimento automatizado mais elaborado[556]. A *Caixa* informa coletar: (i) informações que o usuário fornece voluntariamente – normalmente associadas ao preenchimento de formulários –; (ii) dados fornecidos de forma automática quando da utilização dos serviços – informações que diz coletar apenas de modo estatístico, sem qualquer individualização indevida; dentre esses dados, chama atenção como o número de telefone do usuário, as informações coletadas por *cookies* e os dados de geolocalização podem ser anonimizados –; e (iii) informações recebidas de terceiros – informações disponibilizadas publicamente na internet em redes sociais ou provenientes de empresas afiliadas e parceiras.

---

[555] BRASIL. Caixa Econômica Federal. Política de Privacidade do site e dos aplicativos da Caixa. Disponível em: <http://www.caixa.gov.br/politica-de-privacidade/Paginas/default.aspx>. Acesso em: 11 abr. 2021.

[556] "As informações fornecidas no Internet Banking e nas áreas do site que possuem *login* e senha, como cartões para não clientes, consulta ao saldo do FGTS, PIS, programas sociais como o Bolsa Família, entre outros, são protegidos pela Constituição e por outras leis. Ou seja: essas informações são sigilosas e nunca serão usadas para os fins descritos neste documento".

Dentre as finalidades do uso dos dados coletados – como esperado –, está o oferecimento de "conteúdo mais assertivo, direcionado e específico". Na sequência, os aplicativos informam utilizar *cookies* e outras tecnologias afins, para recolher informações sobre a atividade do usuário, navegador e dispositivo. Ao dividir os *cookies* em cinco espécies, duas chamam particular atenção: (i) *cookies* de publicidade comportamental, que "permitem o direcionamento de publicidade aos usuários e medem a eficácia de campanhas"; e (ii) *cookies* de terceiros, na medida em que, "em algumas partes da Plataforma, você poderá utilizar os serviços de terceiros, incluindo a possibilidade de compartilhamento de publicações em redes sociais como o *Facebook*, *Twitter* e *Google+*".

Sobre a segunda categoria, a *Caixa* informa não se responsabilizar e controlar os referidos arquivos, encargo transferido ao usuário quando da análise das políticas daquelas empresas. Embora isso possa fazer sentido, entende-se que a *Caixa* deveria ser mais transparente, ao menos indicando onde o usuário pode encontrar as política específicas dessas empresas. Afinal, se o seu serviço se beneficia – ainda que por remuneração indireta – da interação com essas redes, não é tão correto pensar que sua responsabilidade é puramente afastada pelo entendimento de que "é de terceiro".

Na sequência, a política informa que a "*Caixa* não aluga nem vende suas informações pessoais para terceiros. Mas pode compartilhar suas informações não pessoais de acordo com os objetivos" já listados anteriormente. Dentre os destinatários do compartilhamento, as afiliadas da *Caixa* e os prestadores de serviços e parceiros chamam atenção, especialmente porque estes são agências de marketing, publicidade online e empresas de mídia social.

E isso é particularmente relevante porque a própria *Caixa* informa permitir que outras empresas – como a *Google*, com sua ferramenta *Google Analytics* – usem *cookies* e outras tecnologias de rastreamento para fins de posterior oferecimento de publicidade online dirigida e assertiva. E também nada impede que os próprios terceiros usem os dados para a finalidade própria de oferecer serviços direcionados.

Ou seja, o *targeting* é ambivalente. Teoricamente, há um "clique aqui" para que o usuário "opte por não ter suas informações de navegação na web usadas para fins comportamentais e de publicidade" (*opt-out*), mas o link sequer está funcionando e há a mensagem, pouco clara e dissuasiva, de que "isso poderá interferir na sua interação com o nosso site". Mas não se explica, de modo detalhado e transparente, de que forma a interação sofreria essa alegada interferência.

Na sequência, o link da política de privacidade do *Sisu* não direciona a página alguma. O aplicativo, assim, não pôde ser aqui analisado.

No mesmo sentido, o *Meu Imposto* também possui política de privacidade genérica da Receita Federal[557], que se limita a informar que "a utilização de *cookies* é necessária para o processamento de consultas em determinadas bases de dados, evitando a ação de mecanismos de pesquisa automáticos". Não se informa como os *cookies* são efetivamente utilizados e se há alguma possibilidade de não concessão dessa permissão. E tudo isso no particular contexto de a Receita possuir, talvez, os dados mais sensíveis do usuário.

A mesma linha é adotada pelo *e-Título*[558], que, para além do *Meu Imposto*, também informa que "alguns aplicativos da Justiça Eleitoral e o sítio do TSE utilizam dados extraídos do *Google Analytics* apenas para fins estatísticos e aprimoramento da experiência do usuário". A questão do aprimoramento da experiência é obscura e é justamente o ponto mais sensível, na medida em que pode chancelar diversas espécies de tratamentos de dados.

O *Coronavírus-SUS*[559] inicia afirmando que o documento "visa registrar a manifestação livre, informada e inequívoca pela qual o Usuário concorda com o tratamento de seus dados pessoais para finalidade específica", em conformidade com a LGPD. Fala-se que os dados estão "notoriamente sem identificações pessoais", de modo que as informações "não são tratadas como sensíveis para o âmbito da LGPD". Também se declara não haver qualquer compartilhamento de dados e que os dados pessoais anonimizados poderão ser mantidos por período indefinido.

A política de privacidade do aplicativo é enxuta e simples, sendo, em parte, aderente à tutela que se entende como adequada à luz das balizas da LGPD. No entanto, dois pontos chamam a atenção: o tratamento em definitivo dos dados pessoais anonimizados, o que parece violar a legítima expectativa do usuário de ver seus dados eliminados após o atingimento da finalidade pública – dados sobre o coronavírus poderiam ser mantidos mesmo após o término da pandemia, por exemplo, o que não parece adequado às normas.

E o segundo ponto diz respeito à declaração inicial de que o documento é válido para manifestar a vontade livre, informada e inequívoca do usuário de consentir com o tratamento dos seus dados. Tal afirmação não tem, em verdade, qualquer validade jurídica, na

---

[557] BRASIL. Receita Federal do Brasil. Política de Privacidade. Disponível em: <http://receita.economia.gov.br/sobre/politica-de-privacidade>. Acesso em: 11 abr. 2021.

[558] BRASIL. Tribunal Superior Eleitoral. Política de privacidade e termos de privacidade. Disponível em: <http://www.tse.jus.br/transparencia/politica-de-privacidade-e-termos-de-uso>. Acesso em: 11 abr. 2021.

[559] BRASIL. Ministério da Saúde. Políticas de Privacidade. Disponível em: <https://validacovid.saude.gov.br/politica-privacidade>. Acesso em: 13 abr. 2021.

medida em que a qualificação do consentimento deve ser obtida a partir da análise do caso concreto: notadamente, da qualidade, à luz da égide da transparência, dos termos de privacidade. Não havendo a devida transparência, não há que se falar em consentimento informado. E não é uma afirmação inicial, com pretensões de ser peremptória, que poderá mudar isso.

De diferente, o *CNH Digital*[560] adverte que as informações coletadas – dentre as quais, além dos dados pessoais necessários ao funcionamento do sistema, estão "quais páginas foram utilizadas", "quando foram acessadas" e "qual o tempo de permanência nelas" – podem ser "usadas para outros objetivos da Administração Pública: auditorias, análises estatísticas, ciência de dados e estudos para lançamento de novos serviços públicos ou para a melhoria dos já existentes, bem como de processos e comunicações".

É justamente esse tipo de repasse para objetivos da Administração que acende o alerta da possível vigilância estatal. Ao revés, a política de privacidade informa não repassar a terceiros "informação de nível individual que por você seja cedida com este aplicativo. Toda e qualquer informação individual a seu respeito só poderá ser repassada mediante sua aprovação expressa ou, ainda, por outros meios, se permitido em lei". *A priori*, o usuário parece estar assegurado do *targeting*.

O *Sine*[561], ao esclarecer as hipóteses de compartilhamento de dados com terceiros, estabelece duas circunstância que parecem particularmente relevantes: (i) compartilhamento de dados na Administração Pública, na forma do Decreto nº 8.789/2016 – que já foi, inclusive, revogado pelo Decreto nº 10.046/2019 –; e (ii) "compartilhamento de informações com empresas que utilizam cookies, web beacons e tecnologias de rastreamento para que nos forneçam informações analisadas sobre como o usuário utiliza nossos serviços", cujos principais objetivos são "oferecer publicidade online dirigida e assertiva, analisar e controlar dados, determinar a popularidade de determinados conteúdos e entender melhor o comportamento do usuário na rede". Chama atenção o fato de haver publicidade comportamental em um aplicativo do governo.

Outro ponto relevante é a fluidez dos conceitos estabelecidos no referido Decreto. As finalidades para o compartilhamento de dados (art. 1º) são genéricas e aptas a justificar qualquer pretensão: (i) a simplificação da oferta de serviços públicos; (ii) a formulação, a

---

[560] BRASIL. Departamento Nacional de Trânsito. Política de Privacidade Carteira Digital de Trânsito. Disponível em: <https://portalservicos.denatran.serpro.gov.br/#/carteiradigital/politicaprivacidade>. Acesso em: 11 abr. 2021.

[561] BRASIL. Ministério do Trabalho. Política de Privacidade. Disponível em: <https://empregabrasil.mte.gov.br/termos-e-privacidade/>. Acesso em: 11 abr. 2021.

implementação, a avaliação e o monitoramento de políticas públicas; (iii) a análise das condições de acesso e manutenção de benefícios sociais e fiscais; (iv) a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e (v) o aumento da qualidade e da eficiência das operações internas da administração.

É claro que os três primeiros pontos parecem relevantes – embora seja questionável a situação de, por exemplo, um beneficiário do Bolsa Família perder o seu benefício porque, quando do compartilhamento de informações pessoais acessadas pelos *smartphones* nos aplicativos públicos, se percebeu que ele não teria o direito; é quase uma prova produzida contra si mesmo de modo coativo –, mas o quarto aspecto é extremamente abrangente e, por isso, desalinhado com a lógica da LGPD.

No que tange às hipóteses de revogação do consentimento, a política de privacidade estabelece que alguns pedidos podem ser negados em razão do interesse da Administração Pública, cláusula abrangente, que poderia chancelar, por exemplo, o mero interesse da Administração de simplesmente manter dados organizados sobre todos os cidadãos, sem maiores justificativas compatíveis com as diretrizes da razoabilidade e da minoração do acesso aos dados pessoais.

O aplicativo *Caesb* não contém uma política de privacidade[562]. Limita-se a informar que "faremos os melhores esforços para proteger a segurança dos dados dos usuários dos nossos aplicativos. A *Caesb* poderá fornecer os dados coletados para cumprimento de solicitações de Autoridades Policiais, do Poder Judiciário e de determinações de qualquer ente da Administração Pública, Direta e Indireta".

Por sua vez, as aplicações *CEB*, *DigiSUS*, *Denatran*, *Meu INSS* e *Novacap* sequer possuem política de privacidade (tradicional mensagem "página não encontrada!"), o que desalinhado com a LGPD e com a dinâmica adequada de proteção da privacidade e dos dados pessoais.

É de se ver, assim, que os aplicativos governamentais, mesmo com aparente preocupação da Administração Pública federal de bem regulamentar a matéria para fins de proteção dos direitos basilares de seus cidadãos, ainda engatinham na proteção concreta aos dados pessoais.

---

[562] BRASIL. Distrito Federal. Companhia de Saneamento Ambiental do Distrito Federal. Política de privacidade de aplicativo mobile. Disponível em: <https://www.caesb.df.gov.br/594>. Acesso em: 11 abr. 2021.

4 A PROPOSTA: *NÍVEIS DE APLICATIVO*

Feita toda essa longa análise crítica dos dados encontrados, passa-se à breve explicação de uma proposta possível para o equacionamento dos interesses em jogo: de um lado, liberdade econômica e sobrevivência da atividade empresarial; de outro, máxima tutela possível da privacidade e dos dados pessoais dos usuários. Como se viu, os aplicativos normalmente transpassam essa ponderação por meio da obtenção do consentimento do usuário ou da aposta no legítimo interesse, que nem sempre é tão legítimo e transparente assim.

Ou seja, partem do pressuposto de que o clique em "download", "concordo", "instalar" e afins é suficiente para fazer prevalecer, no caso concreto, o interesse empresarial de proceder ao tratamento dos dados pessoais, que, como visto, são verdadeiras commodities no mundo moderno.

Contudo, não se pode olvidar que os termos de privacidade são verdadeiros contratos de adesão, o que justificaria eventual provimento judicial para afastar cláusulas verdadeiramente abusivas – e elas são muitas, como se viu na seção anterior. É nesse contexto que se insere a ideia de *nível de aplicativo*, com a qual se busca dar maior negociabilidade às cláusulas dos termos de privacidade e das políticas de privacidade, no sentido de se tentar conceber um consentimento realmente livre e informado, ou um interesse realmente legítimo e transparente.

Isso teria o condão de afastá-los, ainda que ligeiramente, da posição *standard* de meros contratos de adesão, caminhando rumo à maior *paridade de armas*. Para o brevíssimo desenvolvimento da ideia, parte-se do pressuposto de que os aplicativos apenas utilizam os dados pessoais para fins de publicidade comportamental via *targeting* e *profiling*, ou seja, serão esquecidos quaisquer usos diversos.

Pois bem. A ideia de *nível* pode ser encarada de duas formas. A primeira delas é a evolução de uma prática de alguns aplicativos analisados, principalmente os jogos. Com efeito, alguns aplicativos oferecem ao usuário a seguinte opção aproximada: "você pode continuar no jogo sem a exibição de anúncios, desde que faça o *upgrade* para a versão paga, que custa R$ 20,00".

Com isso, a desenvolvedora do *software* está transparecendo que aquele valor cobrado é o resultado do equacionamento entre o custo para disponibilizar o seu produto, até então gratuito, e o lucro almejado para haver interesse empresarial em investir no desenvolvimento da aplicação.

Ou seja, R$ 20,00 seriam o valor aproximado que aquela empresa estaria ganhando dos anunciantes em sua plataforma para cada usuário singular. Contudo, os termos de privacidade dos aplicativos que utilizam essa forma de equacionamento nada informam sobre fazerem cessar a coleta e o tratamento dos dados pessoais quando da ascensão à versão paga da aplicação. Ou seja, parece que os dados pessoais continuam sendo coletados e processados – sendo, inclusive, transmitidos a terceiros, que poderão utilizá-los para anúncios patrocinados, mas em outras plataformas. É o que se convencionou chamar de metodologia *freemium*, em que não há verdadeira diferenciação no funcionamento do aplicativo em suas versões gratuita ou paga.

A ideia seria, então, levar essa política mais à frente, garantindo que o dado do usuário sequer seja processado – e, se possível para o correto funcionamento da aplicação, sequer seja coletado. O ponto pensado é que, em cada cláusula de permissão concedida ou que implicasse individualmente avanço sobre a privacidade do usuário houvesse uma opção da seguinte forma: "Nós coletamos e processamos os seus dados de localização; e, se você permitir nosso acesso ao GPS, coletamos inclusive a sua localização precisa, com vistas a oferecer conteúdo mais relevante ao seu uso. Contudo, se você quiser que não coletemos e processemos esses dados, basta você dar um *check* nessa caixa e pagar a quantia de R$ 5,00; se você permitir nossa coleta, mas quiser evitar o nosso compartilhamento com terceiros, basta pagar a quantia de R$ 3,00".

É claro que essa opção também poderia existir depois que o usuário já começou a usar o aplicativo em sua versão gratuita: ou seja, seria possível ascender para uma versão paga e menos restritiva de sua privacidade, inclusive com garantia de exclusão de todos os dados pessoais anteriormente armazenados e transmitidos a terceiros, desde que viável tecnicamente.

Ou seja, o ponto é fazer o contrato de uso e a política de privacidade dos aplicativos funcionarem de modo mais paritário e discutido, colocando o consentimento ou o legítimo interesse – justamente o que serve legalmente para justificar o cenário que se vive hoje – realmente como a pedra de toque do ordenamento jurídico do mundo digital. Se isso fosse concretamente levado a efeito, o usuário não poderia arguir que não teve a opção de facilmente entender os termos de privacidade daquele aplicativo, o que daria maior resguardo à atividade empresarial sob a ótica de não interferência na produção econômica da empresa.

E, no mesmo sentido, os interesses econômicos da empresa também estariam, em tese, integralmente resguardados, na medida em que aferiria os seus almejados lucros (i) ou com o tratamento dos dados efetivamente consentido pelo usuário, (ii) ou com o seu pagamento

direto para o uso do aplicativo *cru*, sem qualquer pretensão de processamento de dados pessoais de modo que avilte mais a tutela dos dados dos usuários.

De outro lado, os interesses dos usuários também estariam completamente resguardados, na medida em que teriam a opção de (i) ver publicidade comportamental construída a partir de suas preferências pessoais – o que é extremamente legítimo; afinal, como dito na política de privacidade de um dos aplicativos analisados, seria muito chato ver propaganda de hotéis em Paris com uma viagem marcada para Roma –, ou (ii) de retirar o seu consentimento para qualquer tratamento de seus dados pessoais, desde que com o pagamento de uma quantia simbólica e apta a viabilizar o interesse empresarial em ser provedor de aplicações.

E este parece ser justamente o único requisito para que essas cláusulas negocialmente pensadas não sejam abusivas: o valor cobrado deve ser efetivamente simbólico. Não seria razoável que um aplicativo cobrasse de seu usuário R$ 200,00 para não coletar e tratar os dados de localização geográfica, na medida em que dificilmente teria esse retorno com a publicidade via *profiling*. E também não se cogita aqui de um valor único, já que cada categoria de aplicativo tem, naturalmente, acessos muito diferentes à aos dados de seu usuário normal.

Bioni pontua que, dentro do exemplo da aquisição do *WhatsApp* pelo *Facebook*, em que foi modificada a política de privacidade do primeiro para permitir o compartilhamento de dados com o grupo econômico do segundo para o aprimoramento de experiências, a rentabilização média dos dados do usuário custariam cerca de US$ 12.00 ao ano, pouco mais de R$ 60,00. E isso porque, quando do início do aplicativo de mensageria privada, cogitou-se cobrar um valor de US$ 1,00 ao ano de cada usuário, justamente para dar impulsão à lógica da empresa de resguardar a privacidade dos seus usuários[563].

Dentre os aplicativos aqui analisados, por exemplo, pareceu muito claro que o *Pinterest* deve lucrar com o processamento de dados de seus usuários, justamente porque, por pressuposto de utilização da ferramenta, o próprio usuário deve informar seus interesses. Nesse caso, por exemplo, seria mais factível um valor proporcionalmente maior.

Essa proporcionalidade deveria ser aferida por meio da transparência: as empresas poderiam disponibilizar dados gerais, que não comprometessem segredos ou competitividade empresariais, de quanto efetivamente lucram com a publicidade comportamental e, a partir

[563] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

disso, poder-se-ia pensar em faixas de valores, a serem controlados por algum órgão regulador estatal – à semelhança da autoridade nacional de proteção de dados, da LGPD.

Pensa-se que isso poderia equacionar perfeitamente os interesses empresariais e a privacidade do usuário. E aqui não se cogita de que cláusulas dessa forma pudessem significar algo como alienabilidade de direitos fundamentais ou de direitos da personalidade (privacidade, proteção de dados, vida privada), na medida em que se trata de uma opção expressa do usuário.

Trata-se de uma tentativa de elevar o patamar de discussão sobre a disponibilidade relativa dos direitos de personalidade: afinal, se o usuário pode escolher dispor de parte de seus dados pessoais para utilizar o aplicativo – sabendo que está *pagando* o uso do aplicativo com o fornecimento de seus dados –, deve também ser capaz de não concordar com o processamento de dados como forma de contraprestação pelo produto a ele disponibilizado, mesmo que seja com a contraprestação pecuniária direta. A ideia aqui posta simplesmente transforma a contraprestação pecuniária indireta – dados pessoais – em direta – valor financeiro correspondente e razoável.

E se deve partir do mundo concreto para a análise propositiva: as empresas coletam, processam e comercializam os dados de seus usuários; afinal, precisam sobreviver. Esse é o mundo e não há nada que se possa fazer, ou regredir-se-á à época em que sequer existia computador, fazendo várias empresas de tecnologia entrarem em falência e acabando com milhões de empregos legítimos.

Ou seja, o intercâmbio dos dados já está presente, mas só os seus titulares – usuários – não sabem disso com a necessária transparência. Com a inserção dessas cláusulas mais explícitas, o dever de transparência estará cumprido, em estrito atendimento à máxima da boa-fé objetiva, o que permite ao usuário exercer o seu livre convencimento de forma realmente esclarecida.

Leonardo Bessa, aliás, muito antes de a discussão sobre proteção de dados ganhar notória relevância no Brasil, já afirmava que o principal é manter a essência de confiança e proteção mútua, normalmente com caráter preventivo, dada a "criação de deveres jurídicos que objetivam principalmente evitar lesão a valores (a honra, a privacidade, a boa-fé, transparência) que não possuem uma equivalência pecuniária direta". Assim, "o caráter extrapatrimonial do direito à vida privada, além de significar que ele não possui valor pecuniário - não integrando, portanto, o patrimônio material do titular - evidencia que as tentativas jurídicas de protegê-lo devem conferir especial ênfase a prevenção" [564].

[564] BESSA, Leonardo Roscoe. O consumidor e os limites dos bancos de dados de proteção ao crédito. São Paulo: Revista dos Tribunais: 2003, p. 170.

A mesma necessidade de proteção preventiva dos direitos foi ressaltada pela Ministra Rosa Weber quando do julgamento da ADI-MC 6.387/DF, para a qual "a adequada tutela do direito à intimidade, privacidade e proteção de dados pessoais é estruturada pela característica da inviolabilidade. Vale dizer, uma vez afrontada a norma de proteção de tais direitos, o ressarcimento se apresenta como tutela insuficiente aos deveres de proteção"[565].

E é exatamente disso que se cuida: sendo praticamente inviável a tutela *a posteriori* de eventuais lesões ao direito à proteção dos dados pessoais – à exceção da tutela reparatória, que dificilmente repara a real monta do dano –, o foco é investir na atuação protetiva e preventiva, justamente para que eventuais danos não ocorram. O Ministro Luiz Fux, no bojo do mesmo julgamento, assentou sua especial preocupação com o que chamou de ilícito de perigo, que clamaria por uma necessária tutela preventiva, apta a impedir a concretização do risco iminente.

Em tese, os dados pessoais efetivamente não têm uma contraprestação pecuniária direta, na medida em que se trata de direitos cuja proteção se reveste de caráter extrapatrimonial. E essa percepção parece, ainda hoje, insuperável. Contudo, o que se propõe aqui não é sequer uma equivalência pecuniária direta, mas uma espécie de contraprestação por amostragem. Isso é, não será cobrado do usuário X a exata potencialidade patrimonial de seus dados[566], mas um valor médio, calculado de modo minimamente transparente (a partir dos lucros líquidos das provedoras de aplicação, por exemplo), para todos os usuários. E isso, como colocado por Leonardo Bessa, com boa-fé e transparência.

Bruno Miragem lembra, por outro lado, que "há situações em que o fornecedor, para determinar as condições de uma determinada contratação necessita de dados do consumidor, seja para delimitar a prestação ou para formação do preço". É o caso dos preços e fretes, fornecimento de serviços bancários, prestação de securitização, dentre outras[567]. Ou seja, em muitos casos, os dados do consumidor já se revestem de um caráter patrimonial direto – na medida em que influenciam no preço cobrado por determinado serviço.

Bruno Bioni reconhece que o pagamento de muitos serviços e produtos é realizado com os dados pessoais do consumidor, o que é preocupante, na medida em que o titular dos dados não sabe exatamente o *custo efetivo* da transação, sobretudo em um contexto de *big data*.

---

[565] BRASIL. Supremo Tribunal Federal. ADI-MC nº 6.387/DF, Rel. Min. Rosa Weber, julgamento em 7/5/2020.
[566] Imagine-se o caso de um usuário que sabidamente clica em todos os anúncios patrocinados a ele exibidos e efetivamente fecha as aquisições ali dispostas. Certamente os dados desse usuário, para o fazimento da publicidade direcionada, valem muito mais do que os de um usuário que nunca clica em anúncios exibidos.
[567] MIRAGEM, Bruno. A lei geral de proteção de dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais, vol. 1009/2019, nov/2019.

"Os dados pessoais, que são o *trade-off* desses novos modelos de negócios; ao contrário das relações off-line, em que a contrapartida de um bem de consumo é fixada, individual e pecuniariamente, para cada relação de consumo"[568].

Há, assim uma lógica traiçoeira nessa troca: ganha-se um benefício imediato, mas os prejuízos são mediatos e distantes. Dada a racionalidade limitada humana[569], é provável que se decida pela utilidade subjetiva, ou seja, com propensões aos benefícios imediatos[570]. Sendo o aplicativo *gratuito*, é pouco provável que qualquer usuário efetivamente meça as consequências do eventual mau tratamento dos dados pessoais.

Essa racionalidade limitada foi demonstrada empiricamente no contexto da proteção de dados pessoais em aplicativos em magistral artigo de pesquisadoras de Stanford e Carnegie Mellon[571]. Em tal artigo, as autoras demonstraram que poucos usuários (11%) concordavam em pagar a quantia simbólica de 1 dólar para evitar que os provedores de aplicação coletassem suas informações pessoais, ao passo que a maioria (69%) concordava em ganhar 1 dólar para permitir a coleta.

O argumento para a baixa adesão ao pagamento é de que quase todos encaravam a proteção de seus dados como um direito, sendo desnecessário pagar para que as empresas não violassem – 61% chamaram isso de extorsão. Em tese, tal resultado demonstraria a falta de apelo econômico que as pessoas ainda têm em relação aos seus dados pessoais, o que pode ser uma limitação à solução aqui proposta. É verdade que transparência e informação podem ajudar os usuários a mudarem essa percepção, mas não é uma garantia.

De toda forma, "traçando um paralelo com outras operações econômicas, cuja contraprestação pelo bem de consumo é fixada pecuniariamente, sabe-se exatamente o custo da transação caracterizado por um deslocamento patrimonial, enquanto na lógica da economia informacional, é incerto como a disponibilização de uma informação pessoal poderá afetar o seu titular e, por conseguinte, o 'preço' a ser pago pelo bem de consumo"[572].

---

[568] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[569] JOLLS, Christine; SUNSTEIN, Cass R.; THALER, Richard. A behavioral approach to law and economics. Stanford Law Review, v. 50, p. 1.477, 2004.

[570] KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie. Soft surveillance, hard consent. In: KERR, Ian (Ed.). Lessons from the identity trail: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009. p. 17: "It is well known in decision theory that subjective utility – that is, the personal value of an outcome – changes depending on when the outcome will be experienced. In particular, the subjective value of a benefit or loss that will be experienced today is greater than the subjective value of that same benefit or loss if we know that it will be experienced some time in the future".

[571] CRANOR, Lorrie Faith; MCDONALD, Aleecia M. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, p. 1. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>. Acesso em: 3 jun. 2021.

[572] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de

Com efeito, parece que a solução aqui proposta de níveis de aplicativo, sobretudo à luz da lógica de consentimento granular, é compatível com a pretensão de fixações pecuniárias diretas e mais transparentes, desde que, é claro, consiga se garantir que efetivamente não se procederá ao tratamento daqueles dados *negados* dentro da granularidade.

Defende-se que, numa perspectiva de autodeterminação informacional, seria muito mais interessante que o titular dos dados soubesse como os dados são utilizados, inclusive com eventuais cruzamentos com outros dados. Tal transparência mais direta viabilizaria o conhecimento dos custos efetivos da operação econômica de *baixar* e utilizar o aplicativo.

Exatamente nessa linha, parte da doutrina advoga que se reconheça o dado pessoal quase como um direito de propriedade, o que perpassaria pela assunção de que os mercados de dados existem e tentaria resolver os problemas daí decorrentes por meio de mecanismos da teoria econômica para otimização de custos e benefícios[573].

Danilo Doneda defende que "considerar a informação como um bem jurídico e estender a tutela de caráter patrimonial para os dados pessoais, no entanto, não parece uma solução adequada, em vista da multiplicidade de situações e interesses presentes em torno dos dados pessoais, que não se limitam a vetores patrimoniais e que seriam irremediavelmente prejudicados se considerados apenas – ou majoritariamente – a partir de seu valor econômico"[574].

Laura Schertel também advoga contra a concepção de propriedade dos dados pessoais, na medida em que isso comprometeria a igualdade – já que, potencialmente, apenas a parte mais rica da sociedade conseguiria preservá-los adequadamente –, a individualidade – já que os dados a serem produzidos começariam a orientar a própria personalidade, e não o contrário – e a democracia[575].

A mesma posição de que as soluções de mercado são insuficientes para a adequada disposição dos dados pessoais – diante da "multiplicidade de situações e interesses a eles relacionadas, que não se limitam a vetores patrimoniais" – é adotada por Ana Frazão, para quem a disciplina do consentimento "não deve ser tratada sob o viés negocial, mas sim a partir do poder de autodeterminação" e dos direitos fundamentais[576].

Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[573] RULE, James; HUNTER, Lawrence. Towards a property right in personal data. In: Visions of privacy: Policy choices for the digital age. Colin Bennett. Toronto: University of Toronto Press, 1999, pp. 165-181. L

[574] DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

[575] MENDES, Laura Schertel. Privacidade, Proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 122-123.

[576] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito

Assim, para a autora, "renúncias e transações sobre os dados, ainda mais quando realizadas sem as informações necessárias e sem contrapartida minimamente razoável, não são válidas não apenas em razão das disposições específicas da LGPD, mas, também, à luz das disposições de outros diplomas legislativos, tais como o art. 11 do Código Civil". Isso porque "o eixo valorativo da LGPD é a proteção da pessoa humana e de suas situações existenciais relevantes, o que deve ser levado em consideração para a interpretação de todas as suas demais disposições"[577].

A ideia aqui proposta, em verdade, não tem o condão de reduzir os dados pessoais ao aspecto meramente patrimonial. Pelo contrário, tenta permitir que a pessoa, no auge de sua liberdade informada, consiga efetivamente manifestar sua autodeterminação informativa, escolhendo como quer que o aplicativo em questão funcione. Para isso, é básico que haja transparência por parte da plataforma.

Gustavo Tepedino e Chiara Teffé, a seu turno, entendem como "inadequada a caracterização de natureza negocial para o consentimento, visto que tal entendimento reforçaria o sinalagma entre o consentimento para o tratamento dos dados pessoais e determinada vantagem econômica obtida por aquele que consente – a reforçar indesejada índole contratual e de fomento à utilização de esquemas proprietários para o trato dos dados pessoais"[578].

Os autores, contudo, manifestam-se favoravelmente à ideia balizada no art. 18 da LGPD de afastar o consentimento implícito na lógica binária de funcionamento, incentivando "configurações de privacidade personalizáveis e a possibilidade da manifestação do consentimento de forma granular, podendo o cidadão emitir autorizações fragmentadas no tocante ao fluxo de seus dados". Ou seja, de um lado, apesar de a proposta aqui ventilada se basear na contraprestação pecuniária direta, é fato que tenta levar o consentimento granular a outro nível de debate.

Ao revés, Márcio Cots e Ricardo Oliveira entendem que "o consentimento é uma base legal para tratamento de dados pessoais que possui nítida natureza contratual, pois, de um lado, há a manifestação da vontade de uma parte em tratar os dados pessoais para determinada finalidade e, de outro lado, há alguém que anui com tal tratamento". Salientam, contudo, que "o tratamento de dados pessoais em si pode não ser a causa principal da relação jurídica entre

brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[577] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[578] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

as partes, mas o consentimento está longe de ser um contrato acessório, pois não é dependente de nenhum outro ajuste, mantendo-se vigente e eficaz por si mesmo"[579].

Roberta Mauro aponta que "dois fatores principais têm contribuído para a defesa, em sede doutrinária, de que dados pessoais seriam objeto de propriedade: a insuficiência da responsabilidade civil para apresentar soluções a problemas modernos como a prática de *profiling*, sem consentimento do titular dos dados, e a necessidade de recorrer ao direito de sequela, atributo do direito de propriedade e dos direitos reais, na intenção de reaver dados indevidamente transmitidos a terceiros" [580].

A ideia de recorrer aos direitos de propriedade remonta, na verdade, ao trabalho seminal de Warren e Brandeis[581]. Paul Schwartz, a seu turno, identificou a comodificação dos dados pessoais – pacote de informações que poderia ser trocado por outro bem. Descreveu a existência de quatro condições existentes no mundo atual para que isso seja possível: pessoas dispostas a mercantilizar os dados pessoais, empresas de publicidade dirigida, empresas transnacionais de identificação de hábitos de consumo e preferências individuais de cada pessoa[582].

Daniel Solove, a seu turno, considera insuficiente a tentativa de reduzir a privacidade ou a proteção dos dados pessoais apenas a aspectos proprietários, na medida em que não se cuida apenas de uma regulação individual, mas social da informação como bem jurídico relevante, inclusive com valor patrimonial elevado[583]. Assim, parece correta a posição do legislador brasileiro, apontada por Roberta Mauro, de que o art. 17 da LGPD persegue tutela que abranja aspectos patrimoniais e extrapatrimoniais ligados aos dados pessoais[584].

Concorda-se, dessa forma, com a abordagem de que tentar reduzir as informações ou dados pessoais – que compõem a personalidade da pessoa – a valores unicamente patrimoniais não é a melhor abordagem. Afinal, como pontuado por Doneda, há complexidades de toda ordem, inerentes ao próprio desenvolvimento da personalidade enquanto vetor da dignidade humana, que extrapolam a aferição meramente patrimonial do conteúdo do direito.

---

[579] COTS, Márcio, e OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 2ª ed. Rev. Atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019. Pág 86.
[580] MAURO, Roberta. A titularidade de dados pessoais prevista no art. 17 da LGPD: direito real ou pessoal? In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].
[581] WARREN, Samuel D. e BRANDEIS, Louis D. The right to privacy. Harvard Law Review, v. 4, n. 5, p.194.
[582] SCHWARTZ, Paul. Property, Privacy and Personal Data. Harvard Law Review, v. 117, n. 7, 2004, p. 2056.
[583] SOLOVE, Daniel. Understanding privacy. Cambridge: Harvard University Press, 2008. E-book, pos. 327/3424.
[584] MAURO, Roberta. A titularidade de dados pessoais prevista no art. 17 da LGPD: direito real ou pessoal? In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

Contudo, o que se está a propor aqui não é a mera retomada patrimonial dos dados pessoais, mas uma conjugação dessa possibilidade com a obediência a todas as balizas da LGPD e do ordenamento constitucional. Isso é, não basta que apenas se cobre um valor em troca do não processamento dos dados, sendo necessário dar transparência ao usuário para que ele possa optar por uma ou outra possibilidade consentindo de modo informado.

É preciso dar transparência que nada será efetivamente processado. Com essa dicotomia entre as opções de funcionamento, o usuário terá, ao revés da mera patrimonialização de sua personalidade, um ganho informacional, pois tenderá a saber com muito mais precisão do que hoje qual é a cadeia de comunicação dos seus dados pessoais coletados em determinada aplicação.

Claro é que "o consentimento do titular dos dados pessoais não deve ser um recurso para legitimar os mais abusivos e invasivos tipos de tratamentos de dados pessoais, coisificando-o"[585], à luz da própria matriz normativa do Código Civil, que impõe naturais limites à autonomia privada, especialmente quanto aos direitos de personalidade[586]. Mas, à exceção dessas situações extremas e de outros casos com vedação normativa setorial[587], Bioni parece aceitar a ideia de disponibilidade relativa dos dados pessoais por seu titular, inclusive com o ajuste de parâmetros monetários para a troca.

Leonardo Bessa também ressalta o papel central do consentimento do titular dos dados como base legitimadora para o tratamento dos dados, "perspectiva que ressalta a liberdade e autonomia do indivíduo". Para o autor, a proteção de dados é um direito, e não um dever, de modo que deve servir, antes de tudo, "para promover a personalidade humana, privilegiando-se escolhas e decisões individuais, sob pena de tornar-se em verdadeiro e indesejado dever de privacidade"[588].

Afinal, como pontua o autor, a liberdade é um dos aspectos mais relevantes da autodeterminação informativa e da própria dignidade humana[589]. Ou seja, não se pode impor, a

---

[585] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[586] GAMA, Guilherme Calmon Nogueira da; PEREIRA, Daniel Queiroz. Direitos da personalidade e Código Civil de 2002. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org.). Doutrinas essenciais: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 321.

[587] Sigilo e inviolabilidade das comunicações privadas na Internet, a proibição da guarda combinada de logs de acesso e de aplicação pelos provedores de conexão, a limitação do uso de dados pessoais para fins de avaliação de crédito, dentre outros.

[588] BESSA, Leonardo Roscoe. LGPD: direito ou dever de privacidade? Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2021-fev-08/leonardo-bessa-lgpd-direito-ou-dever-privacidade>. Acesso em: 4 jun. 2021.

[589] BESSA, Leonardo Roscoe. A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa>. Acesso em: 4 jun. 2021.

uma sociedade complexa e multidimensional, um dever de privacidade naturalmente unidimensional, mas, sim, devem-se oferecer instrumentos para permitir escolhas individuais conscientes, informadas e dentro do maior poder possível de barganha para o titular dos dados[590].

Isso porque, como aponta Jorge Reis Novais, "a titularidade de uma qualquer posição de direito fundamental envolve, em princípio, o poder de disposição sobre todas as possibilidades de ação que dela decorrem, momento o poder de disposição acerca do 'se', do 'quando' e do 'como' do seu exercício (ou não exercício) fático"[591]. À luz disso, parece ainda mais justificável a pretensão de tornar possível a contraprestação pecuniária direta pelos dados.

Lawrence Lessig[592] defendia, partindo da premissa de real transparência e possibilidade de discriminação de portais por níveis de privacidade, afirmava que a solução de mercado baseada na negociação de dados protegeria melhor o usuário do que a tutela de responsabilidade. Defende-se, aqui, que não há competição, mas coexistência: tutelas *ex ante* e *ex post*, além do funcionamento negocial por níveis.

Frank Pasquale classificava como ficção imaginar que os consumidores poderiam barganhar por privacidade, a ponto de optarem por não utilizar um aplicativo quando pensassem que não estariam devidamente assegurados[593]. Como pontuado por Ana Frazão, "em contextos de ausência de rivalidade e em que a aceitação da política de privacidade é condição *sine qua non* para o acesso ao serviço (as chamadas cláusulas *take it or leave it*), a legitimidade do consentimento sempre será discutível, mesmo que ele tenha sido informado"[594].

É justamente à luz do consentimento granular e da redução da assimetria informacional a partir da necessária transparência ativa por parte dos provedores de aplicação que se defende que a presente solução tem o condão de melhorar o nível de tutela dos dados pessoais no Brasil, nem que seja dando maior engajamento ao tema por parte da população.

A segunda forma de entendimento da ideia de nível de aplicativo é mais básica e merece menos comentários, na medida em que também é uma prática existente em alguns poucos aplicativos. O ponto tangencia o grau de funcionamento da aplicação e, principalmente,

---

590 CANOTILHO, J. J. Gomes; MACHADO, Jónatas E. M. Reality shows e liberdade de programação. Coimbra: Coimbra, 2003. p. 57.

591 NOVAIS, Jorge Reis. Renúncia a direitos fundamentais. In: Miranda, Jorge (Org.). Perspectivas constitucionais: nos 20 anos da Constituição de 1976. Coimbra: Coimbra, 2006, p. 286.

592 LESSIG, Lawrence. Code and other laws of cyberspace. New York: Basic Books, 1999, p. 160.

593 PASQUALE, Frank. The black box society. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 143.

594 FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

as permissões concedidas pelo usuário. Isso significa dizer que, quando o usuário vai utilizar o *software*, deve ter a livre opção de manifestar sua vontade de não fornecer algumas das permissões solicitadas pela ferramenta, sem que isso implique o seu integral não funcionamento.

Pegando um exemplo simples: se o usuário não fornecer permissão para que o *Instagram* tenha acesso à sua localização precisa, deve se conformar com o não funcionamento da possibilidade de marcação específica do local em que aquela determinada foto foi tirada. Essa ideia basilar poderia ser colocada em escala, gerando efetivos níveis de funcionamento da aplicação: do mais completo, desde que o usuário fornecesse todas as permissões solicitadas, ao mais simples, no qual o usuário não concordaria com várias das solicitações.

Do ponto de vista da tecnologia da informação, o desenvolvimento desses níveis de funcionamento parece ser viável. Do ponto de vista econômico, talvez seja necessário equacionar essa segunda proposta com a primeira. Do ponto de vista jurídico, essa acepção do termo parece aderente ao que se concebe como consentimento granular ou fracionário, em que o usuário realmente tem potencialidade de manifestar aquilo com o que concorda ou não no âmbito do tratamento de seus dados pessoais.

Ademais, à luz da necessidade de limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (princípio da necessidade), parece que uma das duas soluções aqui apontadas é o ideal para o funcionamento das ferramentas de modo adequado à LGPD.

Isso porque, partindo do pressuposto de que hoje já uma coleta exorbitante de dados pessoais – como se viu na análise empírica –, na medida em que muitos dados tratados não guardam real pertinência com o produto oferecido no software, de duas uma: ou bem se aceita cobrar pelos produtos para que eles não façam tratamento ilegais dos dados pessoais, ou bem se aceita o funcionamento granular e parcial das plataformas. A terceira solução parece ser a pior: a interrupção do funcionamento das plataformas, que, via de regra, não respeitam as balizas legais e optam por uma monetização incompreensível dos dados pessoais tratados.

Aliás, o princípio da necessidade para justificar o tratamento de dados foi afirmado pelo STJ mesmo antes da edição da LGPD. Com efeito, em 2017, o Tribunal entendeu como abusiva a cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento. Isso por deixar

de atender a dois princípios importantes da relação de consumo – transparência e confiança – e também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão.

O Tribunal ainda afirmou que "a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição"[595].

Daniel Solove, nesse sentido, informa que "sacrifícios a direitos e liberdades civis somente podem ser feitos quando o governo justifica adequadamente por que esses sacrifícios são necessários. É preciso submeter tais restrições a direitos a um escrutínio meticuloso, especialmente porque, em tempos de crise, o medo distorce nosso julgamento. (...) devemos ser extremamente cautelosos ao fazer sacrifícios desnecessários"[596]. Se isso se aplica a governos, mais ainda a empresas provedoras de aplicação.

---

[595] BRASIL. Superior Tribunal de Justiça. Recurso especial nº 1.348.532/SP, Rel. Min. Luis Felipe Salomão, julgado em 10/10/2017. RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES. RAZOABILIDADE. 1. É facultado ao Juízo proferir sua decisão, desde que não haja necessidade de produzir provas em audiência, assim como, nos termos do que preceitua o princípio da livre persuasão racional, avaliar as provas requeridas e rejeitar aquelas que protelariam o andamento do processo, em desrespeito ao princípio da celeridade. 2. A Anadec - Associação Nacional de Defesa do Consumidor, da Vida e dos Direitos Civis tem legitimidade para, em ação civil pública, pleitear o reconhecimento de abusividade de cláusulas insertas em contrato de cartão de crédito. Precedentes. 3. É abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento. 4. A cláusula posta em contrato de serviço de cartão de crédito que impõe a anuência com o compartilhamento de dados pessoais do consumidor é abusiva por deixar de atender a dois princípios importantes da relação de consumo: transparência e confiança. 5. A impossibilidade de contratação do serviço de cartão de crédito, sem a opção de negar o compartilhamento dos dados do consumidor, revela exposição que o torna indiscutivelmente vulnerável, de maneira impossível de ser mensurada e projetada. 6. De fato, a partir da exposição de seus dados financeiros abre-se possibilidade para intromissões diversas na vida do consumidor. Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas. Por isso, a imprescindibilidade da autorização real e espontânea quanto à exposição. 7. Considera-se abusiva a cláusula em destaque também porque a obrigação que ela anuncia se mostra prescindível à execução do serviço contratado, qual seja obtenção de crédito por meio de cartão. 8. Não se estende a abusividade, por óbvio, à inscrição do nome e CPF de eventuais devedores em cadastros negativos de consumidores (SPC, SERASA, dentre outros), por inadimplência, uma vez que dita providência encontra amparo em lei (Lei n. 8.078/1990, arts. 43 e 44). 9. A orientação fixada pela jurisprudência da Corte Especial do STJ, em recurso repetitivo, no que se refere à abrangência da sentença prolatada em ação civil pública, é que "os efeitos e a eficácia da sentença não estão circunscritos a lindes geográficos, mas aos limites objetivos e subjetivos do que foi decidido, levando-se em conta, para tanto, sempre a extensão do dano e a qualidade dos interesses metaindividuais postos em juízo (arts. 468, 472 e 474, CPC e 93 e 103, CDC)" (REsp 1.243.887/PR, Rel. Ministro LUIS FELIPE SALOMÃO, CORTE ESPECIAL, DJe de 12/12/2011). 10. É pacífico o entendimento no sentido de que a revisão da multa fixada, para o caso de descumprimento de ordem judicial, só será possível, nesta instância excepcional, quando se mostrar irrisória ou exorbitante, o que, a meu ver, se verifica na hipótese, haja vista tratar-se de multa diária no valor de R$10.000,00 (dez mil reais). 11. Recurso especial parcialmente provido.

[596] SOLOVE, Daniel J. Nothing to hide: The false tradeoff between privacy and security. Yale University Press, 2011, p. 61.

Partindo desses mesmos argumentos, e mais ainda com baliza recente da LGPD, o Tribunal certamente concluiria que grande parcela do tratamento de dados atualmente empreendido pelos provedores de aplicação é abusiva, pois desnecessária ao adequado funcionamento dos softwares.

Então, espera-se que o desenvolvimento dessas duas propostas (principalmente da primeira delas, que é mais sofisticada) possa mudar o paradigma da visão de negócios das empresas de tecnologia. Isso para que não busquem os lucros apenas com o obscuro tratamento e processamento dos dados pessoais dos usuários, mas para que sejam transparentes o suficiente ao ponto de, *confessando* e *admitindo* que fornecem os dados a parceiros comerciais mediante remuneração, possam informar isso diretamente ao usuário – afinal, o real titular daqueles dados – e dar-lhe a opção de consentir ou não com aquele tratamento determinado.

E, com a informação sendo clara e transparente, o consentimento teria um peso muito mais substancial, o que geraria inclusive maior proteção à atividade empresarial. O mesmo se diz do próprio legítimo interesse, que seria mais explicativo e facilmente inteligível pelo titular dos dados. O desenvolvimento desse conceito seria, sim, muito mais alinhado à ideia basilar de *privacy by design* e de *privacy by default*, pois se pensaria na privacidade a cada passo do ciclo de desenvolvimento da rotina do tratamento por padrão, sem necessidade de provocação pelo usuário[597].

[597] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

CONCLUSÕES

Após a pesquisa aqui desenvolvida, sobretudo com base nos aplicativos móveis mais utilizados pela pessoa ordinária – redes sociais, e-mails, navegadores, ferramentas de compras, bancos, diversão e entretenimento, educação, notícias, turismo e ferramentas de produtividade –, foi possível fazer uma ampla análise a nível macro de como se dá a tutela da privacidade no âmbito da sociedade hiperconectada, em que há mais *smartphones* do que pessoas[598].

Em um primeiro momento, o direito à privacidade foi colocado no prisma do mundo digital, tendo sido abordados o seu conteúdo jurídico clássico e a sua evolução até o âmbito da proteção de dados e dos contratos eletrônicos. Nesse ponto, aliás, desenvolveu-se o panorama nacional dos direitos no âmbito da internet, sobretudo com a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados). Como a criação das leis nacionais foi resultado de positiva pressão internacional por uma proteção minimamente equitativa dos dados pessoais a nível internacional, restou imprescindível um desenvolvimento mais analítico sobre o panorama europeu de proteção de dados privados, com o RGPD – tido internacionalmente como o marco mais avançado na referida tutela.

Como fechamento da introdução teórica, foram desenvolvidos conceitos básicos de direito contratual e de direito do consumidor; afinal, os termos de privacidade dos aplicativos móveis nada mais são do que verdadeiros contratos eletrônicos de adesão imersos numa relação consumerista, de modo que referidos institutos jurídicos foram, durante muito tempo, responsáveis pelo que se entendeu como tutela da proteção dos dados no Brasil.

Feita a breve revisão de conceitos teóricos básicos, passou-se à análise mais detida dos termos de privacidade dos aplicativos selecionados. Para facilitar o estudo – e por decorrência lógica das etapas –, pensou-se em uma análise tripartida. Em primeiro lugar, estudou-se como se dá o consentimento do usuário acerca dos termos de privacidade e das políticas de privacidade dos aplicativos: o objetivo foi de, em suma, verificar a efetiva transparência dos aplicativos e aferir a possibilidade de revogação de consentimento pelo usuário (um direito legalmente previsto).

Para tanto, todos os aplicativos foram instalados no celular utilizado no trabalho e brevemente avaliados – página de instalação e interface intuitiva das funcionalidades principais

---

[598] ESTADÃO. Brasil já tem mais de um smartphone ativo por habitante, diz estudo da FGV. Disponível em: <https://link.estadao.com.br/noticias/geral,brasil-ja-tem-mais-de-um-smartphone-ativo-por-habitante-diz-estudo-da-fgv,70002275238>. Acesso em: 9 abr. 2021.

–, na medida em que uma análise detalhada de mais de uma centena de *softwares* seria inviável para fins deste trabalho, que pretendeu ser mais abrangente do que focado, a fundo, em algum aplicativo específico.

Em segundo lugar, foram avaliadas as principais permissões concedidas aos aplicativos móveis, para aferir as mais comuns e se elas guardavam efetiva correlação com o objeto do aplicativo, sempre sob o prisma do dever legal de coleta do menor número de dados estritamente necessários e adequados ao correto funcionamento da aplicação. Para a comparação crítica, foram montadas diversas tabelas para cada das categorias criadas, estando todas no Apêndice B.

Em terceiro e último lugar, foram avaliados os aspectos mais relevantes dos termos de privacidade de cada um dos aplicativos. Ou seja, foram lidas as dezenas de termos de privacidade para aferir as cláusulas mais interessantes, alinhadas e desalinhadas com a lógica da LGPD, além de obscuras.

Partindo de toda essa análise, os resultados alcançados não foram bons, o que demonstra que a proteção aos dados pessoais ainda *não pegou* no Brasil. Para facilitar a compreensão, o desenvolvimento das conclusões partirá dos problemas de pesquisa formulados ao início do trabalho.

A primeira constatação foi a baixíssima transparência dos *softwares* analisados no tocante à sua política de privacidade. Não são suficientemente informados os dados pessoais coletados e nem o seu destino. Regra geral, todos os aplicativos solicitam permissões excessivas de acesso às informações do usuário, mas se limitam a afirmar que compartilharão com "terceiros confiáveis".

Alguns poucos aplicativos exibem quem realmente são esses terceiros e possibilitam que o usuário faça a revogação específica do consentimento – fala-se aqui explicitamente do *CNN* e do *Fox News*, ambos situados longe do contexto do brasileiro ordinário.

Partindo disso, parece fora de cogitação que a balança da ponderação deve pender mais para a tutela da privacidade, e não para a manutenção das cláusulas contratuais, normalmente abusivas e obscuras. Essa é uma decorrência do próprio direito à privacidade, mas também da proteção à boa-fé contratual e à função social do contrato, afinal não se pode cogitar de que contratos que não possibilitam o consentimento livre e informado efetivamente chancelem o lucro a apenas um dos lados, sem qualquer contraprestação real ao usuário.

Nesse ponto, parece que a experiência da total autorregulação da internet não deu muito certo: a maioria das empresas, infelizmente, tende a abolir os direitos básicos dos

usuários, partindo de um pretenso pressuposto de que, se o usuário fez o *download* do *software*, precisa *aceitar* tudo o que vem nele embutido, inclusive as políticas de privacidade desalinhadas das normas nacionais e internacionais.

Não fosse assim, a Europa não teria editado o RGPD. Falando-se em panorama europeu, é de se frisar que a legislação nacional não fugiu muito daquele paradigma, o que é positivo. Afinal, é preferível que a regulação esteja a um nível similar no âmbito internacional, pois não é factível que as empresas precisem se adaptar a regulações tão díspares no âmbito da internet, que, por conceito, é globalmente conectado.

Assim, se o Brasil fugir muito do panorama internacional, haverá verdadeira fuga das empresas do mercado nacional, na medida em que a adaptação às normas tupiniquins será mais cara do que os eventuais lucros aferíveis com os usuários brasileiros. Mas, comparando a LGPD ao RGPD, é possível ver que o Brasil não fugiu muito do esperado dentro do paradigma internacional.

Na análise específica dos aplicativos governamentais, vê-se que, como as suas funcionalidades são mais específicas e em menor espectro do que todos os demais avaliados, as permissões são em menor número. Ao revés, a transparência também não é o forte dos *softwares* governamentais; e, nesse contexto, a publicidade republicana – de que decorre o dever de transparência – é um princípio constitucional (art. 37 da CRFB/88).

De modo geral, os aplicativos públicos não recorrem à publicidade dirigida, mas a incipiência dos termos de privacidade dificulta ainda mais a correta compreensão de o que é feito com os dados porventura coletados dos usuários. E, em sentido semelhante, parece não haver muitas razões para que um aplicativo oficial tenha acesso à exata localização do usuário e possibilidade de ler arquivos de fotos e armazenamento, inclusive com capacidade de gerenciamento.

Por sua vez, a transparência deve ser a regra dos termos de privacidade dos aplicativos móveis, na medida em que se trata do único modo de garantir que o consentimento do usuário seja realmente livre, consciente, informado, inequívoco e expresso. Afinal, para que uma pessoa abra mão de parcelas de sua privacidade e, possivelmente, dados sensíveis, é necessário que esteja realmente advertida das possíveis consequências. Se, ainda assim, aceitar a compressão da privacidade, o aplicativo estará na linha certa.

O mesmo se diz do legítimo interesse, que, para ser efetivamente legítimo, deve ser balizado pelo teste de proporcionalidade insculpido na LGPD, ao qual é imprescindível a transparência ativa sobre como é feito o tratamento dos dados.

A mesma conclusão aqui apontada foi recentemente relatada também por outros estudiosos. Héctor Valverde e Anna Salles, por exemplo, afirmam que os termos e condições "não tem atingido o seu propósito de informar o consumidor de forma adequada", de modo que "devem ser reformulados para que se tornem mais didáticos, munidos de uma linguagem mais simples e direta, de maneira que se aumente a compreensibilidade do conteúdo, bem como se diminua o tempo de leitura"[599]. Algumas soluções propostas pelos autores, e para as quais aqui também se advoga, são mecanismos de áudios e vídeos, esquemas, resumos, destaques, tabelas. Tudo isso com o foco de tentar dar transparência mais ativa ao usuário dos aplicativos.

Por fim, o conceito de níveis de aplicativos aqui pensado não deve ser encarado como a mercantilização de direitos fundamentais. Ao revés, trata-se de uma forma aparentemente justa de equilibrar os legítimos interesses das empresas de tecnologia – de auferir renda em razão do produto ofertado – e os direitos dos usuários – de serem informados sobre eventuais tratamentos de seus dados. Nesse sentido, a ideia é no sentido de que o usuário terá à sua escolha o cardápio de funcionamento do aplicativo.

Com efeito, se ele quiser permitir que o *software* acesse e utilize seus dados para quaisquer fins – normalmente, publicidade comportamental –, terá essa opção; mas também terá a opção de resguardar determinados dados e tipos de tratamento, sendo isso normalmente associado ao pagamento de algum valor. Além disso, os *níveis* consistiriam no funcionamento de determinadas parcelas do *software*, a depender de quais permissões foram concedidas pelo usuário.

Pensa-se que a solução pelos níveis de aplicativo, com a intrínseca maior transparência às cadeias de tratamento dos dados pessoais dos usuários, é complementar a outras iniciativas tecnológicas para melhorar o trato e o controle dos dados pessoais. Com efeito, o consentimento – aqui materializado na ideia granular dos níveis de aplicativo – ainda terá grande relevância no mercado dos dados pessoais durante muito tempo, mesmo que seja criticado por assumir uma pretensa capacidade do usuário de efetivamente entender aquilo com o que concorda.

Assim, o funcionamento parcial das aplicações e o consentimento granular com a monetização direta do tratamento dos dados é complementar à ideia das Tecnologias de Facilitação da Privacidade (PETs), que buscam se utilizar de uma espécie de virada conceitual: começar a colocar as ferramentas tecnológicas para *jogarem* a favor da maior privacidade e

[599] SANTANNA, Héctor Valverde; RAMOS, Anna Luíza Salles. A efetividade do direito à informação adequada em relação aos termos de uso e serviço e políticas de privacidade. *In*: Revista de Direito do Consumidor, v. 134, 2021.

adequada proteção dos dados pessoais, e não o contrário. Isso porque, como afirma Bioni, dado que "a própria autorregulação mostrou-se frustrante para tal desiderato, necessária se faz, então, uma *intervenção regulatória paternalista (libertária)* para corrigir essa distorção do mercado informacional. Deve haver mecanismos que empoderem o cidadão com um controle efetivo de seus dados pessoais"[600].

Dessa forma, é claro que o caminho da *contratualização* do trato dos dados pessoais não deve ser o único modelo adotado para o resguardo dos direitos fundamentais dos cidadãos. As políticas de privacidade não têm, hoje, o condão de bem tutelar os dados pessoais dos usuários dos aplicativos. Sustenta-se, contudo, que as mudanças relatadas ao longo do trabalho, sobretudo com uma nova lógica de diminuir o caráter de mera adesão das políticas, podem ajudar a melhorar o cenário da proteção dos dados pessoais dos usuários de aplicativos no Brasil. Protege-se, assim, a autonomia do cidadão sob o prisma procedimental e substantivo.

Isso é, com o caminho de integração aqui proposto – proteção de dados por meio de novas ferramentas tecnológicas e com as já antigas balizas de transparência e *accountability* –, supera-se, de certo modo, as três críticas fulcrais ao paradigma do consentimento expressadas por Laura Schertel[601] e Bruno Bioni[602].

Com efeito, com informações mais claras, transparentes e didáticas, fala-se menos em limitações cognitivas do titular dos dados pessoais para efetivamente entender e consentir com o tratamento dos dados; ou, de igual modo, o legítimo interesse do operador do tratamento fica mais evidenciado, a partir da demonstração do teste de proporcionalidade. Então, não se trata mais de um simples "*notice and consent*" ("avisar e consentir")[603], mas de um consentimento baseado em uma informação verdadeira, clara e completa.

A crítica à desigualdade de poderes, que se manifesta pela lógica binária do *take it or leave it* seria atenuada a partir da dinâmica proposta para os níveis de aplicativo, seja com o consentimento granular para o funcionamento parcial das ferramentas – o que parece ser viável do ponto de vista da tecnologia da informação –, seja por meio da contraprestação pecuniária

---

[600] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[601] MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. JOURNAL OF INSTITUTIONAL STUDIES, [S.l.], v. 6, n. 2, p. 507-533, set. 2020. Disponível em: <https://estudosinstitucionais.emnuvens.com.br/REI/article/view/521>. Acesso em: 5 abr. 2021.

[602] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

[603] SOLOVE, Daniel J. The Myth of the Privacy Paradox. GWU Legal Studies Research Paper no. 2020-10, 2020. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265> Acesso em: 4 jun. 2021.

mais direta pelo não tratamento dos dados pessoais. Consegue-se, assim, diminuir o espectro de vulnerabilidade do usuário e consumidor no bojo das contratações eletrônicas[604].

Por sua vez, a crítica ao fato de que o contexto de *Big Data* impossibilita o gerenciamento individual dos riscos no momento da coleta dos dados é mais bem enfrentada pelo desenvolvimento teórico da privacidade contextual, uma verdadeira manifestação da boa-fé no âmbito da manifestação do consentimento ou da aplicação do legítimo interesse[605].

Para isso, é imprescindível que as políticas de privacidade sejam claras quanto à *cadeia de custódia* dos dados pessoais dos usuários e aos seus direitos de exclusão, correção e outros. Não pode haver verdadeiras "caixas pretas" no bojo dos dados pessoais[606]. Afinal, como o STF decidiu, inexiste, em um contexto de processamento eletrônico e ubíquo de dados na sociedade da informação, dado neutro e sem valor[607]. Deve-se sair do paradigma retratado por Frank Pasquale de que, hoje, os controladores de dados têm uma arquitetura baseada na maximização de lucros e na busca pela inovação acima de tudo, e não para tratar de modo correto os titulares dos dados[608]. Esse utilitarismo não é compatível com a ordem constitucional[609].

O caminho rumo à correta tutela da privacidade é longo é árduo, mas parece valer a pena. Hoje, a sociedade hiperconectada e hiperexposta – que ainda é uma novidade para a atual geração – parece algo positivo. O temor é de que no futuro não seja, momento em que já será tarde para mudar o *mindset* de todos os *players* do sistema – usuários, governos e empresas.

---

[604] MARQUES, Claudia Lima; MIRAGEM, Bruno. O Novo Direito Privado e a Proteção dos Vulneráveis. São Paulo: Revista dos Tribunais, 2012, p. 117.

[605] NISSENBAUM, Helen. A Contextual Approach to Privacy Online. Daedalus, the Journal of the American Academy of Arts & Sciences, v. 140, n.4, pp. 32-48, Fall 2011, p. 33.

[606] CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[607] MENDES, Laura Schertel; BIONI, B. R. . O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. REVISTA DE DIREITO DO CONSUMIDOR, v. 124, p. 157, 2019.

[608] PASQUALE, Frank. The black box society. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015. p. 146.

[609] "Em primeiro lugar, direitos fundamentais não podem estar sujeitos, exclusivamente, a juízos de custo-benefício, uma vez que são deontológicos e vinculantes. Em segundo lugar, não necessariamente existe o trade-off entre eficiência e privacidade, diante da multiplicidade de técnicas e ferramentas que podem ser utilizadas para movimentar a economia digital, mas preservando as situações existenciais dos titulares de dados. Em terceiro lugar, ainda que sempre houvesse o trade-off, seria preciso ponderar que a inovação não é um valor absoluto e que, exatamente por isso, não pode ser perseguida de forma irrestrita e às custas do sacrifício das situações existenciais mais elementares dos titulares de dados. Consequentemente, é indispensável que a heterorregulação, assim entendida a regulação pelo Estado, possa endereçar os problemas apontados, tal como é a razão de ser da própria LGPD". FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

E, havendo controvérsias sobre o direito a ser esquecido, são os dados coletados e tratados hoje que definirão boa parte das relações sociais do futuro, de modo que é urgente que se balize o tratamento dos dados pessoais no presente, para que seja legítimo e respeite as balizas legais.

REFERÊNCIAS

4SHARED. 4shared App Privacy Statement. Disponível em: <https://www.4shared.com/privacyForApps.jsp>. Acesso em: 11 abr. 2021.

99. Política de Privacidade. Disponível em: <https://99app.com/legal/privacidade/>. Acesso em: 12 abr. 2021.

ABADE, André da Silva; ALVES, Josilene Dália. Política de privacidade e dados pessoais: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. Facisa on-line, Barra do Garças, n. 1, jul. 2017.

ABREU, Jacqueline de Souza. ESPECIAL: As "permissões" de acesso a dados em apps do governo. Disponível em: <http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-as-permissoes-de-acesso-dados-em-apps-do-governo/>.

ACQUISTI, Alessandro; TAYLOR, Curtis; WAGMAN, Liad. The Economics of Privacy. Disponível em: <https://www.ftc.gov/system/files/documents/public_comments/2017/10/00006-141501.pdf>. Acesso em: 4 jun. 2021.

ADOBE. Política de privacidade da Adobe. Disponível em: <https://www.adobe.com/br/privacy/policy.html>. Acesso em: 11 abr. 2021.

ADSQUARE. Privacy Policy & Opt-Out. Disponível em: <https://www.adsquare.com/privacy/>. Acesso em: 11 abr. 2021.

AIRBNB. Política de Privacidade do Airbnb. Disponível em: <https://www.airbnb.com.br/terms/privacy_policy>. Acesso em: 12 abr. 2021.

ALIBABA. Privacy Policy. Disponível em: <https://rule.alibaba.com/rule/detail/2034.htm>. Acesso em: 13 abr. 2021.

AMAZON. Amazon Privacy Notice. Disponível em: <https://www.amazon.com/gp/help/customer/display.html/?ie=UTF8&nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_467C686A137847768F44B619694D3F7C>. Acesso em: 13 abr. 2021.

ANDRADE, Norberto Nuno Gomes de Andrade. The right privacy and the right to identity in the Age of ubiquitous computing: Friends or foes? A proposal towards a legal articulation. In: AKRIVOPOLOUS, Christina; PSYGKAS, Athanasious (Org.). Personal data privacy and protection in a surveillance era: technologies and practices. New York: Information Science

Reference, 2011. p. 20.

ANTONIALLI, Dennys; CRUZ, Francisco Brito. Privacidade e internet: desafios para a democracia brasileira. Ensaios democracia digital, São Paulo, n. 1, mar. 2017.

APP ANNIE. State of mobile 2021. Disponível em: <https://f.hubspotusercontent20.net/hubfs/8885028/App%20Annie%20-The%20State%20Of%20Mobile%202021%20.pdf>. Acesso em: 7 abr. 2021.

APPLE. Apple Customer Privacy Policy. Disponível em: <https://www.apple.com/legal/privacy/br/>. Acesso em: 12 abr. 2021.

APPLE. Solicitar e fazer compras com o "Pedir para comprar". Disponível em: <https://support.apple.com/pt-br/HT201089>. Acesso em: 17 mar. 2021.

ARDENGHI, Régis Schneider. Direito à vida privada e direito à informação: colisão de direitos fundamentais. Revista da ESMESC. [S.l.], v. 19, n. 25, p. 227-251, 2012. Disponível em: <http://revista.esmesc.org.br/re/article/view/57>. Acesso em: 21 mar. 2021.

ARENDT, Hannah. A condição humana. 10 ed. Rio de Janeiro: Forense Universitária, 2005, p. 33.

ARENDT, Hannah. Reflections on Little-Rock. Dissent Magazine, v. 6, n. 1, inverno, 1959, p. 52-53.

AVAST. Política de Privacidade. Disponível em: < https://www.avast.com/pt-br/privacy-policy>. Acesso em: 11 abr. 2021.

AVG. Política de Privacidade. Disponível em: <https://www.avg.com/pt-br/privacy>. Acesso em: 11 abr. 2021.

BABBEL. Privacy Statement for Babbel. Disponível em: <https://about.babbel.com/en/privacy/>. Acesso em: 11 abr. 2021.

BANCO DO BRASIL. Política de Privacidade. Disponível em: <https://www.bb.com.br/pbb/pagina-inicial/voce/politicas-de-uso-e-privacidade#/>. Acesso em: 12 abr. 2021.

BANCO INTER. Termos de Uso e Política de Privacidade. Disponível em: <https://www.bancointer.com.br/politica-de-privacidade/>. Acesso em: 12 abr. 2021.

BAND. Termos de Uso de Aplicativo e Política de Privacidade. Disponível em: <https://www.band.uol.com.br/segundatela/politicas.html>. Acesso em: 12 abr. 2021.

BARROSO, Luis Roberto. A dignidade da pessoa humana no direito constitucional contemporâneo: A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Fórum, 2016, p. 9-87.

BARROSO, Luís Roberto. Os princípios da razoabilidade e da proporcionalidade no direito

constitucional. Boletim de Direito Administrativo. Doutrina, pareceres e atualidades. Março/97. Pp. 156-166, p. 161.

BAUMAN, Zygmunt. Vigilância líquida: diálogos com David Lyon. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Editor, 2014.

BBC. 5 formas rápidas e fáceis de reduzir seus rastros na internet. Disponível em: <https://www.bbc.com/portuguese/geral-43585945>. Acesso em: 5 abr. 2021.

BBC. Coronavirus: How does the test-and-trace system work? Disponível em: <https://www.bbc.com/news/explainers-52442754>. Acesso em: 8 abr. 2021.

BBC. Cuán cierto es que las empresas usan el micrófono de tu teléfono para escucharte y qué hacer al respecto. Disponível em: <https://www.bbc.com/mundo/noticias-44724389>. Acesso em: 3 jun. 2021.

BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 26 mar. 2021.

BBC. O escândalo que fez o Facebook perder US$ 35 bilhões em horas. Inglaterra, 2018. Disponível em: <http://www.bbc.com/portuguese/internacional-43466255>. Acesso em: 20 mar. 2021.

BBC. The BBC Privacy and Cookies Policy. Disponível em: <http://www.bbc.com/usingthebbc/privacy/privacy-policy/>. Acesso em: 12 abr. 2021.

BELLIZZE, Marco Aurélio; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

BELTRÃO, Silvio Romero. Direitos da personalidade. 2. ed. São Paulo: Atlas, 2014, p. 10.

BENJAMIN. Antônio Herman de Vasconcellos e. Capítulo V – Das Práticas Comerciais. In: GRINOVER, Ada Pellegrini et al. Código de Defesa Brasileiro do Consumidor: comentado pelos autores do anteprojeto. 10 ed. Rio de Janeiro: Forense. 2011. v.1. p. 259-510.

BESSA, Leonardo Roscoe. A Lei Geral de Proteção de Dados e o direito à autodeterminação informativa. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2020-out-26/leonardo-bessa-lgpd-direito-autodeterminacao-informativa>. Acesso em: 4 jun. 2021.

BESSA, Leonardo Roscoe. LGPD: direito ou dever de privacidade? Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2021-fev-08/leonardo-bessa-lgpd-direito-ou-dever-privacidade>. Acesso em: 4 jun. 2021.

BESSA, Leonardo Roscoe. O consumidor e os limites dos bancos de dados de proteção ao crédito. São Paulo: Revista dos Tribunais: 2003.

BIGDOG GAMES. Privacy Policy. Disponível em: <http://www.crystalrover.com/privacy-policy.html>. Acesso em: 12 abr. 2021.

BIONI, Bruno R. Autodeterminação informacional: Paradigmas inconclusos entre os direitos da personalidade, regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação de Mestrado. Faculdade de Direito da Universidade de São Paulo, 2016.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

BIONI, Bruno Ricardo. Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação/GPoPAI da Universidade de São Paulo. 2016, p. 34-35.

BIONI, Bruno. O consentimento como processo: em busca do consentimento válido. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz. Tratado de proteção de dados pessoais. São Paulo: Forense: 2021.

BLUME, Peter. The inherent contradictions in data protection law. International Data Privacy Law, v. 2, n. 1, p. 27, 2012: "Seen from the perspective of the controllers, it is implied that data protection aims to make it legitimate to process personal data. (...) The fundamental observation is that data protection law is viewed as a societal necessity in order to make it possible for controllers to process personal data and to benefit from the information and knowledge processing entails".

BOLESINA, Iuri. O direito à extimidade: as inter-relações entre identidade, ciberespaço e privacidade. Florianópolis: Empório do Direito, 2017, p. 182.

BOLESINA, Iuri; SCHROEDER, Helena Carolina. A "limitação" voluntária dos direitos da personalidade no direito civil contemporâneo. XII Seminário Nacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea. Unisc, ed. 2016.

BOOKING. Política de Privacidade. Disponível em: <https://www.booking.com/content/privacy.pt-br.html?label=gen173nr-1FCBQoggJCB3ByaXZhY3lIHFgEaCCIAQGYARy4AQbIAQzYAQHoAQH4AQKIAgGoAgO4AtOayuUFwAIB&sid=51b8c4d59804d2478b5ba971f8448cb7&tmpl=docs%2Fprivacy-policy&lang=pt-br&soz=1&lang_click=top;cdl=nl;lang_changed=1>. Acesso em: 12 abr. 2021.

BORGES, Roxana Cardoso Brasileiro. Disponibilidade dos direitos de personalidade e autonomia privada. 2. Ed. São Paulo: Saraiva, 2007.

BRADESCO. Diretivas de Privacidade. Disponível em: <https://www.bradescoseguranca.com.br/portal/layout/temas/seguranca-corporativa/pdf/Diretivas-de-Privacidade-Mobile.pdf>. Acesso em: 12 abr. 2021.

BRAINLY. Priavcy policy. Disponível em: <https://brainly.com/pages/privacy_policy>. Acesso em: 13 abr. 2021.

BRASIL, Câmara dos Deputados. (2018). Parecer da Comissão Especial destinada a proferir parecer ao Projeto de Lei nº 4060, de 2016. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=SBT+1+PL406012+%3D%3E+PL+4060/2012>. Acesso em: 6 abr. 2021.

BRASIL. Caixa Econômica Federal. Política de Privacidade do site e dos aplicativos da Caixa. Disponível em: <http://www.caixa.gov.br/politica-de-privacidade/Paginas/default.aspx>. Acesso em: 11 abr. 2021.

BRASIL. Conselho Nacional de Justila. Justiça em números 2020. P. 46. Disponível em: <https://www.cnj.jus.br/wp-content/uploads/2020/08/WEB-V3-Justi%C3%A7a-em-N%C3%BAmeros-2020-atualizado-em-25-08-2020.pdf>. Acesso em: 5 abr. 2021.

BRASIL. Departamento Nacional de Trânsito. Política de Privacidade Carteira Digital de Trânsito. Disponível em: <https://portalservicos.denatran.serpro.gov.br/#/carteiradigital/politicaprivacidade>. Acesso em: 11 abr. 2021.

BRASIL. Distrito Federal. Companhia de Saneamento Ambiental do Distrito Federal. Política de privacidade de aplicativo mobile. Disponível em: <https://www.caesb.df.gov.br/594>. Acesso em: 11 abr. 2021.

BRASIL. Empresa Brasileira de Comunicação. Brasil perde 4,6 milhões de leitores em quatro anos. Disponível em: <https://agenciabrasil.ebc.com.br/educacao/noticia/2020-09/brasil-perde-46-milhoes-de-leitores-em-quatro-anos#:~:text=O%20brasileiro%20l%C3%AA%2C%20em%20m%C3%A9dia,tamb%C3%A9m%20como%20o%20mais%20marcante>. Acesso em: 6 abr. 2021.

BRASIL. Empresa Brasileira de Comunicação. Celular é o principal meio de acesso à internet no país. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2020-04/celular-e-o-principal-meio-de-acesso-internet-no-pais#:~:text=Acesso%20pelo%20celular%20aumentou%20para%2098%2C1%25%20de%202017%20para%202018&text=Os%20aparelhos%20s%C3%A3o%20o%20principal,por%20quase%20todos%20os%20brasileiros.&text=Os%20dados%20mostram%20que%2079,78%2C2%25%20em%202017.>. Acesso em: 26 mar. 2021.

BRASIL. Ministério da Saúde. Políticas de Privacidade. Disponível em: <https://validacovid.saude.gov.br/politica-privacidade>. Acesso em: 13 abr. 2021.

BRASIL. Ministério do Trabalho. Política de Privacidade. Disponível em: <https://empregabrasil.mte.gov.br/termos-e-privacidade/>. Acesso em: 11 abr. 2021.

BRASIL. Receita Federal do Brasil. Política de Privacidade. Disponível em: <http://receita.economia.gov.br/sobre/politica-de-privacidade>. Acesso em: 11 abr. 2021.

BRASIL. Serviço Federal de Processamento de Dados. Consentimento e legítimo interesse: faca de dois gumes. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/2019/consentimento-legitimo-interesse-faca-dois-gumes>. Acesso em: 26 mar. 2021.

BRASIL. Superior Tribunal de Justiça, REsp nº 1.308.830/RS, Rel. Min. Nancy Andrighi, DJe 19/06/2012.

BRASIL. Superior Tribunal de Justiça, REsp nº 1.342.640/RS, Rel. Min. Nancy Andrighi, DJe 14/02/2017.

BRASIL. Superior Tribunal de Justiça, REsp nº 976.836/RS, Rel. Min. Luiz Fux, DJe 05/10/2010.

BRASIL. Superior Tribunal de Justiça. Recurso especial nº 1.348.532/SP, Rel. Min. Luis Felipe Salomão, julgado em 10/10/2017.

BRASIL. Supremo Tribunal Federal. ADI 1790-MC/DF. Rel. Min. Sepúlveda Pertence. Tribunal Pleno. Julgamento em 23/4/1998, publicação em 8/9/2000.

BRASIL. Supremo Tribunal Federal. ADI-MC nº 6.387/DF, Rel. Min. Rosa Weber, julgamento em 7/5/2020.

BRASIL. Supremo Tribunal Federal. RE 418416, Relator: Sepúlveda Pertence, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006.

BRASIL. Supremo Tribunal Federal. RE nº 201.819/RJ, voto do Min. Gilmar Mendes, Segunda Turma, Diário da Justiça - 27/10/2006.

BRASIL. Supremo Tribunal Federal. RHC 132062 / RS - RIO GRANDE DO SUL, Redator do Acórdão Min. Edson Fachin, Julgamento em 22/11/2016, publicação em 24/10/2017, Primeira Turma. No mesmo sentido: HC 91867 / PA – PARÁ, Rel. Min. Gilmar Mendes; e RHC 169682 AgR / RS - RIO GRANDE DO SUL, Rel. Min. Luiz Fux.

BRASIL. Supremo Tribunal Federal. STF conclui que direito ao esquecimento é incompatível com a Constituição Federal. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=460414&ori=1>. Acesso em: 5 abr. 2021.

BRASIL. Tribunal Superior Eleitoral. Política de privacidade e termos de privacidade. Disponível em: <http://www.tse.jus.br/transparencia/politica-de-privacidade-e-termos-de-uso>. Acesso em: 11 abr. 2021.

CABIFY. Política de Privacidade Brasil. Disponível em: <https://cabify.com/brazil/privacy_policy?hidden=true>. Acesso em: 12 abr. 2021.

CALIFÓRNIA, ESTADOS UNIDOS DA AMÉRICA. California Consumer Privacy Act of 2018. Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>. Acesso em 6 abr. 2021.

CANALTECH. Neuralink | O que é e como funciona o projeto que conecta um chip ao cérebro. Disponível em: <https://canaltech.com.br/inteligencia-artificial/neuralink-o-que-e-como-funciona-170585/>. Acesso em: 26 mar. 2021.

CANALTECH. Os aplicativos mais baixados de 2020. Disponível em: <https://canaltech.com.br/apps/aplicativos-mais-baixados-2020-176201/>. Acesso em: 7 abr. 2021.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. Sequência (Florianópolis), Florianópolis, n. 76, p. 213-239, 2017.

CANOTILHO, J. J. Gomes; MACHADO, Jónatas E. M. Reality shows e liberdade de programação. Coimbra: Coimbra, 2003. p. 57.

CANTALI, Fernanda Borghetti Direitos da Personalidade: disponibilidade relativa, autonomia privada e dignidade humana. Dissertação (Mestrado em Direito) – Faculdade de Direito, PUCRS, Porto Alegre, 2008, 271f.

CHEETAH MOBILE CLEAN MASTER. Privacy Policy. Disponível em: <https://www.cmcm.com/protocol/site/privacy.html>. Acesso em: 11 abr. 2021.

CNIL. Data protection around the world. Disponível em: <https://www.cnil.fr/en/data-protection-around-the-world>. Acesso em: 24 mar. 2021.

CNN. CNN Privacy Policy. Disponível em: <https://edition.cnn.com/privacy0?no-st=9999999999>. Acesso em: 12 abr. 2021.

COALIZÃO DIREITOS NA REDE. Seus Dados São Você. Disponível em: <https://direitosnarede.org.br/campanha/seus-dados-sao-voce/>. Acesso em: 26 mar. 2021.

COHEN, Julie E. What Privacy is For. Harvard Law Review, Vol. 126, 2013, p. 1931.

COMISSÃO EUROPEIA. O que são dados pessoais? Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt>. Acesso em: 26 mar. 2021.

CONESA, Fulgencio Madrid. Derecho a la intimidad, informática y Estado de Derecho. Valencia: Universidad de Valencia, 1984, p. 45.

CONJUR. Indicação de URL é imprescindível para remoção de conteúdo da internet. Disponível em: <https://www.conjur.com.br/2020-jan-29/indicacao-url-imprescindivel-remover-conteudo-internet>. Acesso em: 5 abr. 2021.

CONJUR. MP-DF vai investigar vazamento de dados do Facebook. Disponível em: <https://www.conjur.com.br/2018-out-01/mp-df-investigar-vazamento-dados-facebook>. Acesso em: 24 mar. 2021.

CORREIO BRAZILIENSE. Mãe luta para banir memes na internet com foto do filho deficiente. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/mundo/2016/02/01/interna_mundo,516149/mae-luta-para-banir-memes-na-internet-com-foto-do-filho-deficiente.shtml>. Acesso em: 22 mar. 2021.

COTS, Márcio, e OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 2ª ed. Rev. Atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019. Pág 86.

CRANOR, Lorrie Faith; MCDONALD, Aleecia M. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising, p. 1. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>. Acesso em: 3 jun. 2021.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo, São Paulo, v. 13, ano 4, p. 59-67, out.-dez. 2017.

CUEVA, Ricardo Villas Bôas. A proteção de dados pessoais na jurisprudência do Superior Tribunal de Justiça. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

DALLARI, Dalmo de Abreu. Viver em Sociedade. Frutal-MG: Prospectiva. 2ª Edição, 2014, p. 13.

DECOLAR. Política de Privacidade Decolar. Disponível em: <https://comercial.decolar.com/br/confidentiality>. Acesso em: 12 abr. 2021.

DEEZER. Política de privacidade e de cookies. Disponível em: <https://www.deezer.com/legal/personal-datas>. Acesso em: 12 abr. 2021.

DER SPIEGEL. So gehen wir mit Ihren Daten um. Disponível em: <https://www.spiegel.de/extra/datenschutzerklaerung-so-gehen-wir-mit-ihren-daten-um-a-1207780.html>. Acesso em: 12 abr. 2021.

DIGIO. O Digio se compromete com a sua privacidade. Disponível em:

<https://www.digio.com.br/assets/Politica_de_privacidade.pdf>. Acesso em: 12 abr. 2021.

DIGITAL ADVERTISING ALLIANCE. Disponível em: <https://digitaladvertisingalliance.org/>. Acesso em: 7 abr. 2021.

DISNEY. Data protection in Brazil. Disponível em: <https://privacy.thewaltdisneycompany.com/en/current-privacy-policy/data-protection-in-brazil/>. Acesso em: 13 abr. 2021.

DISNEY. Privacy policy. Disponível em: <https://privacy.thewaltdisneycompany.com/en/current-privacy-policy/>. Acesso em: 13 abr. 2021.

DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 13 dez. 2011.

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. 2000. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/8196-8195-1-PB.htm>. Acesso em: 21 mar. 2021.

DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. Rio de Janeiro: Renovar, 2006, p. 125.

DONEDA, Danilo. O IPv6 e a internet das coisas. Disponível em: <http://observatoriodainternet.br/o-ipv6-e-a-internet-das-coisas>. Acesso em 26 mar. 2021.

DOS REIS, Jorge Renato; BOLESINA, Iuri. A disponibilidade (no exercício) dos direitos da personalidade como deferência à dignidade humana no direito civil constitucionalizado. Revista Em Tempo, [S.l.], v. 14, p. 11-30, mar. 2016. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/1287>. Acesso em: 22 maio 2021.

DROPBOX. Dropbox Privacy Policy. Disponível em: <https://www.dropbox.com/privacy?mobile=1>. Acesso em: 11 abr. 2021.

DUOLINGO. Privacy Policy. Disponível em: <https://www.duolingo.com/privacy>. Acesso em: 11 abr. 2021.

EBAY. Aviso de Privacidade do Usuário. Disponível em: <https://www.ebay.com/pages/help/policies/privacy-policy.html>. Acesso em: 13 abr. 2021.

EBAY. User Corporate Rules. Disponível em: <https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf>.

Acesso em: 13 abr. 2021.

EL PAÍS. “Temos de rechaçar a mentalidade do ‘nós contra eles’ que os cínicos tentam nos vender”. Disponível em: <https://brasil.elpais.com/brasil/2016/07/09/internacional/1468096197_045190.html>. Acesso em: 6 abr. 2021.

EL PAÍS. Política de privacidad de los servicios El País. Disponível em: <https://elpais.com/estaticos/politica-privacidad/>. Acesso em: 12 abr. 2021.

ELECTRONIC ARTS. Privacy and Cookie Policy. Disponível em: <https://tos.ea.com/legalapp/WEBPRIVACY/US/en/PC/>. Acesso em: 12 abr. 2021.

ENJOEI. Política de privacidade e confidencialidade da informação. Disponível em: <https://www.enjoei.com.br/ajuda/sobre-o-enjoei/politica-de-privacidade-e-termos-de-uso-do-enjoei/politica-de-privacidade-e-confidencialidade-da-informacao>. Acesso em: 13 abr. 2021.

ESTADÃO. ‘A privacidade na web é uma ilusão’. Disponível em: <https://link.estadao.com.br/noticias/geral,a-privacidade-na-web-e-uma-ilusao,10000032646>. Acesso em: 26 mar. 2021.

ESTADÃO. Brasil já tem mais de um smartphone ativo por habitante, diz estudo da FGV. Disponível em: <https://link.estadao.com.br/noticias/geral,brasil-ja-tem-mais-de-um-smartphone-ativo-por-habitante-diz-estudo-da-fgv,70002275238>. Acesso em: 9 abr. 2021.

ESTRADA, Manuel Martín Pino. O comércio bilionário de dados pessoais na internet. Acadêmica Faculdade Progresso, Guarulhos, n. 2, 2017.

EUROPA. Cyber Chronix, a game to understand data protection rights and raise awareness on privacy risks. Disponível em: <https://ec.europa.eu/jrc/en/research-topic/security-privacy-and-data-protection/cyber-chronix>. Acesso em 4 jun. 2021.

EVANS, David D. The economics of the online advertising industry. Journal of Economic Perspectives, Apr. 2009, p.42. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1376607>. Acesso em: 5 abr. 2021.

EXAME. Apple se mantém como marca mais valiosa do mundo; veja ranking. Disponível em: <https://exame.com/tecnologia/apple-se-mantem-como-marca-mais-valiosa-do-mundo-veja-ranking/>. Acesso em: 5 abr. 2021.

EXAME. Justiça determina que YouTube remova vídeo de Nissim Ourfali. Disponível em: <https://exame.abril.com.br/tecnologia/justica-determina-que-youtube-remova-video-de-nissim-ourfali/>. Acesso em: 22 mar. 2021.

EXAME. Saiba quais foram os aplicativos mais baixados no Brasil e no mundo. Disponível

em: <https://exame.com/tecnologia/saiba-quais-foram-os-aplicativos-mais-baixados-no-brasil-e-no-mundo/>. Acesso em: 7 abr. 2021.

EXAME. Vazamento de dados de "220 milhões de brasileiros" não aconteceu da noite para o dia. Disponível em: <https://exame.com/tecnologia/vazamento-de-dados-de-220-milhoes-de-brasileiros-nao-aconteceu-da-noite-para-o-dia/>. Acesso em: 26 mar. 2021.

FACEBOOK. Política de Dados. Disponível em: <https://www.facebook.com/about/privacy/>. Acesso em: 5 abr. 2021.

FAPESP. Mais velho Homo sapiens, de 300 mil anos, é encontrado no Marrocos. Disponível em: <https://revistapesquisa.fapesp.br/mais-velho-homo-sapiens-de-300-mil-anos-e-encontrado-no-marrocos/>. Acesso em: 26 mar. 2021.

FERNANDES, David Augusto. Dados pessoais: uma nova commodity, ligados ao direito a intimidade e a dignidade da pessoa humana. Revista Jurídica, Curitiba, n. 49, 2017.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo. 1993. v. 88.

FLIPBOARD. Flipboard Privacy Policy. Disponível em: <https://about.flipboard.com/privacy/>. Acesso em: 12 abr. 2021.

FOLHA DE SÃO PAULO. Depois da Cambridge Analytica, especialistas em privacidade têm direito ao 'eu não disse?'. São Paulo, 2018. Disponível em: <https://www1.folha.uol.com.br/mercado/2018/04/depois-da-cambridge-analytica-especialistas-em-privacidade-tem-direito-ao-eu-nao-disse.shtml>. Acesso em: 15 abr. 2021.

FOLHA DE SÃO PAULO. Facebook vira alvo do Ministério da Justiça por vazamento de dados. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/03/facebook-vira-alvo-do-ministerio-da-justica-por-vazamento-de-dados.shtml>. Acesso em: 24 mar. 2021.

FOLHA DE SÃO PAULO. Política de Privacidade - Folha de S.Paulo. Disponível em: <https://www1.folha.uol.com.br/paineldoleitor/2018/05/politica-de-privacidade-folha-de-spaulo.shtml>. Acesso em: 12 abr. 2021.

FOLHA DE SÃO PAULO. Redes sociais criam bolhas ideológicas inacessíveis a quem pensa diferente. Disponível em: <https://www1.folha.uol.com.br/ilustrissima/2017/09/1920816-cada-macaco-no-seu-galho---zuckerman.shtml>. Acesso em: 5 abr. 2021.

FORBES. Data Is The New Oil -- And That's A Good Thing. Disponível em: <https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=614ec1817304>. Acesso em: 26 mar. 2021.

FOURSQUARE. Foursquare Labs, Inc. Política de Privacidade. Disponível em:

<https://pt.foursquare.com/legal/privacy>. Acesso em: 12 abr. 2021.

FOX NEWS. Privacy Policy. Disponível em: <https://www.foxnews.com/privacy-policy>. Acesso em: 12 abr. 2021.

FRANÇA. Déclaration des Droits de l'Homme et du Citoyen de 1789. Disponível em: <https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789>. Acesso em: 3 jun. 2021.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

FUSION MEDIA. Privacy Policy. Disponível em: <https://www.investing.com/about-us/privacy-policy>. Acesso em: 12 abr. 2021.

GAMA, Guilherme Calmon Nogueira da; PEREIRA, Daniel Queiroz. Direitos da personalidade e Código Civil de 2002. In: MENDES, Gilmar Ferreira; STOCO, Rui (Org.). Doutrinas essenciais: direito civil – parte geral – pessoas e domicílio. São Paulo: Revista dos Tribunais, 2011. v. 3, p. 321.

GARENA. 111dots Studio Privacy Policy. Disponível em: <http://ff.garena.com/policy.html>. Acesso em: 12 abr. 2021.

GIZ MODO. Google enfrenta processo nos EUA por rastreamento de dados em navegação anônima. Disponível em: <https://gizmodo.uol.com.br/google-processo-dados-navegacao-anonima/>. Acesso em: 12 abr. 2021.

GLOBO. Conheça canais e aplicativos que ajudam mulheres vítimas de violência doméstica. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2020/06/04/conheca-canais-e-aplicativos-que-ajudam-mulheres-vitimas-de-violencia-domestica.ghtml>. Acesso em: 5 abr. 2021.

GLOBO. Coronavírus: países europeus apostam em aplicativos de rastreamento para retornar

à normalidade. Disponível em: <https://oglobo.globo.com/mundo/coronavirus-paises-europeus-apostam-em-aplicativos-de-rastreamento-para-retornar-normalidade-24378133>. Acesso em: 8 abr. 2021.

GLOBO. Política de privacidade da Globo. Disponível em: <https://www.globo.com/privacidade.html>. Acesso em: 12 abr. 2021.

GLOBO. WhatsApp muda política de privacidade e compartilha dados com o Facebook. Disponível em: <https://www.techtudo.com.br/noticias/2021/01/whatsapp-muda-politica-de-privacidade-e-compartilha-dados-com-o-facebook.ghtml>. Acesso em: 6 abr. 2021.

GLOBO. WhatsApp terá novo alerta sobre mudanças na política de privacidade no app. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/18/whatsapp-tera-novo-alerta-sobre-mudancas-na-politica-de-privacidade-no-app.ghtml>. Acesso em: 6 abr. 2021.

GOMES, Orlando. Contratos. 25. ed. Rio de Janeiro: Forense, 2002.

GOOD JOB. Good Job Games Privacy Policy. Disponível em: <https://goodjobgames.com/policy.html>. Acesso em: 12 abr. 2021.

GOOGLE. Como funcionam os intersticiais de apps para dispositivos móveis. Disponível em: <https://support.google.com/admanager/answer/10320506?hl=pt-BR>. Acesso em: 7 abr. 2021.

GOOGLE. Exigir senha ou autenticação para compras. Disponível em: <https://support.google.com/googleplay/answer/1626831>. Acesso em: 17 mar. 2021.

GOOGLE. Google Chrome Privacy Notice. Disponível em: <https://www.google.com/intl/en/chrome/privacy/>. Acesso em: 12 abr. 2021.

GOOGLE. Plataforma Google Play. Disponível em: <https://play.google.com/store>. Acesso em: 26 mar. 2021.

GOOGLE. Privacidade & Termos. Disponível em: <https://policies.google.com/privacy>. Acesso em: 11 abr. 2021.

GREENWALD, Gleen. Sem lugar para se esconder. Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014.

HABERMAS, Jürgen. Mudança estrutural da esfera pública: investigações sobre uma categoria da sociedade burguesa. Tradução de Denilson Luís Werle. São Paulo: Editora Unesp, 2014.

HALFBRICK. Privacy Policy. Disponível em: <https://docs.halfbrick.com/PrivacyPolicy.htm>. Acesso em: 12 abr. 2021.

HARARI, Yuval Noah. Homo Deus: uma breve história do amanhã (edição eletrônica). São Paulo: Companhia das Letras, 2016.

HILBERT, Martin; LÓPEZ, Priscila. The world's technological capacity to store, communicate, and compute information. Science, v. 332, n. 6025, p. 60-65, 2011.

HUBMANN, Heinrich. Das persönlichkeitsrecht. Münster: Böhlau-Verlag, 1953 apud COSTA JR. Paulo José da. O direito de estar só: tutela penal da intimidade. 2. ed. São Paulo: RT, 1995, p. 30-36.

IAB Europe. Consumers Driving the Digital Uptake: The economic value of online advertising-based services for consumers, p.7, Sept. 2010. Disponível em: <http://www.iabeurope.eu/files/7113/7000/0832/white_paper_consumers_driving_the_-digital_uptake.pdf>. Acesso em: 5 abr. 2021.

IFOOD. Política de privacidade. Disponível em: <https://www.ifood.com.br/privacidade>. Acesso em: 12 abr. 2021.

INTO THE MINDS. Reading privacy policies of the 20 most-used mobile apps takes 6h40. Disponível em: <https://www.intotheminds.com/blog/en/reading-privacy-policies-of-the-20-most-used-mobile-apps-takes-6h40/>. Acesso em: 6 abr. 2021.

ITAÚ UNIBANCO. Privacidade – Autógrafo. Disponível em: <https://www.youtube.com/watch?v=c83z_su9Ty4&ab_channel=Ita%C3%BA>. Acesso em: 7 abr. 2021.

ITAÚ UNIBANCO. Termos de privacidade e política de privacidade. Disponível em: <https://www.itau.com.br/_arquivosestaticos/Tablet/Mobile/termosdeuso.html>. Acesso em: 12 abr. 2021.

JABUR, Gilberto Haddad. A dignidade e o rompimento de privacidade. In: MARTINS FILHO, Ives Gandra; MONTEIRO JUNIOR, Antônio Jorge (coordenadores). Direito à privacidade. São Paulo: Ideias e Letras , 2005. p. 85-106.

JOLLS, Christine; SUNSTEIN, Cass R.; THALER, Richard. A behavioral approach to law and economics. Stanford Law Review, v. 50, p. 1.477, 2004.

KAHOOT!. Privacy Policy. Disponível em: <https://kahoot.com/privacy-policy/>. Acesso em: 11 abr. 2021.

KASPERSKY LAB. Política de privacidade de produtos e serviços. Disponível em: <https://www.kaspersky.com.br/products-and-services-privacy-policy>. Acesso em: 11 abr. 2021.

KERR, Ian; BARRIGAR, Jennifer; BURKELL, Jacqelyn; BLACK, Katie. Soft surveillance, hard consent. In: KERR, Ian (Ed.). Lessons from the identity trail: anonymity, privacy and identity in a networked society. New York: Oxford University Press, 2009. p. 17: "It is well known in decision theory that subjective utility – that is, the personal value of an outcome –

changes depending on when the outcome will be experienced. In particular, the subjective value of a benefit or loss that will be experienced today is greater than the subjective value of that same benefit or loss if we know that it will be experienced some time in the future".

KHAN ACADEMY. Khan Academy Kids Privacy Policy. Disponível em: <https://www.khanacademy.org/kids/privacy-policy>. Acesso em: 11 abr. 2021.

KHAN ACADEMY. Khan Academy Privacy Policy. Disponível em: <https://www.khanacademy.org/about/privacy-policy>. Acesso em: 11 abr. 2021.

KILOO GAMES. Subway Surfers Privacy Policy. Disponível em: <http://www.kiloogames.com/pdf/subway-surfers-privacy-policy.pdf>. Acesso em: 12 abr. 2021.

KING. Privacy Policy. Disponível em: <https://king.com/privacyPolicy>. Acesso em: 12 abr. 2021.

LE FIGARO. Politique de confidentialité. Disponível em: <http://mentions-legales.lefigaro.fr/page/politique-de-confidentialite>. Acesso em: 12 abr. 2021.

LE MONDE. Politique de confidentialité. Disponível em: <https://www.lemonde.fr/confidentialite/>. Acesso em: 12 abr. 2021.

LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2011.

LESSIG, Lawrence. Code and other laws of cyberspace. New York: Basic Books, 1999, p. 160.

LIKEE. Privacy policy. Disponível em: <https://mobile.like.video/live/page-about/policy.html#common>. Acesso em: 13 abr. 2021.

LINKEDIN. Política de privacidade. Disponível em: <https://www.linkedin.com/legal/privacy-policy>. Acesso em: 12 abr. 2021.

LISBOA, Roberto Senise. Prefácio. In: MATTOS, Karla Cristina da Costa e Silva. O valor econômico da informação nas relações de consumo. São Paulo: Almedina, 2012.

LOJAS AMERICANAS. Política de Privacidade. Disponível em: <https://www.americanas.com.br/estaticapop/politica-de-privacidade-lightbox>. Acesso em: 13 abr. 2021.

LONG, Clarissa; Privacy and Pandemics In PISTOR, Katharina. Law in the time of COVID-19. Columbia Law School Books, 2020.

LORENZETTI, Ricardo L. Comércio Eletrônico. São Paulo: Editora Revista dos Tribunais. 2004.

LOVATO, Luiz Gustavo. Contratos Eletrônicos. Rio de Janeiro: Lumen Juris. 2011.

LUHMANN, Niklas. El derecho de la sociedad. Cidade do México: Editorial Herder, 2006, p. 192.

MACHADO, Joana de Moraes Souza. Caminhos para a tutela da privacidade a sociedade da informação: a proteção da pessoa em face da coleta e tratamento de dados pessoais por agentes privados no Brasil. 2014. 186 p. Tese (Doutorado) - Fundação Edson Queiroz, Universidade de Fortaleza, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito Constitucional, 2014. Disponível em: <http://uolp.unifor.br/oul/ObraSiteLivroTrazer.do?method=trazerLivro>. Acesso em: 21 mar. 2021.

MAGAZINE LUIZA. Política de Privacidade. Disponível em: <https://m.magazineluiza.com.br/s/politica-de-privacidade>. Acesso em: 13 abr. 2021.

MAPS.ME. Maps Me Privacy Policy. Disponível em: <http://legal.my.com/us/maps/privacy/>. Acesso em: 12 abr. 2021.

MARQUES, Claudia Lima; MIRAGEM, Bruno. O Novo Direito Privado e a Proteção dos Vulneráveis. São Paulo: Revista dos Tribunais, 2012, p. 117.

MARTINS, Guilherme Magalhães. Contratos Eletrônicos de Consumo. 3 ed. São Paulo: Atlas. 2016.

MARTINS-COSTA, Judith. Pessoa, personalidade, dignidade: ensaio de uma qualificação. Tese (Livre-docência) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2003. p. 107: "Por isso mesmo, a noção de direitos da personalidade é inacabada, transitiva – em uma palavra, é cultivável".

MATTIUZZO, Marcela; PONCE, Paula Pedigoni. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. Revista Internet & Sociedade, v. 1, n. 2, dez. de 2020, páginas 54 a 76. Disponível em: <https://revista.internetlab.org.br/o-legitimo-interesse-e-o-teste-da-proporcionalidade-uma-proposta-interpretativa/>.

MAURO, Roberta. A titularidade de dados pessoais prevista no art. 17 da LGPD: direito real ou pessoal? In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. Big Data: A revolution will transform how we live, work and think. New York: Houghton Mifflin Publishing, 2013.

MCAFEE. Aviso de privacidade da McAfee. Disponível em: <https://www.mcafee.com/enterprise/pt-br/about/legal/privacy.html>. Acesso em: 11 abr. 2021.

MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. I/S: A JOURNAL OF LAW AND POLICY. Vol. 4:3, pp. 543-568, 2008.

MCDONALD'S. Política de Privacidad. Disponível em: <https://api-discover-mcd.gigigoapps.com/app/terms?country=MX&language=en>. Acesso em: 12 abr. 2021.

MELLO, Celso Antônio Bandeira de. Curso de Direito Administrativo. São Paulo: Malheiros, 2000.

MENDES, Laura Schertel Ferreira. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. REVISTA DOS TRIBUNAIS (SÃO PAULO. IMPRESSO), v. 1, p. 35, 2019.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. Revista Pensar, Fortaleza, v. 25, n. 4, p. 1-18, out./dez. 2020.

MENDES, Laura Schertel. Decisão histórica do STF reconhece o direito fundamental à proteção de dados pessoais. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em 24/5/2021.

MENDES, Laura Schertel. Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; BIONI, B. R. . O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. REVISTA DE DIREITO DO CONSUMIDOR, v. 124, p. 157, 2019.

MENDES, Laura Schertel; FONSECA, G. S.. STF Reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. REVISTA DE DIREITO DO CONSUMIDOR, v. 130, p. 471, 2020.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. JOURNAL OF INSTITUTIONAL STUDIES, [S.l.], v. 6, n. 2, p. 507-533, set. 2020. Disponível em: <https://estudosinstitucionais.emnuvens.com.br/REI/article/view/521>. Acesso em: 5 abr. 2021.

MERCADO LIBRE. Políticas de privacidad y confidencialidad de la información. Disponível em: <https://www.mercadolibre.com.ar/ayuda/Politicas-de-privacidad_993>. Acesso em: 12 abr. 2021.

METRÓPOLES. A bolha do Jair: o que o presidente vê quando navega nas redes sociais. Disponível em: <https://www.metropoles.com/brasil/a-bolha-do-jair-o-que-o-presidente-ve-quando-navega-nas-redes-sociais>. Acesso em: 12 abr. 2021.

MICROSOFT. Política de Privacidade da Microsoft. Disponível em: <https://privacy.microsoft.com/pt-br/privacystatement>. Acesso em: 11 abr. 2021.

MILL, John Stuart. A liberdade. São Paulo: Martins Fontes, 2000.

MIRAGEM, Bruno. A lei geral de proteção de dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais, vol. 1009/2019, nov/2019.

MORAES, Maria Celina Bodin de. Apresentação do autor e da obra. In: RODATÀ, Stefano. A vida na sociedade da vigilância. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

MOZILLA. Aviso de privacidade do Firefox. Disponível em: <https://www.mozilla.org/pt-BR/privacy/firefox/>. Acesso em: 12 abr. 2021.

NELSON, Brett. The "Freemium" Model: top flaws and potent fixes. Disponível em: <http://www.forbes.com/sites/brettnelson/2013/07/23/the-freemium-model-top-flaws-and-potent-fixes/>. Acesso em: 5 abr. 2021.

NET E CLARO. Política de privacidade. Disponível em: <https://www.net.com.br/static/conteudo/politica-de-privacidade-now-3.pdf>. Acesso em: 12 abr. 2021.

NETFLIX. Declaração de privacidade. Disponível em: <https://help.netflix.com/legal/privacy>. Acesso em: 12 abr. 2021.

NEW YORK TIMES. Privacy policy. Disponível em: <https://help.nytimes.com/hc/en-us/articles/115014892108-Privacy-policy>. Acesso em: 12 abr. 2021.

NIANTIC. Niantic Privacy Policy. Disponível em: <https://nianticlabs.com/privacy/en/>. Acesso em: 12 abr. 2021.

NISSENBAUM, Helen. A Contextual Approach to Privacy Online. Daedalus, the Journal of the American Academy of Arts & Sciences, v. 140, n.4, pp. 32-48, Fall 2011, p. 33.

NISSENBAUM, Helen. Privacy as contextual integrity. Washington Law Review, v. 79, p. 130, 2004.

NISSENBAUM, Helen. Privacy in Context: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NOVAIS, Jorge Reis. Renúncia a direitos fundamentais. In: Miranda, Jorge (Org.). Perspectivas constitucionais: nos 20 anos da Constituição de 1976. Coimbra: Coimbra, 2006, p. 286.

NUBANK. Política de Privacidade Nubank. Disponível em: <https://nu-assets.s3.amazonaws.com/politica-privacidade.pdf>. Acesso em: 12 abr. 2021.

NUNES, Rizzatto Curso de direito do consumidor. 12. ed. São Paulo: Saraiva Educação, 2018.

OATH. Produtos de comunicação. Disponível em: <https://policies.oath.com/br/pt/oath/privacy/products/communications/index.html>. Acesso em: 12 abr. 2021.

OLHAR DIGITAL. WhatsApp é o app mais usado por brasileiros; veja ranking. Disponível em: <https://olhardigital.com.br/2020/12/21/noticias/whatsapp-e-o-app-mais-usado-por-brasileiros-veja-ranking/>. Acesso em: 7 abr. 2021.

OLX BRASIL. Política de Privacidade Nubank. Disponível em: <https://olxbrasil.zendesk.com/hc/pt-br/articles/211375589>. Acesso em: 13 abr. 2021.

ONEPEAR. Política de Privacidade Jogos Globais. Disponível em: <https://superiorzzr.tumblr.com/post/177787450452/privacy-policy9>. Acesso em: 12 abr. 2021.

OPSAHL, Kurt. Facebook's Eroding Privacy Policy: a timeline. Disponível em: <https://www.eff.org/deeplinks/2010/04/facebook-timeline>. Acesso em: 6 abr. 2021.

OUTFIT7. Política de privacidade para aplicativos. Disponível em: <https://outfit7.com/privacy/pt/>. Acesso em: 12 abr. 2021.

PALCO MP3. Termos de privacidade e política de privacidade. Disponível em: <https://www.palcomp3.com/aviso_legal.htm>. Acesso em: 12 abr. 2021.

PARLAMENTO EUROPEU. Regulamento Geral sobre a Proteção de Dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt>. Acesso em: 25 mar. 2021.

PASQUALE, Frank. The black box society. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PAYPAL. Declaração de Privacidade. Disponível em: <https://www.paypal.com/webapps/mpp/ua/privacy-full>. Acesso em: 12 abr. 2021.

PEREIRA, Caio Mário Silva. Instituições de Direito Civil: Contratos. 20 ed. Rio de Janeiro: Forense, 2016. v.3.

PESSOA. João Pedro Seefeldt. O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI. -- Porto Alegre, RS: Editora Fi, 2020.

PICPAY. Privacidade. Disponível em: <https://picpay.com/site/privacidade>. Acesso em: 13 abr. 2021.

PINHEIRO, Patrícia Peck. Contratos digitais: apenas um meio ou nova modalidade contratual? Disponível em: <https://www.conjur.com.br/2016-jul-29/patricia-peck-contratos-digitais-sao-modalidade-contratual>. Acesso em: 23 mar. 2021.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais – comentários à Lei n. 13.709/2018. São Paulo: Saraiva, 2018.

PINTEREST. Política de privacidade. Disponível em: <https://policy.pinterest.com/pt-

br/privacy-policy>. Acesso em: 12 abr. 2021.

PODER 360. Conheça os aplicativos de rastreamento da covid-19 usados pelos países. Disponível em: <https://www.poder360.com.br/coronavirus/conheca-os-aplicativos-de-rastreamento-da-covid-19-usados-pelos-paises/>. Acesso em: 8 abr. 2021.

POLARIS OFFICE. Privacy & Terms. Disponível em: <https://www.polarisoffice.com/en/privacy>. Acesso em: 11 abr. 2021.

PRISA. Política de cookies. Disponível em: <https://www.prisa.com/es/info/politica-de-cookies>. Acesso em: 12 abr. 2021.

R7. Empresas mais ricas do mundo – Top 10 do Ranking mundial de 2021. Disponível em: <https://segredosdomundo.r7.com/empresas-mais-ricas-do-mundo/>. Acesso em: 5 abr. 2021.

RAMOS, André de Carvalho. O pequeno irmão que nos observa: os direitos dos consumidores e os bancos de dados no Brasil. In: MARQUES, Cláudia Lima; MIRAGEM, Bruno (Org.). Coleção doutrinas essenciais: direito do consumidor – proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, 2011. v.3, p.957-974.

RAPPI. Aviso de Privacidade e Políticas de uso das Informação utilizadas pela Rappi. Disponível em: <https://legal.rappi.com/brazil/aviso-de-privacidade-e-politicas-de-uso-das-informacao-utilizadas-pela-rappi/?_ga=2.167336379.427143798.1555076488-278939625.1555076488&_gac=1.195807640.1555076488.EAIaIQobChMI5Ib7qNfK4QIVEoSRCh3KDAUUEAAYASAAEgKlevD_BwE>. Acesso em: 12 abr. 2021.

REALE, Miguel. Teoria Tridimensional do Direito - situação atual. São Paulo: Saraiva, 1994, 5.ª ed.

REINO UNIDO. Information Comissioner's Office. Lawful basis for processing. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/>. Acesso em: 3 jun. 2021.

REINO UNIDO. Informational Commissioner's Office. Global survey finds 85% of mobile apps fail to provide basic privacy information. Disponível em: <https://www.wired-gov.net/wg/news.nsf/articles/Global+survey+finds+85+of+mobile+apps+fail+to+provide+basic+privacy+information+10092014151000?open>.

RESULTADOS DIGITAIS. Ranking das redes sociais 2020: as mais usadas no Brasil e no mundo. Disponível em: <https://resultadosdigitais.com.br/blog/redes-sociais-mais-usadas-no-brasil/>. Acesso em: 5 abr. 2021.

RICHARDS, Neil; HARTZOG, Woodrow. Taking Trust Seriously in Privacy Law. Stanford Technology Law Review, vol. 19, p. 431-472, 2016.

RIZZARDO, Arnaldo. Contratos. 16. ed. Rio de Janeiro: Forense, 2017.

ROCKSTAR GAMES. Política de Privacidade. Disponível em: <https://www.rockstargames.com/privacy?locale=br>. Acesso em: 12 abr. 2021.

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Elaboratori elettronici e controllo sociale. Bologna: Il Mulino, 1973, p. 14.

ROSENVALD, Nelson; NETTO, Felipe Braga; FARIAS, Cristiano Chaves de. Manual de Direito Civil – Volume único. 4. Ed. rev, ampl. e atual. – Salvador: Ed. JusPodivm, 2019, p. 239.

ROVIO. Rovio Privacy Notice. Disponível em: <https://www.rovio.com/privacy>. Acesso em: 12 abr. 2021.

RULE, James; HUNTER, Lawrence. Towards a property right in personal data. In: Visions of privacy: Policy choices for the digital age. Colin Bennett. Toronto: University of Toronto Press, 1999, pp. 165-181. L

SALTZER, Jerome H. Protection and the Control of Information Sharing in Multics. Commun. ACM, 17(7), 388–402, 1974. Disponível em: https://doi.org/10.1145/361011.361067.

SANTANDER ESP. Condiciones Generales de Uso. Disponível em: <https://www.bancosantander.es/es/aviso-legal>. Acesso em: 12 abr. 2021.

SANTANDER UK. Legal information. Disponível em: <https://www.santander.co.uk/personal/support/customer-support/legal-information>. Acesso em: 12 abr. 2021.

SANTANDER. Políticas de Privacidade. Disponível em: <https://www.santander.com.br/institucional-santander/seguranca/politica-de-privacidade>. Acesso em: 12 abr. 2021.

SANTANNA, Héctor Valverde; RAMOS, Anna Luíza Salles. A efetividade do direito à informação adequada em relação aos termos de uso e serviço e políticas de privacidade. In: Revista de Direito do Consumidor, v. 134, 2021.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz. Tratado de proteção de dados pessoais. São Paulo: Forense: 2021.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilhere; MITIDIERO, Daniel. Curso de direito constitucional. 2. Ed. São Paulo: Editora Revista dos Tribunais, 2013, p. 403.

SARTORI, Ellen Carina Mattias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet. Revista de Direito Civil Contemporâneo, São Paulo,

v. 9, ano 3, p. 49-104, out.-dez. 2016.

SBT. Política de privacidade. Disponível em: <https://www.sbt.com.br/politica-de-privacidade>. Acesso em: 12 abr. 2021.

SCHERTEL MENDES, Laura; MATTIUZZO, Marcela. DISCRIMINAÇÃO ALGORÍTMICA: CONCEITO, FUNDAMENTO LEGAL E TIPOLOGIA. Direito Público, [S.l.], v. 16, n. 90, dez. 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3766>. Acesso em: 5 abr. 2021.

SCHERTEL, Laura; RODRIGUES JÚNIOR, Otávio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otávio Luiz. Tratado de proteção de dados pessoais. São Paulo: Forense: 2021.

SCHREIBER, Anderson. Direitos da personalidade. 2. ed. São Paulo: Atlas , 2013.

SCHWARTZ, Paul. Property, Privacy and Personal Data. Harvard Law Review, v. 117, n. 7, 2004, p. 2056.

SERASA CONSUMIDOR. Políticas do site. Disponível em: <https://www.serasaconsumidor.com.br/politicas-do-site>. Acesso em: 11 abr. 2021.

SHARE IT. Privacy Policy. Disponível em: <http://cdn.ushareit.com/shareit/w/privacy/pr_en/index.html>. Acesso em: 11 abr. 2021.

SHOPEE. Política de privacidade. Disponível em: <https://shopee.ph/legaldoc/privacy>. Acesso em: 13 abr. 2021.

SIGNAL. Signal Terms & Privacy Policy. Disponível em: <https://signal.org/legal/#terms-of-service>. Acesso em 13 abr. 2021.

SKYSCANNER. Privacy Policy. Disponível em: <https://www.skyscanner.net/media/privacy-policy>. Acesso em: 12 abr. 2021.

SNAP. Política de privacidade. Disponível em: <https://www.snap.com/pt-BR/privacy/privacy-policy/>. Acesso em: 12 abr. 2021.

SOLOVE, Daniel J. Nothing to hide: The false tradeoff between privacy and security. Yale University Press, 2011, p. 61.

SOLOVE, Daniel J. The Myth of the Privacy Paradox. GWU Legal Studies Research Paper no. 2020-10, 2020. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265> Acesso em: 4 jun. 2021.

SOLOVE, Daniel J.; HARTZOG, Woodrow. The FTC and the New Common Law of Privacy

114, Columbia Law Review 583 (2014), GWU Legal Studies Research Paper No. 2013-120: "Another of the most prominent FIPPs is the individual's right to consent to the collection and use of her personal data. These two FIPPs became the backbone of the U.S. self-regulatory approach, with privacy policies seeking to satisfy the right to notice, and with user choice seeking to satisfy the right to consent"

SOLOVE, Daniel. Understanding privacy. Cambridge: Harvard University Press, 2008. E-book, pos. 327/3424.

SOUZA, Carlos Affonso Pereira de. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

SPOTIFY. Política de Privacidade do Spotify. Disponível em: <https://www.spotify.com/br/legal/privacy-policy/>. Acesso em: 12 abr. 2021.

STATCOUNTER. Mobile Operating System Market Share Brazil. Disponível em: <https://gs.statcounter.com/os-market-share/mobile/brazil>. Acesso em: 26 mar. 2021.

STRANDBURG, Katherine J. Free Fall: The Online Market's Consumer Preference Disconnect. NYU School of Law, Public Law Research Paper n.13-62, p.96, Oct. 2013. Disponível em: <http://ssrn.com/abstract=232396>. Acesso em: 5 abr. 2021.

SUPER INTERESSANTE. Não li e concordo. Disponível em: <https://super.abril.com.br/tecnologia/nao-li-e-concordo/>. Acesso em: 13 abr. 2021.

TARODO, Salvador Tarodo. La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano. En: Derecho y Salud, Pamplona, v. 14, n. 1, pp. 127-147, ene-jun. 2006, p. 136. Tradução livre.

TARTUCE, Flávio. Direito civil, v. 3: teoria geral dos contratos e contratos em espécie. 13. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.

TARTUCE, Flávio. Manual de direito do consumidor: direito material e processual. 7. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2018.

TECHTUDO. 9 em cada 10 brasileiros usam celular Android, diz relatório do Google. Disponível em: <https://www.techtudo.com.br/noticias/2020/09/9-em-cada-10-brasileiros-usam-celular-android-diz-relatorio-do-google.ghtml>. Acesso em: 26 mar. 2021.

TECHTUDO. Sete riscos de baixar extensões no navegador do PC. Disponível em: <https://www.techtudo.com.br/listas/2020/07/sete-riscos-de-baixar-extensoes-no-navegador-do-pc.ghtml>. Acesso em: 12 abr. 2021.

TED. Privacy Policy. Disponível em: <https://www.ted.com/about/our-organization/our-

policies-terms/privacy-policy>. Acesso em: 11 abr. 2021.

TELE SÍNTESE. “Interesse legítimo” supera “consentimento” no tratamento de dados pessoais pelas empresas. Disponível em: <https://www.telesintese.com.br/interesse-legitimo-supera-consentimento-no-tratamento-de-dados-pelas-empresas/>. Acesso em: 26 mar. 2021.

TELEGRAM. Telegram Privacy Policy. Disponível em: <https://telegram.org/privacy>. Acesso em: 12 abr. 2021.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

THE ECONOMIST. The world’s most valuable resource is no longer oil, but data. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 26 mar. 2021.

THE GUARDIAN. Cookie policy. Disponível em: <https://www.theguardian.com/info/cookies>. Acesso em: 12 abr. 2021.

THE GUARDIAN. Former Cambridge Analytica exec says she wants lies to stop. Disponível em: <https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies>. Acesso em: 26 mar. 2021.

THE GUARDIAN. Privacy policy. Disponível em: <https://www.theguardian.com/help/privacy-policy>. Acesso em: 12 abr. 2021.

TIKTOK. Privacy Policy. Disponível em: <https://www.tiktok.com/en/privacy-policy>. Acesso em: 12 abr. 2021.

TINDER. Privacy. Disponível em: <https://www.gotinder.com/privacy>. Acesso em: 12 abr. 2021.

TRIPADVISOR. Privacy Policy. Disponível em: <https://tripadvisor.mediaroom.com/us-privacy-policy>. Acesso em: 12 abr. 2021.

TRIVAGO. Trivago's privacy policy. Disponível em: <https://www.trivago.com/privacy-policy>. Acesso em: 12 abr. 2021.

TUDO CELULAR. WhatsApp recua frente aos protestos e adia mudança na política de privacidade. Disponível em: <https://www.tudocelular.com/seguranca/noticias/n169019/ministerio-justica-whatsapp-termo-privacidade.html>. Acesso em: 6 abr. 2021.

TUDO GOSTOSO. Terms. Disponível em: <https://www.tudogostoso.com.br/mobile/pages/terms.html>. Acesso em: 12 abr. 2021.

TUMBLR. Política de privacidade. Disponível em: <https://www.tumblr.com/privacy/pt>. Acesso em: 12 abr. 2021.

TWITCH. Aviso de privacidade. Disponível em: <https://www.twitch.tv/p/pt-br/legal/privacy-notice/>. Acesso em: 13 abr. 2021.

TWITTER. Política de Privacidade Twitter. Disponível em: <https://twitter.com/pt/privacy>. Acesso em: 26 mar. 2021.

UBER. Cookie policy global. Disponível em: <https://www.uber.com/legal/privacy/cookies/en/>. Acesso em: 12 abr. 2021.

UBER. Política de Privacidade. Disponível em: <https://privacy.uber.com/policy/>. Acesso em: 12 abr. 2021.

UC BROWSER. Privacy policy. Disponível em: <http://www.ucweb.com/company/privacy/>. Acesso em: 12 abr. 2021.

UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Grande Secção), 13 de maio de 2014. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131>. Acesso em: 5 abr. 2021.

UNICEF. Declaração Universal dos Direitos Humanos. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 5 abr. 2021.

UNITED NATIONS COMISSION ON INTERNATIONAL TRADE LAW. Model Law on Electronic Commerce with Guide to Enactment 1996. New York: United Nations. 1999. Disponível em: <http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf>. Acesso em: 24 mar. 2021.

UOL. Ataque hacker no STJ: peritos temem vazamento em massa de dados copiados. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/11/09/ataque-no-stj-hacker-continua-com-o-controle-de-documentos-sigilosos.htm>. Acesso em: 26 mar. 2021.

UOL. Como descobrir o que o Facebook sabe sobre você. São Paulo, 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/bbc/2018/03/27/como-descobrir-o-que-o-facebook-sabe-sobre-voce.htm?cmpid=copiaecola>. Acesso em: 16 abr. 2021. Veja-se que essa ferramenta não é recente, mas certamente não era de conhecimento dos usuários: BBC Brasil. Como descobrir o que o Facebook sabe sobre você. São Paulo, 2018. Disponível em: <http://www.bbc.com/portuguese/noticias/2015/11/151014_facebook_salasocial_informacoes_cc>. Acesso em: 16 abr. 2021.

UOL. Criança gasta mais de R$30 mil com jogos no celular durante pandemia sem o pai saber. Disponível em: <https://paisefilhos.uol.com.br/familia/crianca-gasta-mais-de-r30-mil-com-

jogos-no-celular-durante-pandemia-sem-o-pai-saber/>. Acesso em: 7 abr. 2021.

UOL. Normas de segurança e privacidade. Disponível em: <https://sobreuol.noticias.uol.com.br/normas-de-seguranca-e-privacidade.html>. Acesso em: 12 abr. 2021.

UOL. Privacidade gera guerrinha de indiretas entre Apple, Facebook e Google. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/05/30/por-que-apple-facebook-e-google-estao-fazendo-barraco-por-privacidade.htm>. Acesso em: 26 mar. 2021.

US NEWS. The Illusion of Online Privacy. Disponível em: <https://www.usnews.com/news/articles/2015/08/25/the-illusion-of-online-privacy>. Acesso em: 26 mar. 2021.

USTARAN, E. (Org.). (2018). European data protection: Law and practice. an IAPP Publication, International Association of Privacy Professionals.

VARELLA, Marcelo Dias; XAVIER, Izabella Ribeiro; ROCHA, Antônio Glauter Teófilo da; PINTO, Marcos Cesar de Oliveira. Rastreamento de contatos como ferramenta de combate à transmissão do SARS-CoV-2: benchmark internacional, soluções tecnológicas e considerações éticas. Revista do Programa de Pós-Graduação em Direito da UFC. v. 40 n. 1 (2020): jan/jun 2020, pp. 99-122, p. 118.

VEJA. MP investiga se farmácias repassam dados de clientes a planos de saúde. Disponível em: <https://veja.abril.com.br/economia/mp-investiga-se-farmacias-repassam-dados-de-clientes-a-planos-de-saude/>. Acesso em: 26 mar. 2021.

VIBER. Viber Privacy Policy. Disponível em: <https://www.viber.com/terms/viber-privacy-policy/>. Acesso em: 12 abr. 2021.

VIEIRA, Tatiana Malta. O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 p. Dissertação (Mestrado) - Universidade de Brasília, Faculdade de Direito, Programa de Pós-Graduação em Direito, Estado e Sociedade, 2007. Disponível em: <http://repositorio.unb.br/bitstream/10482/3358/1/2007_TatianaMaltaVieira.pdf>. Acesso em: 21 mar. 2021.

VIGO. Vigo Política de privacidade. Disponível em: <http://www.vigovideo.net/hotsoon/in_app/privacy_policy/>. Acesso em: 12 abr. 2021.

WARREN, Samuel D.; BRANDEIS, Louis, D. Right to privacy. Harvard Law Review, v. IV, n. 5, December, 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>. Acesso em: 21 mar. 2021.

WAZE. Waze Privacy Policy. Disponível em: <https://www.waze.com/pt-BR/legal/privacy>.

Acesso em: 12 abr. 2021.

WEBER, Rof H. Internet of Things – New security and privacy challenges, p.23.

WECHAT. WeChat Privacy Protection Summary. Disponível em: <https://www.wechat.com/mobile/htdocs/en/privacy_policy.html>. Acesso em: 12 abr. 2021.

WHATSAPP. WhatsApp Privacy Policy. Disponível em: <https://www.whatsapp.com/legal?eea=1#privacy-policy>. Acesso em: 26 mar. 2021.

WISH. Privacy Policy. Disponível em: <https://www.wish.com/en-privacy-policy>. Acesso em: 12 abr. 2021.

WPS OFFICE. Privacy Policy. Disponível em: <https://wps.com/privacy-policy/?lang=ptbr>. Acesso em: 11 abr. 2021.

YAHOO FINANÇAS. Políticas de privacidade: aceitar sem ler é hábito comum entre os internautas. Disponível em: <https://br.financas.yahoo.com/noticias/pol%C3%ADticas-privacidade-aceitar-sem-ler-121900683.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMjCWlBlCge6yfMCtSRxC35HGpfh0cIdF4TZXCu1lw-LQXzcYMuZobDwPbgJPjkY7t5uThYjHVp-hxgJkb3C1a4wdzhVbjZFQ13_8-LL5sB7mb6oNy2-PqLcdNbTG31QYilkVSbg60b6F5YTPACln2Tr26wvXtW_JQjNF6tmdxkz>. Acesso em: 6 abr. 2021.

ZAKEH. Privacy Policy. Disponível em: <http://help.pou.me/privacy-policy.php>. Acesso em: 12 abr. 2021.

ZANINI, Leonardo Estevam de Assis. Contratação na sociedade massificada. Revista Brasileira de Direito Civil – RBDCivil | Belo Horizonte, vol. 14, p. 75-98, out./dez. 2017, p. 76.

ZÉ DELIVERY. Política de Privacidade. Disponível em: <https://www.ze.delivery/privacy>. Acesso em: 13 abr. 2021.

ZINGALES, Luigi. Digital platforms and concentration. In: STIGLER CENTER. 2018 antitrust and competition conference. Disponível em: <www.youtube.com/watch?v=O_pxLvKQBE8>. Acesso em: 4 jun. 2021.

ZOOM. Zoom Privacy Statement. Disponível em: <https://explore.zoom.us/trust/privacy>. Acesso em: 13 abr. 2021.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the propects of an information civilization. Journal of Information Technology, 30, 2015, p. 75-89, p. 80-81.

APÊNDICE A

1. Comunicação e redes sociais

Em sua página inicial, o *Pinterest* informa que, ao continuar, o usuário concorda com os termos de serviço e a política de privacidade do aplicativo, sendo os dois documentos escritos em português. Para continuar, é preciso fazer um cadastro, com o *Facebook*, o *Google* ou algum e-mail simples. Feito isso, no menu de configurações, também é possível acessar os documentos e, supostamente, ver a política de anúncios personalizados – a qual, contudo, remete a uma página vazia, com erro 404.

É possível revogar algumas opções pré-marcadas de consentimento, sobretudo no que diz respeito à personalização dos resultados de pesquisa e ao uso de informações por parceiros anunciantes, ou seja, exatamente o escopo da publicidade comportamental.

Ao iniciar, o *LinkedIn* também exibe, logo em sua página de cadastro, o contrato do usuário, a política de privacidade e um documento específico para a sua política de *cookies*, todos escritos em português. Em seu menu específico de configurações, o aplicativo também permite o acesso aos documentos e um amplo espectro de revogações, sobretudo no que diz respeito à exibição de anúncios de vagas personalizados de acordo com sites visitados, conexões, categorias de interesse, etc.

Após o *login*, mas ainda em sua página inicial, o *Messenger* pede solicitação expressa de acesso aos contatos do celular, sob a alegação de que "o carregamento contínuo dos seus contatos ajuda o *Facebook* e o *Messenger* a sugerir conexões e fornecer e melhorar os anúncios para você e outras pessoas, além de melhorar o serviço fornecido". É possível recusar.

Na tela seguinte, o aplicativo solicita que se "adicione um número de telefone à sua conta", sob a justificativa de que "ajuda a redefinir sua senha facilmente, encontrar amigos, ver anúncios relevantes, receber notificações por SMS e muito mais". Também é possível recusar.

No menu de configurações, também é possível fazer uma ampla revogação do consentimento previamente definido sobre publicidade comportamental dirigida. Além disso, também é possível fazer o *download* de um arquivo compilado com todas as informações que a rede social tem sobre o usuário. Isso parece aderente à tutela da privacidade que se entende como adequada.

Em sua página inicial, o *Telegram* solicita permissão para o recebimento de chamadas, sob a justificativa de poder confirmar o número do telefone do usuário automaticamente, mas é possível recusar. Na página seguinte, o aplicativo exibe os seus enxutos

"Termos de Serviço", que se resumem a orientar o usuário a não cometer golpes, promover violência ou exibir conteúdo pornográfico na rede. O documento é incipiente.

Na tela seguinte, o aplicativo pede acesso aos contatos do usuário, "para que possa se comunicar com seus amigos através de todos os seus dispositivos". Para dar pretensa segurança ao usuário, o aplicativo informa que "seus contatos serão continuamente sincronizados na nuvem fortemente criptografada no *Telegram*". Também é possível recusar. No menu de configurações, é possível encontrar a política de privacidade, inteiramente escrita em inglês. Contudo, à exceção de meras configurações das próprias funcionalidades do aplicativo, não é possível fazer qualquer revogação de consentimento no tocante à privacidade do usuário.

Em sua primeira tela, o *WeChat* pede acesso às fotos, mídia e arquivos do dispositivo e ao fazimento e gerenciamento de chamadas telefônicas, não sendo possível recusar nenhuma das solicitações. Na página de cadastro, há a indicação de que, ao continuar, o usuário concorda com os termos de serviço e a política de privacidade, documentos escritos em inglês e português, respectivamente.

Na página seguinte, aparece uma aba específica em que o usuário precisa rolar a página e dar o *check* em "eu li e aceito as condições da política de privacidade acima", o que o torna diferente dos demais aplicativos avaliados, que sequer isso fazem. Na sequência, o *WeChat* informa que "carregará seu livro de endereço de seu servidor para ajudar a descobrir quais contatos móveis estão usando *WeChat*".

Para incentivar o usuário, informa que "seus dados enviados são usados apenas para correspondência de contatos e não serão salvos para outros fins". Apesar de pouco intuitivo, é possível recusar essa solicitação. Dentro do menu de configurações, é possível encontrar a política de privacidade, inteiramente escrita em português. Contudo, à semelhança do *Telegram* e à exceção de meras configurações das próprias funcionalidades do aplicativo, não é possível fazer qualquer revogação de consentimento no tocante à privacidade do usuário.

Em sua tela inicial, o *Snapchat* solicita a habilitação de permissões do aplicativo para facilitar a criação de contas, dentre as quais a de acesso aos contatos e a de fazimento e gerenciamento de chamadas telefônicas, mas é possível recusá-las. Na página seguinte, é exibida a mensagem de que, ao continuar, o usuário concorda com os termos de serviço e a política de privacidade, ambos escritos em português.

Após o rápido cadastro, aparece uma mensagem de que "seus contatos serão enviados aos servidores do *Snapchat* para que você e outros possam encontrar amigos, e para melhorar a sua experiência". Embora pouco intuitivo, é possível recusar a solicitação. Na página

seguinte, o aplicativo solicita acesso à câmera e à gravação de vídeos e às fotos, mídias e arquivos do dispositivo, não sendo possível recusar.

No menu de configurações, embora possível o acesso a todos os termos de privacidade, não é possível fazer qualquer revogação adicional de consentimento – até mesmo porque as permissões originais não foram concedidas.

Na página inicial do *Tumblr*, há a indicação de que, ao continuar, o usuário concorda com os termos de serviço e a política de privacidade, documentos escritos em inglês e português, respectivamente. Após o breve cadastro, é possível acessar um painel de privacidade no menu de configurações, no qual se pode revogar a permissão para o envio de anúncios e conteúdos personalizados. Além de tudo, é possível solicitar o *download* de um arquivo organizado sobre todos os dados que o aplicativo dispõe sobre o usuário, o que está alinhado ao direito de acesso da LGPD.

Ao iniciar, o *Viber* exibe seus termos de serviço, escritos parcialmente em português. Há a tradicional mensagem sobre armazenamento de cookies ("ao continuar navegando, você concorda com o armazenamento de cookies de primeira e terceira partes em seu navegador para melhorar a navegação no site, analisar o uso do site e ajudar nosso marketing") e, na página seguinte, o aplicativo solicita acesso aos contatos e permissão para o fazimento e gerenciamento de chamadas telefônicas, o que, nesse momento, é possível recusar.

Após, há nova solicitação de acesso aos contatos, às fotos, mídia e arquivos, à câmera e aos recursos de gravação de vídeos e áudios e à localização do dispositivo. Em tese, também é possível negar todos os pedidos. No menu específico de configurações, cinco informações e opções são disponíveis:

(i) o *Viber* informa coletar dados analíticos de atividades para melhorar o produto e desempenho, não sendo os dados usados para outros fins. De toda forma, é possível retirar o consentimento para essa coleta;

(ii) o aplicativo informa permitir conteúdo personalizado a ser exibido na plataforma, baseado nos interesses do usuário e para aprimorar a sua experiência. Também é possível retirar o consentimento para isso;

(iii) o *Viber* também informa que fornece dados de localização precisa para parceiros confiáveis que oferecerão serviços com base nessas informações. Mais uma vez, a revogação é possível;

(iv) o usuário também pode solicitar uma cópia de seus dados pessoais armazenados pela plataforma; e

(v) pode-se solicitar a exclusão dos dados pessoais armazenados. O leque é amplo, razão por que o aplicativo parece aderente à tutela da privacidade que se entende como adequada.

Ao abrir o *Skype*, são exibidos ao usuário os termos de privacidade e a política de privacidade, ambos escritos em português. Contudo, os termos são genéricos para todos os produtos da *Microsoft*, e não especificamente destinados ao aplicativo em si. Na página seguinte, o aplicativo informa que, para ajudar o usuário a encontrar amigos, "sincronizará e armazenará periodicamente os contatos".

Aparentemente, é possível recusar. Na página seguinte, o aplicativo pede acesso à câmera e ao microfone, o que também é possível recusar. Nesse ponto, dada a funcionalidade principal da ferramenta, as permissões até fazem sentido. Embora seja possível acessar as políticas de privacidade no menu específico de configurações, não é possível fazer revogações adicionais de consentimento, mesmo que o aplicativo indique promover anúncios em sua plataforma – o que, colocado em escala, pode ser desalinhado com a lógica da LGPD.

Ao abrir, *Twitter* exibe seus termos de serviço, políticas de privacidade e termos específicos sobre o uso de *cookies*, todos escritos em português. Desde a primeira tela do aplicativo, já é possível fazer algumas revogações pontuais de consentimento: evitar que outros usuários encontrem pelo e-mail ou número de celular, por exemplo.

No menu de configurações, também há um amplo espectro de revogações possíveis de consentimento, sobretudo relacionadas às permissões porventura concedidas e à publicidade comportamental especificamente dirigida ao usuário.

Ao iniciar o processo de cadastro no *Instagram*, o aplicativo solicita acesso aos contatos – sob o pretexto de facilitar eventual recuperação de conta, o que não parece justificável –, mas é possível recusar. No pouco transparente rodapé da página seguinte, há a tradicional disposição de que, "ao continuar, você concorda com nossos termos, política de dados e política de cookies", sendo todos os documentos escritos em português. Feito isso, ao se clicar na opção de "postar uma foto", o aplicativo solicita expresso acesso à câmera (tirar fotos e gravar vídeos), à localização do dispositivo, à gravação de áudio e ao acesso a fotos, mídia e arquivos do dispositivo.

Pelas funcionalidades conhecidas do *software*, todas as permissões parecem fazer sentido e é até aderente à tutela da privacidade que se entende como adequada que só sejam solicitadas nesse momento específico em que serão realmente úteis. A que deixa mais dúvidas é aquela relativa ao acesso à localização. No menu de configurações, embora seja possível fazer algumas revogações de funcionalidades específicas e mais intromissivas do aplicativo, não é

viável revogar o consentimento de nenhuma permissão mais sensível à tutela da privacidade e dos dados pessoais do usuário.

Ao abrir o *Facebook* em sua opção de criação de conta, o aplicativo, de plano, requer autorização para fazer e gerenciar chamadas telefônicas e acessar os contatos, mas é possível negar. Após a inserção de alguns dados, o usuário precisa concordar com os termos de privacidade, a política de dados e a política de *cookies* do *software*, todos escritos em português.

Na mesma página, novamente é solicitado o acesso aos contatos do usuário, para que o aplicativo possa "sugerir amizades e fornecer e melhorar os anúncios para você e outras pessoas". É possível, contudo, manter a recusa. Já na tela inicial de funcionamento do aplicativo, ele solicita acesso à localização do dispositivo, o que não parece pertinente com as funcionalidades básicas do aplicativo.

Ora, se o usuário quiser postar uma foto com a legenda fazendo referência ao seu lugar, que a permissão seja especificamente solicitada para aquele ato, e não de modo geral. É possível recusar o pedido. No menu de configurações, é possível fazer algumas revogações pontuais de consentimento, sobretudo no que tange aos anúncios patrocinados. Contudo, as opções não são tão intuitivas quanto as do *Twitter* e do *Viber*.

Já na interface de uso do *WhatsApp*, é possível acessar os termos de privacidade e a política de privacidade no menu específico de configurações, estando ambos escritos em português.

Não é possível, no entanto, fazer nenhuma revogação de ponto diretamente afeto à privacidade do usuário, mas apenas edições de funcionalidades do próprio aplicativo, que podem tutelar, em maior ou menor escala, a privacidade, mas sempre de modo indireto.

O *Zoom*, ao iniciar, exibe sua política de privacidade em menu apartado de configurações, escrita em português e com aparente organização para facilitar a compreensão do usuário, embora longa. Depois de efetuado o registro, que pode ser com as contas do *Gmail* ou do *Facebook*, e já no modo de operação do aplicativo, não é possível fazer nenhuma revogação de consentimento, salvo alguns ajustes de funcionalidades próprias do aplicativo que, indiretamente, podem aumentar o padrão da proteção dos dados, à semelhança do que ocorre no *WhatsApp*.

O *Google Meet*, em sua primeira página após fazer o *login* com o *Gmail* – que é um pré-requisito para o funcionamento do *Android* –, afirma "Conheça o *Meet*", logo abaixo do que aparecem os termos de serviço e a política de privacidade, que são genéricos para todos os serviços da empresa. Nesse ponto, porém, relevante apontar que a política de privacidade é

acompanhada de pequenos vídeos explicativos de algumas questões pontuais afetas à proteção dos dados, mas que são em inglês.

Ao continuar, o *Meet* pede acesso ao gravador e à câmera do aparelho – o que é compatível com as finalidades do aplicativo –, mas é possível recusar. Já no menu após a inicialização, não é possível fazer qualquer revogação senão referente ao envio de informações para diagnóstico do funcionamento da plataforma.

Por fim, o *Signal*, em sua página inicial, afirma: "Leve sua privacidade com você. Seja você em cada mensagem", o que passa uma mensagem positiva para o usuário mais preocupado com sua privacidade. Nessa página, há também menção à política de privacidade e aos termos de uso, ambos escritos, contudo, em inglês. Ao continuar, o aplicativo pede acesso aos contatos, "para te conectar com seus amigos, trocar as mensagens e fazer ligações seguras", mas é possível recusar. Dentro do menu, não é possível revogar qualquer permissão senão aquelas referentes à funcionalização do próprio aplicativo, à semelhança do *WhatsApp*.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos dezessete aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

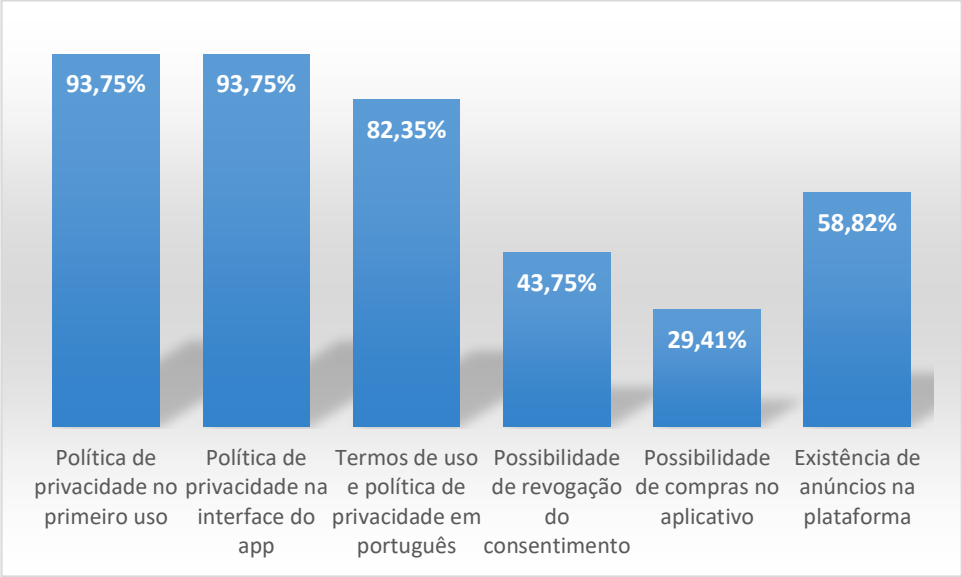

Figura 7 – Estatísticas análise consentimento na categoria "*Comunicação e redes sociais*"

2. Navegadores e e-mails

Ao abrir o *Yahoo*, o usuário é direcionado para uma página de cadastro que contém a política de privacidade e os termos de privacidade, ambos em português. Como o correto

funcionamento do aplicativo pressupõe a existência de conta na empresa, não foi possível fazer a análise detalhada da interface da aplicação, razão por que ela foi descontada para fins do fazimento do gráfico comparativo.

O *Outlook* também exibe, em sua página inicial, política de privacidade e os termos de privacidade, ambos em português. Também é possível consultar os termos na interface do próprio aplicativo, mas nenhuma revogação de consentimento inicial é viável.

Quanto ao *Gmail*, é possível acessar os termos de privacidade e as políticas de privacidade na interface da aplicação, havendo um amplo espectro de possibilidade de revogações de permissões, na medida em que o gerenciamento do *Gmail* acaba significando o gerenciamento de todas as contas *Google* do usuário – que, por pressuposto para o funcionamento do sistema operacional *Android*, deve existir.

Ao acessar o *MS Edge*, o usuário se depara com a recomendação de se fazer o *login* por alguma conta de e-mail, para que haja o aproveitamento do histórico de navegação em vários dispositivos. Nessa página, há a política de privacidade da *Microsoft*, que – assim como a do *Outlook* – é geral para quase todos os produtos da empresa, sem detalhamentos específicos de cada aplicativo.

Na página de configurações do navegador, é possível acessar novamente os termos de privacidade e fazer revogações de consentimento, inclusive do armazenamento de *cookies* por sites de terceiros e pelo próprio aplicativo. Nesse sentido, há aderência à tutela da privacidade que se entende como adequada.

O *Mozilla Firefox* tem comportamento muito semelhante ao do *Edge*. Do mesmo modo o *Google Chrome*, que, contudo, não pôde ser aferido em sua tela inicial, pelos mesmos motivos do *Gmail*.

Na tela inicial, o *UC Browser* é semelhante aos dois navegadores retro, exibindo termos e uso e política de privacidade logo ao iniciar, ambos em português. Na tela seguinte, solicita permissão de fazimento e gerenciamento de chamadas telefônicas, com o suposto intuito de "aumentar a velocidade de navegação".

Não parece haver muita pertinência lógica – apesar de se buscar a transparência –, mas é possível recusar o pedido. Também é possível fazer algumas revogações de consentimento, dentre as quais a de exibição de anúncios personalizados. Não parece haver, contudo, um modo de impedir os *cookies* de serem armazenados, ou seja, parece que a preocupação é apenas com o final da cadeia, instalando uma espécie de filtro contra a exibição de publicidade comportamental. Ainda assim, as possibilidades de revogações são amplas.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos sete aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

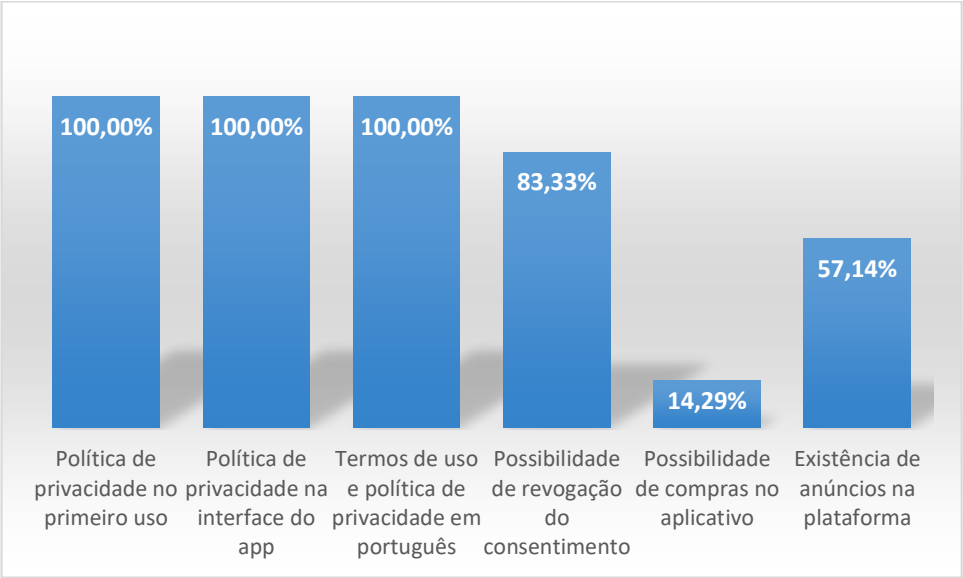

Figura 8 – Estatísticas análise consentimento na categoria "*Navegadores e e-mails*"

3. Entretenimento, vídeos e músicas

O *Deezzer*, logo em sua tela inicial, exibe as políticas de privacidade e os termos de privacidade, ambos escritos em português. Ao seguir a etapa de cadastramento, aparece um aviso relevante e destacado sobre a política de cookies. A transparência chama a atenção, na medida em que o aplicativo tenta realmente explicar o porquê das concessões. Também é possível acessar os documentos pelo menu específico de configurações, mas é inviável proceder a revogações de consentimento, pois o aplicativo define como "necessários" os cookies[610].

O *Google Music* também exibe os termos de privacidade e políticas de privacidade em sua tela inicial, estando todos em português. Além disso, também exibe a opção de ascensão à versão paga do aplicativo, o que inibiria os anúncios, provavelmente apenas na metodologia *freemium*, já que os dados pessoais continuariam sendo tratados, só não utilizados para a publicidade comportamental no âmbito específico da plataforma. Também é possível acessar os documentos pelo menu específico de configurações, mas é inviável proceder a revogações de consentimento.

[610] "Importante: política de cookie e tecnologia de rastreamento. Ao continuar, você aceita o uso de cookies de outras tecnologias de rastreamento pela Deezer e seus parceiros para o oferecimento de conteúdo e ofertas sob medida aos seus interesses, anúncios personalizados e análise de nosso tráfego".

O *Spotify* segue o mesmo padrão, mas há possibilidade de revogação do consentimento por meio de ferramenta de gerenciamento de dados pessoais. De modo específico, é possível fazer duas revogações: dados do *Facebook* e anúncios personalizados. E o aplicativo ainda permite que o usuário baixe um arquivo consolidado com todos os dados de que a plataforma dispõe sobre ele, o que permite um maior *accountability* pelo consumidor/usuário. Isso parece aderente à tutela da privacidade que se entende como adequada, sobretudo no tocante ao direito de acesso livre[611].

Na contramão do *Spotify*, o *Palco MP3* só exibe suas políticas de privacidade e termos de privacidade em menu específico de configurações, ambos em português e sem possibilidade de qualquer revogação de consentimento, o que se torna particularmente pernicioso dado o contexto de que o aplicativo exibe anúncios na plataforma – provavelmente direcionados.

Também na contramão, o *Shazam* só exibe suas políticas de privacidade e termos de privacidade em menu específico de configurações, ambos em inglês. A única possibilidade de revogação de consentimento é sobre o armazenamento dos dados de localização – dado que não parece guardar qualquer relação de adequação e necessidade com o *player* de músicas.

De toda forma, o aplicativo permite a utilização sem que seja criada uma conta – o que parece aderente à tutela da privacidade que se entende como adequada. Ou seja, *a priori*, não é feito o *targeting* do usuário que navega sem *login* na plataforma[612].

O *Vigo* exibe sua política de privacidade e seus termos de privacidade logo na inicialização, ambos em português. Também exibe os termos no menu específico de configurações, permitindo que o usuário edite e revogue algumas concessões previamente definidas. Contudo, as revogações aqui envolvem mais a usabilidade da rede social – quem pode seguir o usuário, quem pode ver as informações, quem pode mandar mensagem a você e etc. – do que propriamente a tutela da privacidade em si.

O *TikTok* tem funcionamento idêntico ao do *Vigo*, com a única ressalva de que os documentos estão em inglês. Outra observação interessante é que, nele, há termos de

---

[611] (i) "Dados do Facebook: Quando você opta por não processar seus dados do Facebook no Spotify, interrompemos todo o processamento de dados do Facebook compartilhados com o Spotify, exceto os dados pessoais que permitem que você se inscreva no Spotify usando sua conta do Facebook"; e (ii) "Anúncios personalizados: Se você usa o serviço gratuito com suporte de anúncios do Spotify e opta por não receber anúncios personalizados, não combinaremos sua conta com as informações compartilhadas com o Spotify por parceiros de publicidade terceirizados. Isso significa que você ainda receberá anúncios com base nas informações básicas da sua conta do Spotify, mas eles não serão personalizados para você".

[612] "A ID de instalação do Shazam não gera identificação pessoal e é usada para fins de análise e resolução de problemas. Ela é compartilhada com terceiros. Não está associada a você, a menos que crie e acesse uma conta do Shazam com seu endereço de e-mail ou acesse sua conta com credenciais de terceiros".

privacidade específicos para usuários que residem na União Europeia, em razão de o regime de proteção de dados ser mais apertado lá.

Quando de sua inicialização, o *YouTube Kids* apresenta ferramentas interessantes de controle parental dos acessos da criança. Ainda na tela inicial, é exibida uma espécie de resumo dos termos de privacidade (que são mostrados em formato mais analítico quando do menu específico de configurações, em português), cuja leitura é muito mais fácil e intuitiva do que de todos os demais aplicativos analisados[613]. O desejável é que todos os aplicativos se inspirassem nisso por padrão, na medida em que facilitar a compreensão do usuário é um dos nortes principais da LGPD.

Apesar de ser possível fazer a limpeza do histórico – o que, em tese, dificulta o *targeting* –, é inviável tomar maiores controles acerca da revogação de permissões inicialmente concedidas. De toda forma, o aplicativo parece, nesse ponto, aderente à tutela da privacidade que se entende como adequada. A ideia é exatamente a mesma no *YouTube* normal, que, em acréscimo, possibilita um modo anônimo de navegação, em que não são armazenados arquivos de *cookies* para fins de posterior publicidade dirigida.

O aplicativo *Now Net e Claro* não exibe seus termos de privacidade ou sua política de privacidade durante a inicialização e em qualquer parte do menu específico de configurações. Por consequência, também não permite a revogação de qualquer consentimento inicialmente dado. A suposição é de que a empresa admita que o consentimento seria implícito ao ter a assinatura da Net ou da Claro, o que, *a priori*, não parece sustentável juridicamente, sobretudo à luz do preceito de privacidade contextual.

O *RecordTV* já inicia exibindo um anúncio patrocinado e, após, solicitando acesso à localização do dispositivo, o que é recusável. Também não são indicados os termos de privacidade e a política de privacidade em nenhum lugar. O que há, em verdade, são incessantes *banners* de anúncios variados. O aplicativo *Band*, por exemplo, apesar de não permitir qualquer

[613] Em suma, a mensagem lá escrita é a seguinte: "Coleta e uso de informações no YouTube Kids: Tomamos precauções consideráveis para proteger a privacidade dos usuários do nosso aplicativo. O YouTube Kids é uma experiência de aplicativo sem *login*, o que significa que ele não coleta, usa ou divulga dados pessoais conectados com uma conta do Google, como nome, endereço ou informações de contato". A mensagem ainda continua: "Este aplicativo coleta alguns identificadores anônimos usados para apoiar as operações internas dos nossos serviços, como prevenção de spam e de condutas abusivas e controle de frequência de anúncios e de vídeos. Nós coletamos o histórico de visualizações e de buscas no aplicativo para usarmos como um sinal quando recomendamos vídeos. Visite as configurações dos pais para limpar ou pausar o histórico de visualizações e de buscas". E arremata: "Quando você limpa seu histórico, o aplicativo reconfigura seus Vídeos Recomendados e Assista Outra Vez. O aplicativo automaticamente apaga seus históricos de visualizações e de busca quando você aciona Busca Desligada. Quando seu histórico é pausado, o aplicativo para de usar vídeos que você assiste e termos que você busca como sinais para Vídeos Recomendados e Assista Outra Vez".

revogação e não exibir os termos logo quando de sua inicialização, ao menos é transparente no menu específico de configurações.

O *SBT*, ao iniciar, solicita acesso (i) ao fazimento e gerenciamento de chamadas telefônicas, (ii) à localização do dispositivo e (iii) às fotos, mídia e arquivos do dispositivo. Nesse momento, é possível recusá-las, até porque não há qualquer pertinência lógica entre os dados solicitados e o produto oferecido, o que, em tese, significa uma maximização indevida do acesso aos dados pessoais.

Ao iniciar o cadastro, o aplicativo informa ser necessária a concordância com os termos de privacidade, mas não os exibe, o que é inadequado. No menu de configurações, não há como acessar nenhuma das cláusulas contratuais necessárias, o que demonstra falta de transparência da empresa.

Ao iniciar, o *GShow* pede acesso à localização do dispositivo – o que também não parece fazer sentido –, mas é possível recusar. No fazimento do cadastro – que não é a página inicial do aplicativo, mas um menu específico das configurações –, é possível acessar os termos de privacidade e a política de privacidade, mas ambos os documentos são genéricos para todos os produtos da *Globo*, não sendo específicos para o aplicativo ora analisado.

Contudo, não é possível acessar as informações fácil e intuitivamente no menu de configurações do aplicativo, o que denota falta de zelo da aplicação para com a tutela da privacidade dos usuários. Tudo isso é particularmente pernicioso dado o contexto de que o próprio aplicativo admite exibir anúncios em sua plataforma.

O *Netflix* exibe apenas seus termos de privacidade quando da página inicial de cadastro no aplicativo, nada versando sobre a política de privacidade, mas o documento está em português. No menu específico de configurações, contudo, é possível ter o acesso completo aos documentos, embora também seja inviável a revogação de qualquer consentimento inicialmente fornecido. Ao menos, a plataforma informa não exibir anúncios, o que minora as chances de mapeamento de dados para fins de publicidade comportamental.

Ao iniciar, o *Globoplay* pede que o usuário habilite o GPS para "melhorar sua experiência", sem haver maiores explicações de como isso se daria. Sendo o pedido apelativo e sem a necessária transparência efetiva, é de se dizer que contraria a LGPD, mas é possível negar. Depois, afirma que fazer o *login* implica ter ofertas personalizadas, mas também é possível recusar.

Na sequência, aparece um *banner* fixo na parte inferior da tela alertando sobre a política de privacidade, que o usuário pode ler (em português), mas não pode discordar de nada e precisa aceitá-la para que o *banner* suma. Dentro do menu de configurações, é possível acessar

a política de privacidade, mas também sem possibilidade de revogações. Nesse menu, é possível baixar a íntegra da política de privacidade em arquivo compilado de impressionantes 17 páginas.

No *Twitch*, não é disponibilizada a política de privacidade no primeiro acesso, tampouco no menu, pois o aplicativo exige o fazimento de uma conta na plataforma para começar a operar de modo mais personalizado. Ao iniciar o cadastro, é exibido o aviso de privacidade, em português. O termo "aviso", contudo, não passa uma conotação positiva, pois transparece haver menos opções ainda para o usuário revogar eventuais permissões.

O *Likee* opera de modo muito semelhante, embora exiba os conteúdos sem o *login* e chame o documento de política de privacidade, escrito em inglês e acessível apenas no menu. Após o cadastro rápido, cria-se um usuário genérico, dentro do qual já é possível fazer alguns ajustes de privacidade, o que é adequado. Contudo, o acesso completo à plataforma só é possível após a vinculação às contas do *Gmail* ou do *Facebook*, ou com o fornecimento manual de mais dados pessoais.

Por sua vez, o *Disney+* só permite acesso mediante cadastro pago, mas, nessa tentativa de fazimento de cadastro, é possível selecionar o recebimento de notícias e ofertas especiais da *Disney* (*opt-in*) e também é possível ler a política de privacidade, escrita em português e que contempla uma seção dedicada especialmente para a LGPD, o que é diferente dos demais aplicativos analisados.

O *Amazon Prime* exibe, em sua primeira página, o aviso de que é necessário fazer o *login* ou o cadastro na plataforma da empresa e que, ao continuar, "você concorda com a política de privacidade", que é acessível, mas escrita em inglês, o que é inesperado para um empresa do porte da *Amazon* e com tantos usuários no Brasil. Após o *login*, é possível acessar o menu e recusar a exibição de recomendações personalizadas, ofertas especiais, limpar o histórico de pesquisas (útil para tentar sair da bolha), além de ser possível acessar formalmente a política de privacidade, mas sem nenhuma espécie de revogação mais ampla do que as já citadas.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos vinte aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

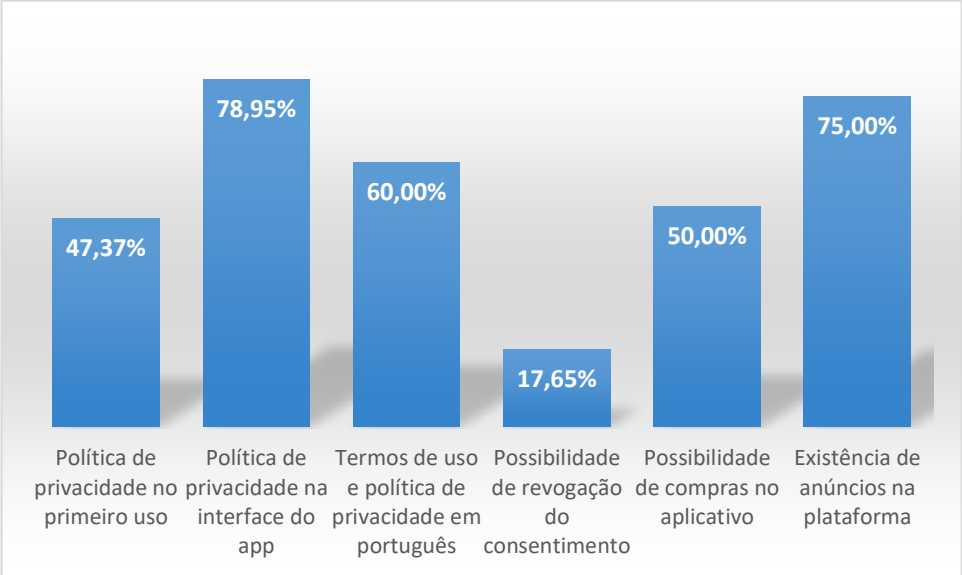

Figura 9 – Estatísticas análise consentimento na categoria *"Entretenimento, vídeos e música"*

4. Comer e beber

Ao iniciar, o *Tudo Gostoso* solicita acesso à localização do celular, sem maiores justificativas aderentes ao critério legal da transparência e da minimização do acesso aos dados pessoais. Contudo, é possível rejeitar a solicitação. A política de privacidade e os termos de privacidade só são exibidos no menu de configurações próprio, mas não há qualquer possibilidade de revogação de consentimento, o que seria importante, dada a publicidade comportamental existente no aplicativo.

O *McDonalds* segue exatamente a mesma linha, com a única vantagem de não haver anúncios no aplicativo – é claro que há as ofertas da própria empresa, mas se pressupõe, com alguma razoabilidade, que o usuário, ao baixar um aplicativo tão específico, estaria tacitamente aceitando esse tipo de ofertas.

Quanto ao *Foursquare*, a política de privacidade e os termos de privacidade só podem ser acessados no menu específico de configurações do aplicativo, mas ambos estão em português. Também é possível revogar dois consentimentos relevantes: (i) permissão para que o aplicativo vincule o perfil criado àquele do *Facebook*, compartilhando informações de contato; e (ii) permissão para que o aplicativo veicule anúncios de segmentação comportamental fora da própria plataforma. A postura da empresa – embora seja uma configuração *opt-out*, ao passo que o mais correto seria a *opt-in* – parece aderente à tutela da privacidade que se entende como adequada.

O *Rappi* exibe seus termos de privacidade e política de privacidade já em sua tela inicial, sendo condição para a utilização do aplicativo a sua aceitação. Ambos os documentos estão em português. No passo seguinte, é possível fazer o *login* com *Facebook*, *WhatsApp*, *Google* ou e-mail normal. Também é possível acessar os documentos pelo menu específico de configurações, mas não é viável qualquer revogação de consentimento.

Ao iniciar, o *Ifood* solicita acesso à localização do dispositivo, mas é possível recusar. Quando da tela de verificação do número do celular, o aplicativo informa utilizar a tecnologia Account Kit, do *Facebook*. Ou seja, ao ali inserir o número, os dados do usuário já são compartilhados com a plataforma *Facebook*, o que pode ser indesejável. Segundo o aplicativo, há a possibilidade de a verificação ser feita por SMS – e não pelo *Facebook* –, mas não há maiores informações de como isso ocorreria.

Com o envio do código verificador, a tela seguinte indica que continuar significa "aceitar os termos, a política de dados e o uso de cookies do *Facebook* e a política de privacidade e os termos de serviço do *Ifood*". Nesse caso, parece haver uma *venda casada* dos aplicativos, o que não é aceitável sob a ótica da LGPD. No menu de configurações, apesar de também haver referência à política de privacidade e aos termos de privacidade – ambos em português –, não parece haver qualquer possibilidade de revogação dos consentimentos.

Ao iniciar o *Uber Eats*, não são exibidos os termos e uso e de privacidade do aplicativo. Mas, no menu, é possível ver a política de privacidade da empresa, escrita em português, embora sem possibilidade de revogação do consentimento. Os termos, ao menos, parecem escritos especificamente para o Brasil, embora sejam os mesmos daquele do *Uber* usado para o transporte individual de passageiros.

Por sua vez, o *Zé Delivery*, ao iniciar, solicita acesso à localização do usuário, o que é possível negar. Ao pretender criar uma conta, o que pode ser efetuado com o *login* do *Facebook* ou da *Apple*, aparece a política de privacidade organizada de modo aparentemente didático, com uma espécie de quadro-resumo no início. Além disso, aparece *banner* embaixo informando que o aplicativo usa "cookies que são necessários ao funcionamento adequado de suas páginas", sendo inviável impedir que os "estritamente necessários" funcionem.

No cadastro, são solicitadas algumas informações pessoais – idade, CPF e celular –, que o aplicativo explica serem necessárias para confirmar a possibilidade de o usuário comprar bebidas alcoólicas e para evitar fraudes. Nessa linha, o aplicativo pareceu adequado à tutela da privacidade e dos dados pessoais balizada pela LGPD, na medida em que, ao menos, há possibilidade de revogações e há explicações sobre os motivos dos acessos.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos sete aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

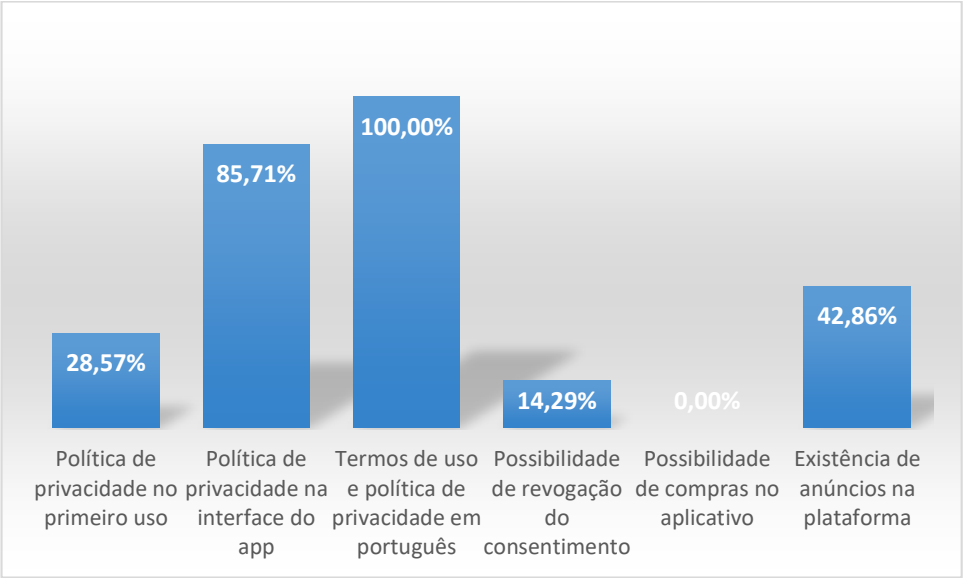

Figura 10 – Estatísticas análise consentimento na categoria "*Comer e beber*"

5. Infantis e jogos

Na página inicial, o *Garena* exibe uma "descrição de acesso", para a qual, apesar da transparência explicativa, a única opção é aceitar[614]. Na página seguinte, o aplicativo pede permissão expressa de "acesso às fotos, mídia e arquivos do dispositivo", de "fazimento e gerenciamento de chamadas telefônicas" e de "gravação de áudio", sendo todos os pedidos vinculados.

Na página inicial seguinte, há o pedido de *login*, ocasião em que são exibidos os termos de serviço e a política de privacidades, ambos em inglês. É possível encontrar os mesmos documentos no menu específico de configurações, mas não há qualquer opção de revogação de consentimentos.

Em sua página inicial, o *Subway Surfers* pede o *login* com alguma conta *Google*, por meio do qual serão compartilhados o nome e a foto de perfil. Na página seguinte, aparece uma mensagem com o seguinte teor: "Por meio deste, eu dou meu consentimento para que a

[614] "[Permitir o acesso à leitura de dados] registra as informações de conta de usuário para *login* rápido; salva as atualizações e fotos do jogo. [Permitir o acesso à leitura de estado do celular] lê IMEI para identificar os dispositivos que usam hacks. [Permitir o acesso ao microfone] suporta chat de voz para conversar quando joga".

Kiloo [desenvolvedora do jogo] divulgue a ID de publicidade do meu dispositivo para empresas de redes de publicidade para fins de publicidade no jogo com base em minhas preferências pessoais".

Há, contudo, afirmação de que é possível revogar o consentimento. Também é possível acessar a política de privacidade da desenvolvedora (para todos os seus aplicativos, e não especificamente para o ora analisado), integralmente em inglês.

O *Meu Talking Tom 2* exibe a política de privacidade logo em sua tela inicial, inteiramente em português, mas aparentemente aplicável a todos os aplicativos desenvolvidos pela empresa responsável pelo desenvolvimento do software, ou seja, não atende ao requisito da especificidade. Durante a curta utilização do aplicativo, contudo, não se vislumbrou qualquer forma de fácil e intuitiva de revogar os consentimentos fornecidos ou de acessar novamente os termos de privacidade, o que denota falta de transparência do aplicativo.

O *Pou* não exibe sua política de privacidade na tela inicial ou nas configurações do aplicativo, embora haja anúncios na plataforma – em forma de vídeos que, se assistidos, dão recompensas ao jogador. Durante o curto período de utilização, foi solicitada permissão expressa de acesso ao microfone do dispositivo, mas é possível recusá-la. Também há lacuna de transparência, o que se mostra inadequado frente às balizas da LGPD.

Em sua tela inicial, o *Fifa* exibe a política de privacidade e o contrato de usuário da desenvolvedora do *software* (ambos escritos em português), ou seja, não se trata de algo especificamente pensado para o jogo em si, mas para todos os outros produtos da empresa. Para continuar, é necessário aceitar os termos.

No menu de configurações, é possível "desativar o compartilhamento das informações de uso", na medida em que, por padrão, o aplicativo "coleta dados do seu dispositivo para fornecer e melhorar produtos e serviços e personalizar a sua experiência. Ao desativar o compartilhamento de dados de uso, o usuário limita a coleta de dados do dispositivo ao necessário para a operação do próprio jogo". Parece inadequado às normas de proteção de dados o fato de que, por padrão, o compartilhamento é ativado, sendo que o preferível seria o contrário.

O *Candy Crush*, em sua tela inicial, informa que, "para continuar jogando, o usuário precisa aceitar os termos de serviço e estar ciente da política de privacidade", ambos escritos em português. É possível acessar os mesmos documentos no menu de configurações do aplicativo, mas não é viável proceder à revogação do consentimento inicial. Ao menos, o aplicativo informa não veicular anúncios na plataforma.

O *Buddy Toss* não exibe sua política de privacidade na tela inicial ou no menu de configurações, ou seja, falta de transparência. Ao revés, aliás, durante o curto período de utilização do aplicativo (dois minutos), foram exibidos seis anúncios – em formatos diversos, sendo alguns fixos na tela do jogo e outros de vídeos. Ao menos, há uma opção para que o usuário cancele a exibição de publicidade, desde que pague R$ 7,49 pela versão *menos publicitária* do aplicativo.

Isso parece alinhado ao conceito de níveis de aplicativos. Contudo, como não há qualquer referência à política de privacidade, não é possível aferir se esse pagamento impediria a coleta de dados e, por consequência, todo o ciclo produtivo da publicidade comportamental, ou se consistiria apenas em um filtro da última etapa – a exibição do anúncio direcionado. Seria bom, nessa linha, se se pudesse falar em versão que menos trata os dados pessoais dos seus usuários, mas isso não deve ocorrer, dada a metodologia de aplicativos *freemium*.

O *Hopping Ball* segue exatamente a mesma linha, mas o preço para a não exibição dos anúncios é de R$ 14,99. O *Paint Pop 3D* também segue linha parecida, mas, ao iniciar, solicita permissão expressa de acesso às fotos, mídia e arquivos do dispositivo e ao seu local, mas é possível recusá-las. Também há uma opção para que o usuário cancele a exibição de publicidade, desde que pague R$ 11,99 pela versão *menos publicitária* do aplicativo.

O *Demo Minecraft* também não exibe sua política de privacidade e seus termos de privacidade na tela inicial ou no menu de configurações (ao menos, não é localizável de modo fácil e intuitivo). Pelo menos, o aplicativo informa não conter anúncios, mas falta transparência sobre a coleta e tratamento de dados pessoais. Não se criou, contudo, a conta necessária para dar prosseguimento ao jogo.

O *Fruit Ninja* só exibe sua política de privacidade e seus termos de privacidade no menu específico de configurações, estando os dois documentos em inglês. Contudo, apesar de o aplicativo informar a existência de anúncios em sua plataforma, não é possível proceder a qualquer revogação de consentimento nela.

Ao iniciar, o *Angry Birds* informa que, para jogar, o usuário deve concordar com os termos de privacidade e a política de privacidade, ambos escritos em português e de modo genérico e abrangente para todos os aplicativos do desenvolvedor do jogo. Contudo, apesar de o aplicativo também informar a existência de anúncios em sua plataforma, não é possível proceder a qualquer revogação de consentimento na plataforma.

O *Pokémon Go* segue exatamente a mesma linha, com a única observação de que, diversamente dos demais jogos, informa não haver anúncios em sua plataforma.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos quinze aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

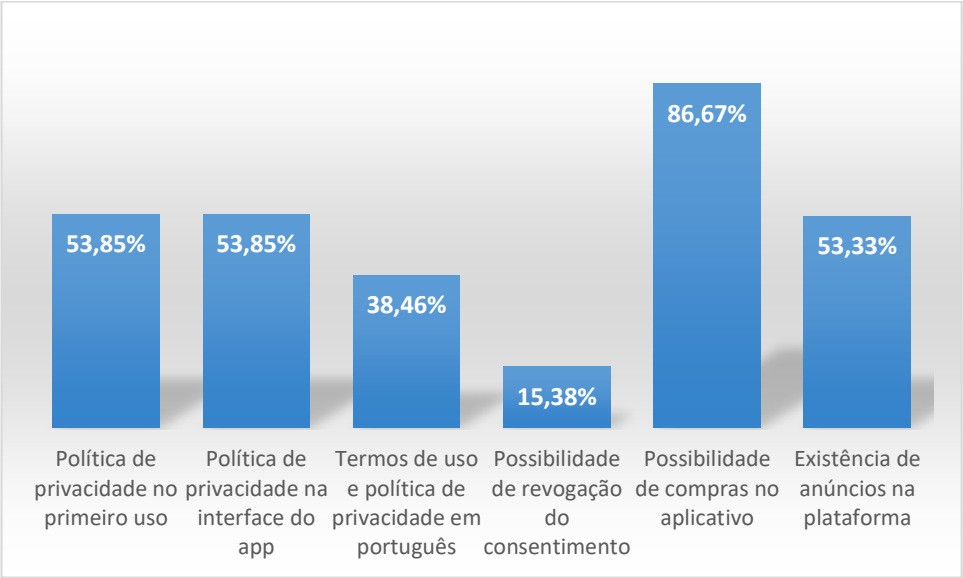

Figura 11 – Estatísticas análise consentimento na categoria "*Infantis e jogos*"

6. Finanças e crédito

O *Banco do Brasil* exibe sua política de privacidade no menu de configurações, que, por sua vez, redireciona para as próprias configurações do sistema *Android* para permitir a revogação do consentimento de algumas permissões previamente concedidas. Frise-se, aliás, que o acesso ao menu específico de configurações é uma forma de revogação do consentimento de permissões para qualquer aplicativo instalado no celular, mas o interesse aqui é avaliar quão fácil é proceder a essa ação na própria interface do aplicativo, e não no menu de configurações do sistema do próprio celular.

Ao abrir o aplicativo *Caixa*, a página de "cadastro de usuário com conta" exibe um contrato geral com definições sobre o funcionamento do aplicativo móvel, mas não é dada nenhuma informação mais enfática a respeito da política de privacidade da ferramenta. Também não foi encontrado nenhum mecanismo de revogação de consentimentos de modo simples.

O *Itaú* solicita que, para a criação da conta, o cliente baixe outro aplicativo específico, o *Itaú abreconta*. Ao baixá-lo, a página inicial solicita acesso expresso à localização do dispositivo – sem maiores justificativas para tanto –, mas é possível recusá-la. Por sua vez, a política de privacidade e os termos de uso aparecem na página inicial, mas também há uma

informação relevante e alinhada ao que se falou anteriormente: embora a classificação do aplicativo na loja *Google Play* seja "livre", o requisito inicial para a abertura da conta é ser maior de dezoito anos.

Frisa-se o mesmo ponto: a classificação indicativa deveria ser mais criteriosa. Voltando ao aplicativo normal – sem abrir a conta –, vê-se que é fácil acessar os termos de privacidade na própria interface da página inicial, mas não foi encontrada nenhuma forma de revogação das permissões.

O aplicativo *Serasa Consumidor* também segue o mesmo padrão. Embora a *Serasa* seja uma empresa privada, o seu banco de dados é considerado de caráter público – passível, até mesmo, da impetração de *habeas data*. Contudo, o aplicativo permite que o usuário faça o seu cadastro por meio dos dados das contas *Facebook* e *Google*, o que pode ser preocupante.

Afinal, parece pernicioso que essas duas empresas – que gerenciam, sobretudo, redes sociais e outras ferramentas de comunicação – possam ter acesso às informações financeiras do usuário, que deveriam ser gerenciadas sob estrito sigilo pelo aplicativo *Serasa*. Caso haja essa intercomunicação entre as plataformas – e é difícil se certificar de que não há –, o usuário pode ser prejudicado pela violação ao dever de privacidade contextual[615] e às expectativas de privacidade[616].

Bioni, nesse sentido, afirma que "devem-se esgotar os elementos contextuais da relação sob análise, verificando-se, dentre outros aspectos: i) quais são os propósitos do tratamento dos dados pessoais, levando-se em consideração o contexto da relação subjacente ao fluxo informacional; ii) como terceiros podem estar inseridos no fluxo informacional e sob quais condições; iii) quais são as implicações do tratamento dos dados pessoais sobre seu titular: iii.a) no que diz respeito ao desenvolvimento da sua personalidade; iii.b) para que ele se relacione livremente em outras e nas diversas esferas sociais"[617].

Ao iniciar, o *Bradesco* solicita cinco permissões expressas: (i) acesso à localização do dispositivo; (ii) acesso a fotos, mídia e arquivos; (iii) permissão para o fazimento e gerenciamento de chamadas telefônicas; (iv) permissão para gravar áudio; e (v) permissão para tirar fotos e gravar vídeos. Em um primeiro momento, foi possível recusar todas.

---

[615] NISSENBAUM, Helen. Privacy in Context: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010; NISSENBAUM, Helen. Privacy as contextual integrity. Washington Law Review, v. 79, p. 130, 2004.

[616] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: RT, 2020 [livro eletrônico sem numeração de páginas].

[617] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020 [livro eletrônico sem numeração de páginas].

Ao clicar na opção seguinte de "abrir conta", entretanto, a ferramenta informa ser necessário conceder as permissões (ii), (iv) e (v) retro, de modo vinculado. É fácil encontrar os termos de privacidade no menu de configurações do aplicativo, mas, até onde se seguiu no procedimento da pretensa abertura de conta, esses dados não foram exibidos ao usuário na tela inicial. Também não foi encontrada qualquer forma intuitiva de revogação de consentimento.

Quanto ao *Nubank*, o aplicativo, antes mesmo de exibir a política de privacidade, exige que o usuário insira o número do CPF e um e-mail. Seria mais aderente se, antes disso, as *regras do jogo* fossem a primeira informação dada ao usuário. Dentro do menu do aplicativo, é possível acessar a política de privacidade, em inglês, e revogar algumas permissões concedidas por padrão à ferramenta, inclusive no tocante ao acesso à localização – supostamente necessária para evitar fraudes.

Situação muito parecida ocorreu com o aplicativo *Banco Inter*, que exige a inserção dos dados pessoais na primeira tela da criação da conta, sem nenhuma informação *a priori* sobre as políticas de privacidade. O mesmo também acontece com o *Digio*, com a única peculiaridade de que, ao abrir o *software*, já se solicita a permissão expressa de acesso à localização do dispositivo.

Ao abrir o *PayPal* na opção de "criar conta", a primeira mensagem do aplicativo é um pedido de "acesso às suas informações de contato", para facilitar o preenchimento dos dados do formulário, mas é possível recusá-la. Diferentemente das três plataformas retro, já nessa página inicial há links específicos que direcionam ao contrato de usuário, à declaração de privacidade e aos termos e condições do aplicativo, todos escritos em português.

Como não se deu continuidade ao cadastro, não foi possível avaliar critérios de revogação do consentimento e a transparência da própria interface de uso do aplicativo, mas essa transparência inicial da plataforma pareceu aderente à tutela da privacidade que se entende como adequada e à frente das outras três imediatamente concorrentes. O mesmo ocorreu com o *PicPay*, que afirma "não se preocupe! Seus dados estão seguros conosco e são necessários para confirmar sua identidade". É uma mensagem que, embora possa ser abstrata e vazia, tem o condão de gerar algum nível de engajamento no usuário.

Como nenhum dos últimos 3 aplicativos efetivamente "funcionou" no celular usado na análise – porque exigiam, de plano, o fornecimento de dados pessoais para a criação da conta –, eles foram retirados da contagem dos critérios de "política de privacidade na interface do *app*" e de "possibilidade de revogação do consentimento", para fins do gráfico a ser construído.

O *Mercado Pago* também teve transparência semelhante, mas com a opção de criar a conta por meio das credenciais de usuário da *Google* ou do *Facebook*. No caso desse

aplicativo, como o presente autor já tinha conta cadastrada, foi possível o acesso ao menu de configurações, onde não foi encontrada, de modo fácil e intuitivo, a política de privacidade. Tampouco se achou qualquer mecanismo de revogação de consentimento prévio.

Em sua página inicial, o *Investing* apresenta longo documento de política de privacidade e de termos de privacidade, com a opção binária de concordar ou discordar. O porém reside no ponto de que ambos estão escritos em inglês, o que pode dificultar sobremaneira o entendimento pelo usuário ordinário brasileiro. Dentro do menu de configurações, também é possível acessar tais documentos de modo fácil e intuitivo, além de ser possível ascender à versão paga, sem anúncios de publicidade comportamental. Não foi encontrada, contudo, qualquer forma de revogação do consentimento.

Ao iniciar, o *Santander* faz duas solicitações expressas de permissões: (i) fazimento e gerenciamento de chamadas telefônicas e (ii) acesso à localização do dispositivo, cujas concessões são vinculadas. Como o aplicativo solicita a criação de conta com dados pessoais logo na tela seguinte, não foi possível avaliá-lo nos outros critérios.

O *Santander ESP* também solicita a criação de conta, mas não pede as permissões do brasileiro logo ao iniciar. Ainda mais adequado à tutela dos dados pessoais, o *Santander UK* exibe, em sua tela inicial, as políticas de uso e de privacidade: sem a concordância expressa, não há como continuar no aplicativo. Por tais motivos, estes aplicativos também foram retirados da contagem dos critérios de "política de privacidade na interface do *app*" e de "possibilidade de revogação do consentimento", para fins do gráfico a ser construído. E os dois aplicativos internacionais foram desconsiderados do critério "termos em português".

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos quinze aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

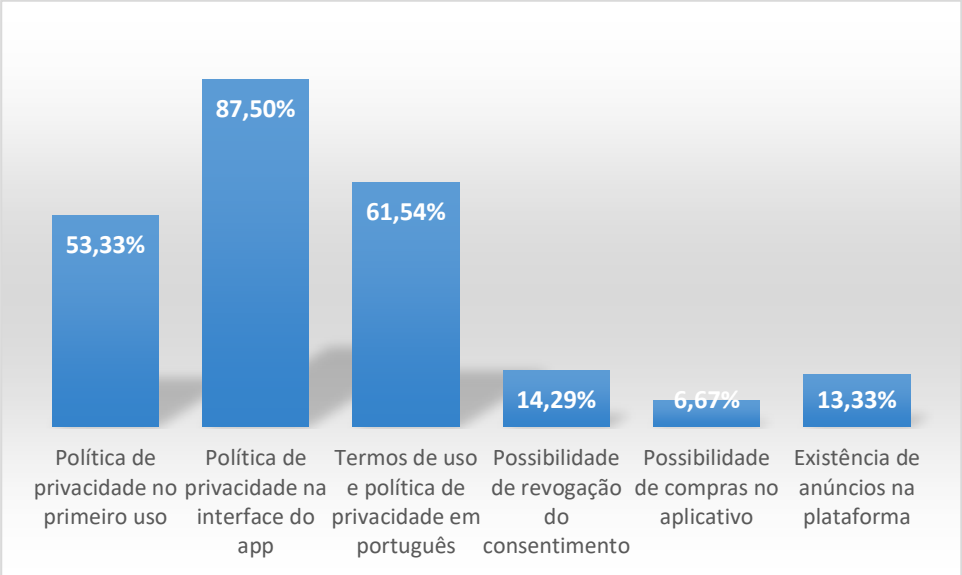

Figura 12 – Estatísticas análise consentimento na categoria "*Finanças e crédito*"

7. Compras

O *Mercado Livre* não exibe qualquer informação sobre política de privacidade ou termos de privacidade em sua primeira página ou no menu específico de configurações. Aliás, só é possível acessar referido menu se o usuário fizer o *login* na plataforma, o que parece inadequado sob a perspectiva de transparência mais ativa prevista na LGPD.

O *Wish*, em sua primeira página, exibe a necessidade de se fazer *login*, seja por novo cadastro ou por acesso pelas contas *Google* e *Facebook*. Na mesma página, estão exibidos os termos de privacidade e a política de privacidade, ambos em inglês. Após a criação de uma conta, foi possível acessar o menu de configurações, onde, além de estar novamente exibida a política de privacidade, também há como revogar o acesso do *Facebook* para usar os dados coletados para personalizar o conteúdo de anúncios. É curioso o fato de que o *Facebook* é exibido como empresa com acesso aos dados em quase todos os aplicativos aqui avaliados.

Em sua primeira página, o *OLX* requer permissão de acesso à localização do aparelho, para supostamente ficar mais fácil visualizar anúncios da região do usuário. Particularmente, não se entende como adequada essa justificativa para o acesso a informação tão relevante, na medida em que, durante a utilização da ferramenta, não é difícil fazer os filtros das localidades.

Justamente nesse sentido, é possível negar a permissão e, logo na sequência, escolher o local manualmente, de modo simples. O mesmo acontece com o aplicativo *Zé Delivery*, já analisado. No menu de configurações, é possível acessar os termos e condições do

aplicativo e a política de privacidade. Não foi encontrada qualquer forma de revogação de consentimento.

O *Magazine Luiza* só exibe a política de privacidade no menu específico de configurações. Não é possível, contudo, qualquer revogação de consentimento. Ainda menos transparente, o aplicativo *Americanas* não exibe sua política de privacidade em qualquer lugar intuitivamente localizável. O *AliExpress* só exibe sua política de privacidade no menu específico de configurações, em texto integralmente em inglês, mas também não há qualquer possibilidade de revogação do consentimento de permissões concedidas.

O aplicativo *Amazon* exibe as condições de uso e as políticas de privacidade na página inicial, ao criar conta, e em menu específico de configurações, sendo ambos de português. De interessante, o aplicativo apresenta um menu específico para explicar o funcionamento dos anúncios baseados em interesses. Contudo, não parece haver mecanismos de revogação das permissões concedidas. Nesse aspecto, é relevante pontuar que o aplicativo *Amazon Prime*, que deveria operar de modo muito semelhante à loja, pareceu menos aderente às normas da LGPD.

O *Ebay*, por sua vez, só exibe a política de privacidade e os termos de privacidade em menu específico de configurações, todos em português. Teoricamente, seria possível revogar as permissões concedidas, mas a página específica afirma que as marcações ali feita "só afetam clientes na Área Econômica Europeia (AEE)", havendo a empresa parceira que cuida da publicidade em cada segmento.

O *Enjoei*, ao iniciar, pede acesso aos contatos, fotos, mídias e arquivos do usuário, o que é possível recusar. Afinal, não parece haver razoabilidade nesse pleito de acesso. Ao pretender criar a conta, para a qual é possível usar os dados do *Facebook*, só são disponibilizados os termos de serviço, e não a política de privacidade. Como não se criou a conta, não foi possível aferir o funcionamento da plataforma após o *login*.

Por sua vez, o *Shopee* inicia requerendo acesso à localização do usuário, o que se daria integralmente, o que é possível recusar. Ao iniciar o cadastro, é exibida a política de privacidade, integralmente em inglês. Como não se criou a conta, não foi possível aferir o funcionamento da plataforma após o *login*.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos dez aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

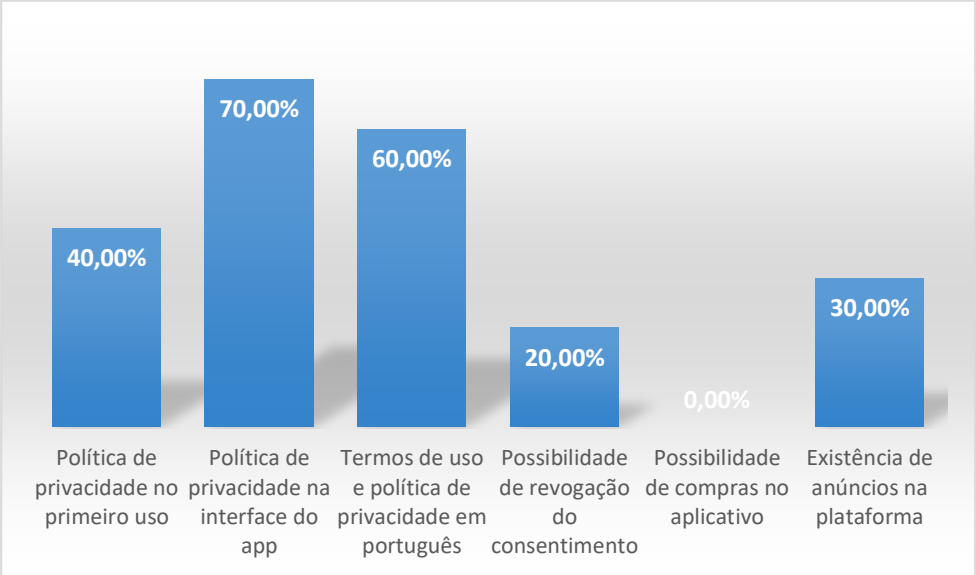

Figura 13 – Estatísticas análise consentimento na categoria "*Compras*"

8. Notícias e revistas

Ao iniciar, o *G1* pede acesso à localização do dispositivo, mas é possível recusar a permissão. Contudo, não são exibidos os termos de privacidade e a política de privacidade durante o primeiro uso. Eles sequer são fácil e intuitivamente encontrados no menu de configurações do aplicativo, o que denota uma lacuna na tutela da privacidade dos usuários. Tudo isso é particularmente pernicioso dado o contexto de que o próprio aplicativo admite exibir anúncios em sua plataforma.

De modo semelhante, o aplicativo *Folha de SP* também não exibe os termos de privacidade e a política de privacidade em sua tela inicial, mas é possível encontrá-la no menu de configurações, obviamente em português. Contudo, continua sendo impossível revogar qualquer consentimento tacitamente fornecido.

Por sua vez, o *UOL Notícias* mostra, em sua primeira tela, a necessidade de fazer *login* para acessar o conteúdo. É possível entrar com o *Facebook*, com o *Google* ou criar uma conta alheia às redes sociais. Esse ponto, aliás, é um importante distintivo das duas aplicações anteriores, que não exigiam qualquer espécie de *login* para dar acesso às notícias. Na mesma página, há link que remete diretamente à política de privacidade, inteiramente em português.

Também é possível acessar a política em menu próprio de configurações, mas não é viável revogar qualquer permissão concedida. E isso também seria relevante aqui, na medida em que há anúncios na ferramenta. Ou seja, embora o *UOL* seja um pouco mais transparente do que os dois anteriores, há um excesso de acesso aos dados no sentido de exigir o

credenciamento do usuário. Diversos portais jornalísticos, é verdade, vêm adotando essa metodologia mais recentemente.

O *El País* não exibe as políticas de privacidade e os termos de privacidade em sua página inicial ou sequer no menu de configurações. Por consequência, também não é possível revogar o consentimento de qualquer permissão. Mesmo selecionando a versão europeia do aplicativo, nada modifica. Há, assim, aparente lacuna na proteção da privacidade dos usuários, sobretudo por também haver anúncios.

Em sua página inicial, o *Flipboard* exibe a mensagem de que, "ao continuar, você aceita os termos de privacidade e a política de privacidade", ambos escritos em português. Contudo, também não há como revogar eventuais permissões concedidas. O *CNN* também exige, em sua primeira página, os termos de serviço e a política de privacidade, cuja opção é vinculada pela aceitação.

O *Fox News* segue exatamente o mesmo padrão do *CNN*, inclusive com a possibilidade de retirar o consentimento da publicidade comportamental de todas as empresas responsáveis por isso. Trata-se, como o aplicativo prevê, de uma posição de deferência à "Digital Advertising Alliance (DAA)[618], que estabelece e aplica práticas de privacidade responsáveis em toda a indústria para publicidade digital relevante, proporcionando aos consumidores maior transparência e controle através de Princípios multifacetados que se aplicam a Dados Multi-Site e Dados entre Aplicativos reunidos em ambientes de *desktop* ou móveis".

Na comparação com o *CNN*, o *Fox* parece um pouco melhor, na medida em que permite a retirada do consentimento de todas as empresas de publicidade comportamental, ao passo que o *CNN* exibe a opção "saiba mais" em determinadas empresas, como o *Facebook*.

O *NY Times* segue a mesma lógica dos dois anteriores, mas não permite que o usuário manifeste a *opt-out* no que tange às empresas de publicidade comportamental. Também não há qualquer outra forma de revogação de consentimentos. Nesse sentido, os concorrentes *Fox* e *CNN* parecem mais adequados quanto à tutela da privacidade que se entende por adequada e aderente à LGPD – claro que o paradigma não é esse para essas empresas – e a outras normas internacionais de proteção de dados.

O *Le Figaro* não fala nada sobre privacidade ou termos de privacidade em sua página de inicialização ou no menu específico de configurações – ao menos em uma busca rápida por parâmetros intuitivos. Isso parece peculiar, na medida em que o RGPD exige

[618] DIGITAL ADVERTISING ALLIANCE. Disponível em: <https://digitaladvertisingalliance.org/>. Acesso em: 7 abr. 2021.

requisitos apertados para o tratamento de dados, colocando a transparência em posição máxima de destaque, dado que o consentimento precisa ser efetivamente informado para autorizar o tratamento – se que é esse é o permissivo legal efetivamente utilizado para o tratamento dos dados.

Ao revés, aliás, o que se viu durante o curto período de uso do aplicativo foi a exibição de dois *banners* de tela cheia sobre anúncios publicitários de lojas brasileiras. A mesma linha é seguida pelo *Der Spiegel*. Apesar de muito parecido, o *Le Monde* exibe a política de "confidentialité" no menu específico de configurações, o que lhe dá ligeira vantagem na competição pelo zelo da privacidade.

O *BBC*, apesar de não exibir os termos de privacidade em sua tela inicial, contém todos os documentos no menu específico de configurações. É possível fazer a revogação simples do compartilhamento de estatísticas, que o aplicativo diz usar apenas para analisar e melhorar os serviços oferecidos no aplicativo – dentre os quais, supõe-se, a própria publicidade comportamental.

Por sua vez, o *The Guardian*, embora não exiba os seus termos de privacidade em nenhum lugar de intuitivo e de fácil acesso, permite que o usuário proceda à revogação de serviços de rastreio para fins de publicidade comportamental.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos treze aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas (com a observação de que, no terceiro quesito, foram considerados os seis aplicativos tipicamente voltados ao público brasileiro – *G1*, *UOL Notícias*, *CNN*, *Folha de SP*, *Flipboard* e *El País*); afinal, não faria sentido avaliar se o *Der Spiegel* tem termos de privacidade em português:

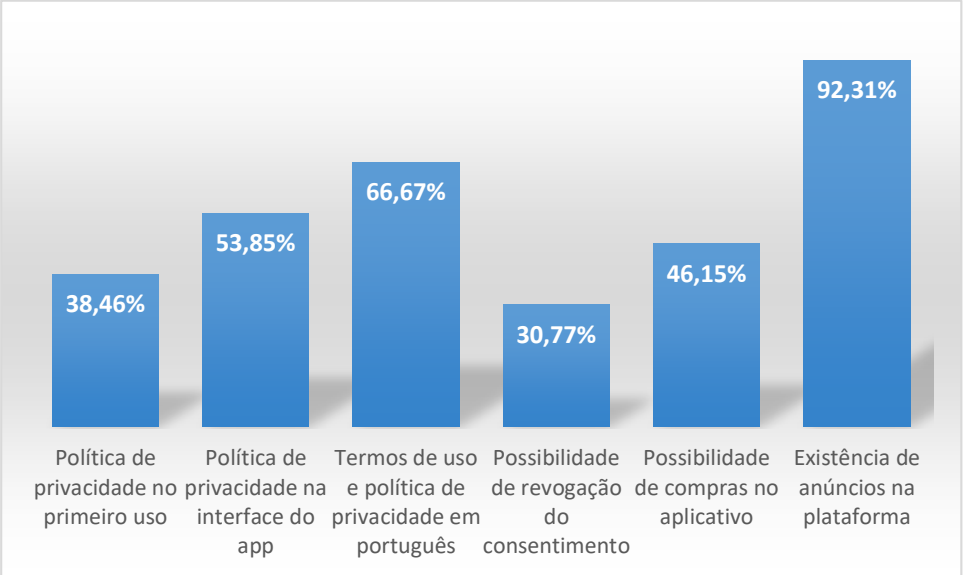

Figura 14 – Estatísticas análise consentimento na categoria "*Notícias e revistas*"

9. Turismo, locais, mapas e navegação

O *Cabify* exibe, em sua primeira tela, o aviso de que, "ao continuar, o usuário aceita a política de privacidade e os termos e condições", ambos escritos em português. Quando da tela de verificação do número do celular, o aplicativo informa utilizar a tecnologia Account Kit, do *Facebook*. Ou seja, ao ali inserir o número, os dados do usuário já são compartilhados com a plataforma *Facebook*, o que pode ser indesejável para o usuário e parece inadequado aos preceitos da LGPD.

Segundo o aplicativo, há a possibilidade de a verificação ser feita por SMS – e não pelo *Facebook* –, mas não há maiores informações de como isso ocorreria. Mas, com o envio do código verificador, a tela seguinte indica que continuar significa "aceitar os termos, a política de dados e o uso de cookies do *Facebook* e a política de privacidade e os termos de serviço do *Cabify*".

Nesse caso, parece haver uma espécie de *venda casada* dos aplicativos, o que é peculiar e parece inadequado à luz da LGPD. Na tela seguinte, o aplicativo solicita permissão de acesso à localização do dispositivo, o que é natural para a funcionalidade oferecida. No menu de configurações, não parece haver qualquer possibilidade de revogação dos consentimentos.

O *Uber*, em sua primeira tela, requer acesso à localização do aparelho, mas é possível negar. Na tela inicial, não há qualquer menção à política de privacidade e aos termos de privacidade do aplicativo, mas essas informações são encontradas, em português, no menu de configurações do *software*.

Embora haja, no menu, uma opção expressa de privacidade – "controle as informações que você compartilha com a gente" –, ela parece ser inócua, na medida em que só permite a revogação do próprio acesso à localização. Ou seja, nada além do estritamente esperado para o tipo de funcionalidade disponibilizada.

O *99*, em sua primeira tela, requer acesso às "fotos, mídia e arquivo do dispositivo", à "localização" e ao fazimento e gerenciamento de chamadas telefônicas, todas vinculadas, ou seja, impassíveis de negativa. Todos os comentários sobre políticas de privacidade e termos de privacidade aplicáveis ao *Uber* também servem aqui.

Nesse ponto, contudo, não há qualquer revogação de consentimento possível. Em verdade, a única manobra de privacidade que se pode fazer é esconder o número do telefone para o motorista, o que, *a priori*, não parece tão relevante para a tutela específica da privacidade do usuário a nível macro, especialmente no sentido de possível compartilhamento dos dados para fora do contexto em que coletados.

O *Airbnb* exibe, em sua primeira tela, o aviso de que, "ao continuar, o usuário aceita a política de privacidade e os termos e condições", ambos escritos em português. Na página seguinte, há uma etapa interessante do consentimento: o usuário deve concordar em "tratar todas as pessoas da comunidade do *Airbnb* com respeito e sem julgamentos ou preconceitos, independentemente de sua raça, religião, nacionalidade, etnia, deficiência, sexo, identidade de gênero, orientação sexual ou idade". Nas configurações, entretanto, não é possível revogar nenhum consentimento fornecido.

O *Booking* e o *Tripadvisor* têm idêntico funcionamento, com a única exceção de que não foi possível encontrar os termos de privacidade e a política de privacidade após a criação de uma conta (nas configurações do aplicativo), mas apenas na etapa inicial, sendo todos escritos em português. O *TripAdvisor* solicita permissão expressa de acesso à localização dos dispositivos – para melhorar as suas funcionalidades –, mas é possível recusá-la.

O *Decolar*, por sua vez, não mostra os termos de privacidade e sua política de privacidade quando do uso inicial do aplicativo, mas, na tela seguinte, solicita permissão de acesso à localização do dispositivo, o que é possível recusar. Nas configurações, é possível acessar tais documentos, todos escritos em português.

Logo ao iniciar, o *Skyscanner* exibe o aviso seguinte: "Seus dados. Suas escolhas. Coletamos informações sobre como e quando você usa nosso aplicativo. Isso nos ajuda a oferecer a melhor experiência possível e a personalizar o que exibimos, inclusive anúncios. Os terceiros de nossa confiança coletam informações semelhantes para melhorar seus serviços e exibir anúncios relevantes para você". Na mesma tela, é possível acessar a política de *cookies*,

inteiramente em português, e gerenciar as configurações de privacidade, podendo revogar, desde logo, a personalização dos anúncios pela leitura das informações coletadas.

O *Trivago* não exibe suas políticas de privacidade e termos de privacidade quando do primeiro uso, mas é possível encontrar essas informações no menu de configurações, em português. Também não é possível revogar qualquer permissão – ao menos sem proceder à criação de uma conta, que não é o objetivo deste trabalho.

O *Google Street View* tem funcionamento idêntico, com a única exceção de que as políticas de privacidade encontradas em suas configurações são abrangentes e aplicáveis a quase qualquer produto *Google*. Trata-se da tradicional dificuldade em fazer a análise das aplicações da empresa em razão de ela ser a provedora do sistema operacional *Android* e, por consequência, vincular as informações ao próprio *Gmail*, por padrão. Essa vinculação automática, aliás, parece perniciosa, pois não foi dada qualquer opção prévia de obstar o *login* com o e-mail já vinculado ao celular.

O *Google Earth* e o *Google Maps*, apesar de terem o funcionamento semelhante ao *Street View*, são mais transparentes no que tange às políticas de privacidade e aos termos de privacidade, na medida em que ambos são disponíveis – e especificamente relacionados ao produto – na aba de configurações da ferramenta, sendo todos os textos em português. Contudo, também não é possível revogar qualquer permissão. No que tange especificamente ao *Google Maps*, a opção de revogação seria particularmente relevante, na medida em que o aplicativo informa exibir anúncios em sua plataforma.

Ao inicializar, o *Waze* solicita expresso fornecimento de acesso à localização do aparelho, o que é natural e aceitável para a funcionalidade oferecida. Na tela seguinte, é solicitada a aceitação dos termos de privacidade e da política de privacidade, ambas escritas em inglês. A aceitação nesse momento é vinculada.

Nas configurações do aplicativo, é possível revogar a permissão de personalização dos anúncios, o que, teoricamente, impediria as consequências da publicidade comportamental. Não é feita qualquer ressalva no sentido de que a revogação implicaria a cessação da coleta dos dados do usuário – e, se essa não for a consequência, não parece haver muito sentido na revogação. Também é possível "ficar invisível no mapa" e revogar algumas permissões de comunicação com o *Facebook*. O escopo das revogações parece, portanto, amplo e, dada a média dos outros aplicativos analisados, aderente à tutela da privacidade que se entende como adequada.

O *Maps.ME*, em sua tela inicial, solicita acesso ao armazenamento e à localização do dispositivo, "para que possa transferir mapas, ver locais e o trânsito próximo e utilizar a

navegação", de modo vinculado, ou seja, não é possível recusar. A transparência, contudo, é aderente à tutela da privacidade que se entende como adequada, na medida em que se explica exatamente ao usuário a funcionalidade daquela permissão que ele está concedendo.

Por outro lado, não são exibidas a política de privacidade e a cópia dos termos de privacidade, sequer nas configurações da plataforma. Contudo, é possível revogar a "recolha de estatísticas de utilização anônima do aplicativo" e a existência de aplicativos, desde que se faça o pagamento de uma quantia anual "simbólica" (R$ 14,79). Mas não há informações sobre o fato de esse pagamento eventualmente também implicar a vedação ao recolhimento das informações, o que seria o ideal. Na omissão, é de se assumir que só implicaria a vedação à exibição dos anúncios – ou seja, as informações continuariam sendo coletadas, mas não para a finalidade de publicidade comportamental dentro do aplicativo específico.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos catorze aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

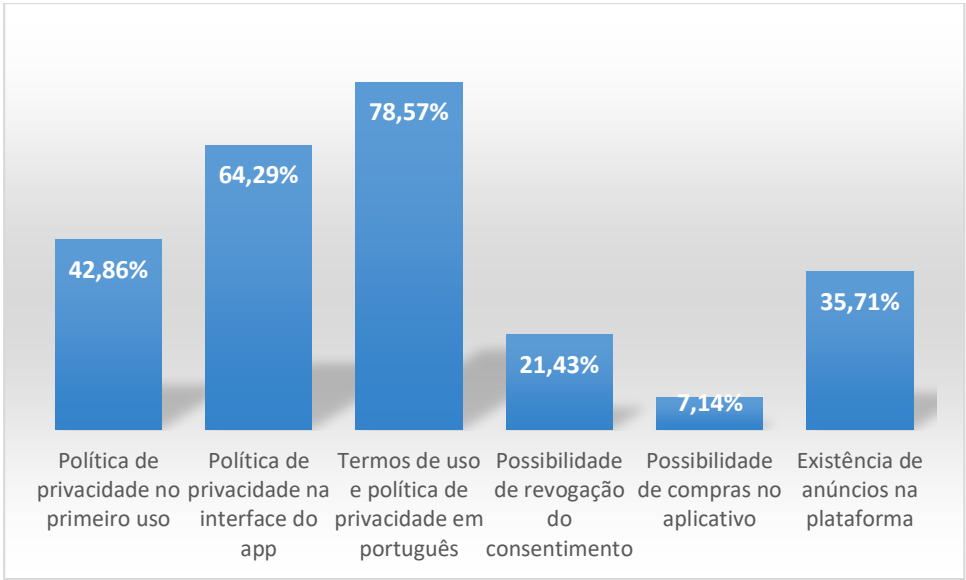

Figura 15 – Estatísticas análise consentimento na categoria "*Turismo, locais, mapas e navegação*"

10. Educação

O *Duolingo* não exibe qualquer política de privacidade quando da abertura do aplicativo e também não foi possível encontrar qualquer referência a ela nas configurações do *software*. Da mesma forma, também não foi possível revogar qualquer consentimento

previamente concedido de modo automático. E, durante o curto período de utilização, foram exibidos diversos anúncios publicitários, o que demonstra algumas lacunas no bojo da proteção de dados que se sustenta como adequada.

Na página inicial do *Babbel*, há o aviso de que, ao prosseguir, o usuário concorda com a política de privacidade e os termos de serviço, cujos links remetem a materiais escritos em português. Apesar disso, também não é possível qualquer espécie de revogação de consentimento nas configurações do aplicativo. O aplicativo, ao menos, informa não exibir anúncios em sua plataforma.

O *TED* não exibe qualquer informação sobre privacidade quando do primeiro uso do aplicativo, mas, dentro da plataforma, é possível acessar as políticas de privacidade, inteiramente escritas em inglês, mas sem qualquer possibilidade de revogação do consentimento implícito e geral fornecido, embora haja clara afirmação de existência de anúncios no *software*.

Ao iniciar, o *Khan Academy* solicita permissão expressa de acesso aos contatos, que é vinculada (não há possibilidade de recusar), mas não há qualquer exibição das políticas de privacidade. Dentro das configurações do aplicativo, é possível acessar a referida política e os termos de serviço, cujos links remetem a materiais escritos em português e inglês, respectivamente. Contudo, também não é possível qualquer espécie de revogação de consentimento nas configurações do aplicativo. Ao menos, não há anúncios na plataforma. Contudo, não parece aderente ao mínimo privilégio o acesso aos dados dos contatos do usuário.

De modo muito similar, funciona o *Khan Academy Kids*, que, quando de sua inicialização, solicita permissão expressa de acesso ao microfone, que é vinculada. A diferença aqui reside no fato de que a política exibida no aplicativo é escrita em inglês, o que é avesso às normas da LGPD de transparência ativa para o público infantil. Contudo, deve-se temperar tal crítica pela percepção de que, em sua maioria, os usuários do aplicativo são estrangeiros. Por outro lado, não merece temperamento a crítica ao fato de o acesso ao microfone ser vinculado e abrangente, sendo que o mais adequado à tutela exposta na LGPD é que só se requeressem esses acessos mais sensíveis no momento da efetiva necessidade do dado.

Ao iniciar, o *Kahoot!* exibe seus termos de privacidade e de privacidade, ambos em inglês. Não é possível, contudo, fazer qualquer revogação do consentimento geral e implícito dado ao início, quando do próprio *download* da ferramenta.

Por sua vez, a página inicial do *Google Classroom* estabelece que, “ao participar, você concorda em compartilhar dados de contato com as pessoas da sua turma”. Contudo, não foram encontradas quaisquer informações mais detalhadas sobre as políticas de privacidade e

os termos de privacidade, sequer nas configurações do aplicativo. Por consequência, não se vislumbrou modo de revogação de consentimento, embora o aplicativo informe não exibir anúncios patrocinados em sua plataforma.

A seu turno, o *Brainly* permite o uso do aplicativo – até certo ponto, imagina-se – sem o cadastro. Ao tentar empreendê-lo, o usuário é informado das políticas de privacidade, inteiramente escritas em português. Como não se procedeu ao cadastramento, contudo, não foi possível aferir o funcionamento da aplicação no tocante aos demais critérios.

Por fim, o *Google Tradutor* não exibe qualquer informação, não disponibiliza os seus termos de uso e de privacidade de modo fácil e intuitivo e, por consequência, obsta qualquer possível revogação de consentimento. Talvez isso se deva ao fato de que, como os dispositivos utilizados para o estudo continham sistema operacional *Android*, a configuração automática do sistema já implica importação de todos os dados da conta *Gmail* vinculada ao aparelho.

Contudo, isso denota falta de transparência para com o usuário, especialmente porque parece partir-se de um consentimento amplíssimo prévio – um consentimento para toda a plataforma *Google*, e não para seus aplicativos específicos –, o que vai na contramão da legislação de regência, que tutela o consentimento específico e balizado pela dinâmica contextual em que coletado o dado pessoal.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos nove aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

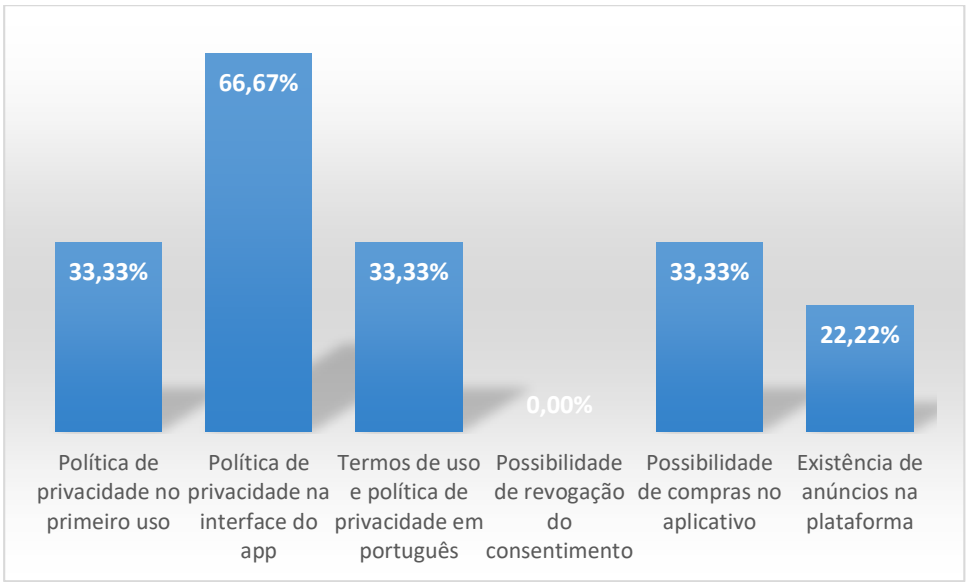

Figura 16 – Estatísticas análise consentimento na categoria "*Educação*"

11. Produtividade e antivírus

Logo na primeira abertura do aplicativo *WPS Office*, aparece um "lembrete de permissão de privacidade do WPS"[619]. Na mesma página, há um *link* de direcionamento à política de privacidade do aplicativo, inteiramente escrita em inglês. Isso pode ser uma potencial dificuldade dos usuários para um efetivo consentimento informado. Nesse momento inicial, contudo, a opção é binária: ou se concorda com tudo, ou não se acessa o aplicativo. Após o aceite, aparece uma solicitação expressa de permissão de acesso às "fotos, mídia e arquivos do dispositivo". Ao negar a permissão, aparece uma mensagem no sentido de que o aplicativo não funcionará.

Ou seja, não se trata de uma verdadeira opção de permissão, mas de um mero aceite. Ao menos, há certa transparência em exibir a caixa de *check*, o que corrobora para um consentimento mais informado. Ao buscar pelas configurações de privacidade do aplicativo, é possível alterar a permissão inicial para a coleta de dados, recusando a futura operação e eliminando os dados já coletados.

No que tange às configurações de publicidade, há opções pré-marcadas de compartilhamento de hábitos de navegação com os parceiros *Google* e *Facebook*, com o suposto fim de saber no que o usuário está interessado. É possível, contudo, desabilitar esse compartilhamento. A crítica, nesse ponto, subsiste quanto ao fato de as opções serem previamente selecionadas, talvez por causa do consentimento geral, inicial e vinculado do usuário ao abrir o aplicativo pela primeira vez. Ao menos, contudo, é possível, em tese, revogar as permissões que impliquem publicidade comportamental e coleta mais abrangente dos dados.

Ao iniciar o uso do aplicativo *Polaris Office*, aparece uma solicitação expressa de permissão de acesso às "fotos, mídia e arquivos do dispositivo". Ao negar a permissão, aparece uma mensagem no sentido de que o aplicativo não exercerá suas funcionalidades máximas, mas, ainda assim, é possível usá-lo com a recusa, apesar de persistir um *banner* no canto inferior da tela solicitando incessantemente a permissão.

Ao buscar pelas configurações de privacidade do aplicativo, há um *link* de direcionamento à política de privacidade do aplicativo e ao contrato de uso do aplicativo, inteiramente escritos em inglês. Não foi encontrada, contudo, nenhuma forma fácil e intuitiva

---

619 "Nós (ou com nossos parceiros) recomendaremos anúncios para você com base em seus interesses. Para acompanhar a conversão de anúncios, nós (ou com nossos parceiros) podemos coletar seus registros operacionais ou endereços IP. Você tem o direito de retirar seu consentimento por meio das configurações de anúncio".

de revogar permissões de acesso aos dados e de seu compartilhamento com terceiros, o que denota inadequação às normas da LGPD.

Ao iniciar o aplicativo *MS Word*, aparece a mensagem típica de um contrato de adesão: "Ao usar este aplicativo, você concorda com os termos de privacidade", cujo link direciona para uma página escrita em português. Não há, previsivelmente, como recusar nenhuma das cláusulas.

Sem haver um prévio cadastro com criação de conta nos servidores da *Microsoft*, não foi encontrada nenhuma forma fácil e intuitiva de revogar permissões de acesso aos dados e de seu compartilhamento com terceiros. Nesse ponto, contudo, é relevante pontuar que o aplicativo informa não promover anúncios na plataforma, o que pode indicar que as informações porventura coletadas realmente não são compartilhadas, mas deveria haver maior transparência.

Ao inicial o *Adobe Reader*, o usuário se depara com a mensagem: "A Adobe coleta dados de análise para melhorar sua experiência". Nesse momento inicial, não há como revogar essa permissão geral, mas, por padrão, o aplicativo informa não ter acesso aos contatos, à câmera e à memória do dispositivo – dados que podem ser voluntariamente fornecidos pelo usuário na aba de configurações do *software*. Ainda dentro do menu de configurações, o usuário consegue revogar a permissão de compartilhamento de informações sobre o uso. Assim, o aplicativo parece alinhado aos ditames da proteção de dados pessoais.

Quanto ao *Google Docs* e ao *Google Drive*, não foi possível aferir como funciona o consentimento inicial da plataforma. Isso se deve ao fato de que, como os dispositivos utilizados para o estudo continham sistema operacional *Android*, a configuração automática do sistema já implica importação de todos os dados da conta *Gmail* vinculada ao aparelho.

Contudo, em uma rápida busca na interface do aplicativo, não foi possível encontrar qualquer remissão às políticas de privacidade ou aos termos de privacidade do *software*, o que denota falta de transparência para com o usuário. Nesse ponto, contudo, é relevante pontuar que os aplicativos informam não promover anúncios na plataforma, o que pode indicar que as informações porventura coletadas realmente não são compartilhadas com terceiros (embora o mero compartilhamento com a *Google*, controladora, já seja suficiente para despertar interesse), mas deveria haver maior transparência.

No primeiro uso do *4Shared*, aparece uma solicitação expressa de permissão de acesso às "fotos, mídia e arquivos do dispositivo". É possível continuar negando a permissão, mas não é informada qualquer consequência da negativa. Na janela seguinte, aparece uma página sobre a declaração de privacidade, cujo link exibe conteúdo inteiramente escrito em

inglês. É possível não dar o consentimento com a política de privacidade nesse momento, mas, na página seguinte, é requisitado que se faça o *login* com as contas *Google*, *Facebook* ou e-mail genérico.

Com a criação da conta, há expresso aceite aos termos de serviço e à política de privacidade, contratos de adesão escritos inteiramente em inglês. Após a criação de uma conta, aparece uma solicitação expressa de permissão que o aplicativo "faça e gerencie chamadas telefônicas", mas é possível negá-la. Na página de configurações, é possível permitir a coleta e uso de dados por terceiros e dar acesso à câmera. Assim, o aplicativo parece razoavelmente alinhado aos ditames da privacidade, já que, apesar da baixa transparência, aparentemente é possível manter a negativa de compartilhamento e acesso a dados e permissões mais sensíveis[620].

No primeiro acesso ao *Dropbox*, o aplicativo solicita a criação de conta ou o *login* com outra já existente, ocasião em que são exibidos links de acesso à política de privacidade e aos termos de serviço do *software*, inteiramente escritos em português. Após a seleção de conta existente, aparece uma página em que o *Dropbox* informa desejar: (i) "ver, editar, fazer download e excluir permanentemente seus contatos"; e (ii) "ver suas informações pessoais, inclusive aquelas que você disponibiliza publicamente".

Apesar de haver o botão "negar", a opção pelo "permitir" é vinculada, já que o aplicativo não funciona caso não se dê tal permissão. Apesar de algumas opções mais sensíveis estarem desabilitadas por padrão – acesso à câmera, por exemplo –, não foi encontrada nenhuma maneira fácil e intuitiva de revogar as permissões concedidas *by standard* (por padrão). Nesse sentido, parece que o que é perquirido *by design* e *by default* não é exatamente a privacidade, mas o seu contrário.

Na página inicial do *Share It*, há o aviso de que, ao prosseguir, o usuário concorda com a política de privacidade e os termos de serviço, cujos links remetem a materiais escritos em inglês. Na sequência, aparecem três solicitações expressas de permissão de acesso às "fotos, mídia e arquivos do dispositivo", além de que o aplicativo "faça e gerencie chamadas telefônicas" e "acesso à localização do dispositivo", só sendo possível negar as duas últimas. Na página de configurações, é possível revogar algumas permissões originalmente pré-

[620] Entretanto, durante o curto período de uso do aplicativo, uma situação peculiar aconteceu: foi exibido um vídeo de propaganda de outro aplicativo, cuja funcionalidade seria a limpeza de arquivos inúteis do celular (concorrente do aplicativo Clean Master, aqui analisado). Talvez isso tenha acontecido justamente pela percepção de que, no fazimento do trabalho, se estava baixando aplicativos semelhantes – e provavelmente teria interesse naquele produto –, o que é típico da publicidade comportamental. O vídeo foi iniciado sozinho e sem qualquer previsibilidade pelo usuário, mesmo com a não concessão inicial das permissões.

concedidas, mas sem muita transparência. Também durante o curto uso desse aplicativo, foi exibido vídeo publicitário.

Na página inicial do *Clean Master*, há o aviso de que, ao prosseguir, o usuário concorda com a política de privacidade e os termos de serviço, cujos links remetem a materiais escritos em português e inglês, respectivamente. Não foram encontradas formas fáceis e intuitivas de revogar as permissões implicitamente concedidas quando do *download* da ferramenta. Porém, para que o aplicativo realmente opere sua função principal – limpar arquivos inúteis do dispositivo –, há pedido de consentimento expresso de alguns acessos.

Na página inicial do *Avast*, há o aviso de que, ao prosseguir, o usuário concorda com a política de privacidade (aqui também política de VPN – rede virtual privada) e os termos de serviço, cujos links remetem a materiais escritos em português e inglês, respectivamente. Na página seguinte, há a opção de comprar uma versão paga do aplicativo ou de continuar na sua versão gratuita, sendo que esta contém anúncios publicitários. Ou seja, aqui parece claro que, para cobrir os custos da ferramenta gratuita, o *software* aposta no lucro gerado com a venda de dados para a publicidade comportamental. De certa forma, essa diferenciação é compatível com o conceito de *níveis de aplicativo* que se deseja implementar neste trabalho.

Na página de configurações, é possível revogar a opção pré-definida de compartilhamento de dados de utilização do aplicativo e do dispositivo com terceiros para análise. O *Avast*, portanto, parece alinhado à tutela da privacidade do usuário. O *AVG* segue exatamente a mesma linha, com a única diferença de que todos os termos são escritos em português.

Na página inicial do *McAfee*, há o aviso de que, ao prosseguir, o usuário concorda com a política de privacidade e os termos de serviço, cujos links remetem a materiais escritos em português. Da mesma forma do que os dois aplicativos anteriores, também é possível seguir em uma versão paga e teoricamente livre de anúncios. Na página seguinte, há pedido expresso de algumas permissões, para ser possível "aproveitar ao máximo o aplicativo".

Dentre elas, há pedidos que envolvem acessibilidade, sobreposição de aplicativos, leitura de uso de aplicativos e acesso à localização. Em um primeiro momento, é possível pular essas concessões. Não foi encontrada nenhuma forma intuitiva e fácil de revogação do consentimento. Nesse aplicativo, há uma ferramenta interessante de análise comparativa da proteção à privacidade em todos os aplicativos instalados no dispositivo. Contudo, os resultados não parecem muito aderente ao esperado, pois todos os *softwares* deste usuário foram classificados como "protege a privacidade conforme a média da categoria". Ou seja, algo inconclusivo.

Em sua primeira página, o *Kaspersky* afirma que, para funcionar corretamente, precisa acessar o armazenamento do sistema ("para verificar o dispositivo quanto a arquivos maliciosos") e o telefone ("para executar o aplicativo e bloquear chamadas feitas por contatos que estão em sua lista negra"). Transparência e clareza, apesar de as concessões serem obrigatórias: não há como continuar sem fornecê-las.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos catorze aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

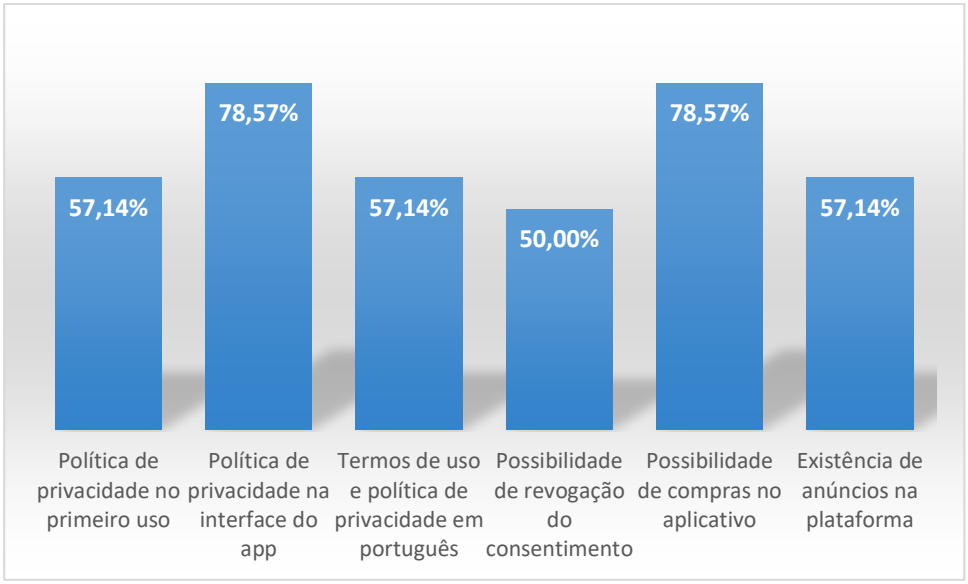

Figura 17 – Estatísticas análise consentimento na categoria "*Produtividade e antivírus*"

12. Governamentais

O aplicativo *FGTS* é o único que solicita, como requisito à sua instalação, a permissão de acesso a determinadas informações. Mesmo assim, contudo, essas informações são menos detalhadas do que as permissões efetivamente concedidas, segundo a própria loja da *Google*. Ao abrir o aplicativo pela primeira vez, é possível selecionar a opção "primeiro acesso" – que, contudo, sequer é o padrão do *software* –, o que levará a uma janela com as cláusulas gerais do contrato, sem qualquer detalhamento. O consentimento, como tradicional, é do gênero binário, tudo ou nada.

O aplicativo *Sisu* não solicita nenhuma informação prévia ao *download* e não informa qualquer aspecto de sua política de privacidade nesse momento. Infelizmente, também não foi possível ver o quão transparente é esse dado durante o uso do aplicativo, na medida em

que o *software* não estava funcionando no momento deste estudo – apenas aparece a mensagem "processo seletivo encerrado".

Os aplicativos *Caixa Trabalhador* e *Bolsa Família*, embora do mesmo desenvolvedor do *FGTS* (a própria *Caixa Econômica Federal*), parecem ter um modo de obtenção do consentimento distinto, pois não há qualquer informação prévia ao *download* e também não há qualquer informação sobre o "primeiro uso". E, mesmo vasculhando as opções dos aplicativos, não há como se acessar qualquer informação sobre a política de privacidade.

O mesmo padrão é seguido pelos aplicativos *e-Título* e *CNH Digital*, justamente dois aplicativos que servem para a exibição eletrônica de documentos que contêm informações pessoais sigilosas. O padrão também é seguido pelos aplicativos *DigiSUS* e *CEB*.

Embora os aplicativos *Sine*, *Caesb* e *Novacap* também sigam o mesmo padrão de não transparência, durante o seu uso prefacial – na primeira página –, é possível clicar em opções que solicitam permissões específicas. No *Sine*, por exemplo, uma das formas de fazer o *login* é por meio de um *QR Code*, o que leva o aplicativo a solicitar a permissão específica de acesso à câmera do celular.

No *Caesb* e *Novacap*, por exemplo, uma das funcionalidades é informar vazamento de água na rua ou informar buraco na rua, o que leva o aplicativo a solicitar permissão específica de acesso à localização do dispositivo. Entende-se que essa metodologia de solicitar permissões específicas para cada funcionalidade, com transparência do efeito da recusa da permissão – se o usuário negar a permissão no *Sine*, por exemplo, aparece a mensagem de falha "*Camera not authorized*" (câmera não autorizada) –, é um bom mecanismo para resguardar a privacidade à luz das balizas da LGPD.

O aplicativo *Meu Imposto de Renda* não solicita nenhuma permissão prévia e não informa nada sobre a política de privacidade antes do *download*. Ao abrir a aplicação pela primeira vez, contudo, aparece a solicitação de acesso a "fotos, mídia e arquivos do dispositivo".

A priori, é possível rejeitar a permissão, mas nada é informado sobre as eventuais consequências disso. Nenhuma outra permissão é solicitada e não há como acessar, de modo intuitivo e simples, a política de privacidade pelo próprio aplicativo. O mesmo acontece com o aplicativo *Denatran*, mas em relação à permissão de acesso à localização do dispositivo.

O aplicativo *Meu INSS* não requer nenhuma permissão prévia ao *download*, mas há opção de acesso à política de privacidade do *software* em sua página inicial. Contudo, o suposto arquivo indexado pela opção está indisponível, ou seja, também não é possível acessar a política de privacidade.

O *Caixa Auxílio Emergencial* não foi passível de análise nesse ponto, uma vez que não exibe sua política de privacidade na plataforma. Em verdade, parece se tratar de um aplicativo de mera consulta de informações, e não de real interação.

No tocante ao *Coronavírus-SUS*, a tela inicial afirma que "a sua privacidade está segura", no sentido de que "o aplicativo não rastreia seus movimentos, não conhece sua identidade, nem a identidade das pessoas com quem entrou em contato". Há, inclusive, uma explicação esquemática sobre como funciona o aplicativo. Na página seguinte, detalha-se a ideia de privacidade segura, ponto a ponto, aparecendo, ao final da tela de rolagem, a política de privacidade e uma opção não pré-selecionada para o usuário marcar que concorda com os termos ali dispostos. A concordância é vinculada.

Após, pede-se o acesso ao *bluetooth* do usuário com a justificativa de que facilitaria o rastreamento das infecções, mas é possível negar. Na página de funcionamento do aplicativo, não se localizou, de modo intuitivo, a política de privacidade, que estava transparente nas telas iniciais.

Dito tudo isso, para facilitar a visualização de como é a obtenção do consentimento nos dezesseis aplicativos analisados, montou-se o seguinte gráfico esquemático, que serve de resumo sobre as principais características observadas:

Figura 18 – Estatísticas análise consentimento na categoria "*Governamentais*"

APÊNDICE B

Tabela 2 – Lista de permissões requeridas pelos aplicativos da categoria "*Comunicação e redes sociais*"

PERMISSÕES	WhatsApp	Signal	Google Meet	Zoom	Facebook	Instagram	Viber	Twitter	Skype	Tinder	Tumblr	Snapchat	WeChat	Telegram	Messenger	LinkedIn	Pinterest
PERMISSÕES DE HARDWARE																	
(Des)Ativar sincronização	X	X			X		X	X	X		X		X	X	X	X	
(Des)Conectar da Wi-Fi	X	X			X	X			X	X		X	X		X		
(Des)Instalar atalhos	X	X			X	X		X			X		X	X	X		
Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*				X	X	X	X					X	X		X		
Controlar NFC	X										X		X		X	X	
Controlar a lanterna/*flash*												X					
Definir papel de parede		X			X		X										
Desativar bloqueio de tela		X					X		X								
Dimensionar papel de parede					X												
Download de arquivos sem conhecimento					X								X		X		
Editar barra de *status*					X												
Enviar SMS	X	X							X					X			
Fazer transmissão	X	X		X	X		X		X				X		X		
Fazer transmissão WAP-PUSH		X															
Fechar outros aplicativos							X										
Gravar áudio	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	
Ler configurações de sincronização	X	X			X		X	X	X		X		X	X	X	X	
Ler estatísticas de sincronização	X						X		X							X	
Ler informações de bateria					X	X									X		

Ler o editor de quadros						X											
Ligar diretamente para números de telefone		X	X	X													
Manter o aparelho ativo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Medir tamanho aplicativo			X					X					X				
Modificar a orientação da tela						X											
Modificar áudio	X	X	X	X	X	X	X		X			X	X	X	X		X
Modificar conectividade à rede		X	X		X		X		X			X			X		
Modificar configurações do sistema	X			X	X		X		X				X				
Parear com *Bluetooth*	X	X	X	X	X		X		X	X		X	X	X	X		
Permitir recepção por Wi-Fi Multicast													X				
Realizar ligações					X	X	X		X					X	X		
Receber SMS	X	X				X			X			X			X		
Rodar ao ligar	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
Tirar fotos e gravar vídeos	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X
Vibrar	X	X		X	X	X	X	X	X	X		X	X	X	X	X	
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO																	
Acessar a localização aproximada	X	X		X	X		X	X	X	X	X		X	X	X		
Acessar a localização precisa	X	X		X	X	X	X	X	X	X		X	X	X	X	X	X
Acessar as contas	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X
Acessar o ID do dispositivo e informações da chamada		X		X													
Acessar o sistema USB de armazenamento de arquivos		X											X				
Acessar os contatos	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X
Acessar sensores corporais (como monitor cardíaco)													X				

Atualizar estatísticas de uso de componentes													X				
Criar contas e editar senhas	X	X	X	X	X		X	X	X		X		X	X	X	X	
Editar agenda e enviar e-mails sem conhecimento		X		X	X												
Editar as contas	X		X	X	X		X	X	X		X		X	X	X	X	
Editar fluxo social							X										
Editar fotos, mídia e arquivos	X				X	X	X	X	X	X	X	X	X	X	X	X	X
Editar memória externa USB	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X
Editar registro de chamadas					X												
Editar SMS		X													X		
Ler a agenda e informações confidenciais		X		X	X										X	X	
Ler configuração de serviço da Google	X		X		X		X	X		X				X	X		X
Ler configurações e atalhos da página inicial													X				
Ler fluxo social							X										
Ler fotos, mídia e arquivos	X				X	X	X	X	X	X	X	X	X	X	X	X	X
Ler memória externa USB	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ler o próprio cartão de contato	X	X			X	X		X	X			X	X	X	X		X
Ler registro de chamadas					X										X		
Ler SMS		X			X				X						X		
Ler *status* do telefone e identidade	X	X		X	X	X	X	X	X			X	X	X	X		
Modificar os contatos	X	X			X		X		X				X	X	X	X	
Receber dados da internet	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X
Recuperar aplicativos em execução	X				X	X	X		X	X			X				

Reordenar aplicativos em execução					X												
Sobrepor outros aplicativos				X	X		X	X	X				X	X	X		
Usar contas do aparelho	X			X		X	X	X	X								X
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	

Tabela 3 – Lista de permissões requeridas pelos aplicativos da categoria "*Navegadores e e-mails*"

PERMISSÕES	**Google Chrome**	**UC Browser**	**Mozilla Firefox**	**Microsoft Edge**	**Gmail**	**Yahoo**	**Outlook**
PERMISSÕES DE HARDWARE							
(Des)Ativar sincronização	X	X	X	X	X	X	X
(Des)Conectar da Wi-Fi		X	X				
(Des)Instalar atalhos	X	X	X	X	X		
Acessar a internet	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*	X	X		X			
Controlar NFC	X		X	X	X		
Controlar a lanterna/*flash*				X			
Definir papel de parede		X					
Desativar bloqueio de tela		X					
Dimensionar papel de parede		X					
Download de arquivos sem conhecimento	X		X	X	X		
Editar barra de *status*		X					
Editar favoritos e histórico da Web	X	X		X			
Excluir dados *cache* do aplicativo		X					
Fechar outros aplicativos		X					
Gravar áudio	X		X	X			
Ler configurações de sincronização	X		X	X	X	X	X
Ler estatísticas de sincronização	X	X	X	X	X	X	X
Licença completa para interagir entre usuários		X					
Manter execução eterna do aplicativo		X					
Manter o aparelho ativo	X	X	X	X	X	X	
Medir tamanho aplicativo		X			X		
Modificar áudio	X	X					
Modificar conectividade à rede		X		X			
Modificar configurações do sistema		X	X				
Parear com *Bluetooth*	X	X		X			
Permitir recepção por Wi-Fi Multicast		X					
Rodar ao ligar	X	X	X	X	X	X	X
Tirar fotos e gravar vídeos	X	X	X	X		X	X
Vibrar	X	X	X	X	X	X	X
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO							
Acessar a localização aproximada	X	X	X	X		X	
Acessar a localização precisa	X	X	X	X		X	X

Acessar as contas	X	X	X	X	X	X	X
Acessar o gerenciador de *downloads*		X					
Acessar o sistema USB de armazenamento de arquivos		X					
Acessar os contatos	X	X	X	X	X	X	X
Atualizar estatísticas de uso de componentes		X					
Criar contas e editar senhas		X	X	X	X	X	X
Editar agenda e enviar e-mails sem conhecimento					X		X
Editar as contas	X	X	X	X	X	X	X
Editar *feeds* assinados					X		
Editar fotos, mídia e arquivos	X	X	X	X	X	X	X
Editar memória externa USB	X	X	X	X	X	X	X
Editar registro de chamadas					X		
Ler a agenda e informações confidenciais					X		X
Ler configuração de serviço da Google	X				X		
Ler configurações e atalhos da página inicial		X					
Ler favoritos e histórico da Web	X	X	X	X			
Ler *feeds* assinados					X		
Ler fotos, mídia e arquivos	X	X	X	X	X	X	X
Ler memória externa USB	X	X	X	X	X	X	X
Ler o próprio cartão de contato				X	X		X
Ler registro de chamadas					X		
Ler registro sensível de dados		X					
Ler *status* do telefone e identidade		X		X			
Modificar os contatos					X	X	X
Receber dados da internet	X	X	X	X		X	X
Recuperar aplicativos em execução		X					
Reordenar aplicativos em execução	X			X			
Sobrepor outros aplicativos		X	X				
Usar contas do aparelho	X	X	X	X	X	X	X
Ver conexões à internet	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X	X		X	

Tabela 4 – Lista de permissões requeridas pelos aplicativos da categoria "*Entretenimento, vídeos e músicas*"

PERMISSÕES	**Netflix**	**Globoplay**	**Amazon Prime**	**Likee**	**Twitch**	**Disney+**	**SBT**	**Band**	**GShow**	**RecordTV**	**Now Net e Claro**	**YouTube**	**YouTube Kids**	**TikTok**	**Vigo**	**Shazam**	**Palco MP3**	**Spotify**	**Google Music**	**Deezer**
PERMISSÕES DE HARDWARE																				
(Des)Ativar sincronização		X		X					X			X		X	X	X			X	
(Des)Conectar da Wi-Fi		X		X										X	X		X		X	
(Des)Instalar atalhos														X				X		
(Des)Ligar o aparelho																				X
Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Acessar as configurações do *Bluetooth*		X		X												X		X		
Controlar a lanterna/*flash*				X										X	X					
Controlar NFC												X				X		X		
Desativar bloqueio de tela																				X
Download de arquivos sem conhecimento											X					X				
Executar o trabalho de segundo plano agendado do aplicativo																			X	
Fazer transmissão				X												X		X		X
Fechar outros aplicativos																				X
Gravar áudio	X	X		X	X	X						X	X	X	X	X		X	X	X
Ler configurações de sincronização		X		X					X			X			X	X			X	
Manter o aparelho ativo	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Medir tamanho aplicativo				X								X	X			X			X	
Modificar áudio	X			X										X	X	X		X		X
Modificar conectividade à rede		X										X			X				X	
Parear com *Bluetooth*	X	X		X							X					X		X	X	X
Permitir recepção por Wi-Fi Multicast	X	X																X		
Rodar ao ligar		X	X	X	X	X	X			X	X	X	X	X	X	X	X	X	X	X
Tirar fotos e gravar vídeos		X		X	X							X		X	X	X		X		
Vibrar		X		X					X	X	X	X		X	X	X		X		X

PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO																				
Acessar a localização aproximada		X		X			X		X			X			X	X	X			
Acessar a localização precisa		X		X			X		X	X		X			X	X	X		X	X
Acessar as contas	X	X					X	X	X	X		X	X	X	X	X		X	X	X
Acessar o ID do dispositivo e informações da chamada		X		X																
Acessar os contatos	X			X			X	X	X	X		X	X	X	X	X		X	X	X
Agir como Serviço de Gerente de Conta																			X	
Controle de reprodução de mídia e acesso a metadados																			X	
Criar contas e editar senhas		X							X					X	X	X			X	
Deletar aplicativos																				X
Editar as contas		X							X			X		X	X			X	X	
Editar configurações de exibição do sistema				X																
Editar configurações e atalhos da página inicial														X						
Editar *feeds* assinados																			X	
Editar fotos, mídia e arquivos	X						X	X		X	X	X	X	X	X	X	X	X	X	X
Editar informações sobre programa ou canal de TV		X	X		X	X													X	
Editar memória	X	X		X	X		X	X		X	X	X	X	X	X	X	X	X	X	X

externa USB																				
Gerenciar armazenamento de documentos												X								
Histórico do *app* e do dispositivo				X																
Ler configuração de serviço da Google		X				X			X	X		X	X			X	X		X	
Ler configurações e atalhos da página inicial														X						
Ler *feeds* assinados																			X	
Ler fotos, mídia e arquivos	X						X	X		X	X	X	X	X	X	X	X	X	X	X
Ler informações sobre programa ou canal de TV		X	X		X	X													X	
Ler memória externa USB	X	X		X	X		X	X		X	X	X	X	X	X	X	X	X	X	X
Ler registro sensível de dados															X					X
Ler *status* do telefone e identidade	X	X		X			X			X	X	X		X		X	X	X	X	X
Modificar configurações do sistema															X		X		X	
Obter informações atuais do aplicativo				X																
Receber dados da internet	X	X		X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X
Recuperar aplicativos em execução	X			X					X					X	X					X
Reordenar aplicativos		X		X											X					

em execução																			
Sobrepor outros aplicativos				X	X				X			X	X		X	X			X	
Usar contas do aparelho		X							X	X		X		X	X			X	X	X
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	X

Tabela 5 – Lista de permissões requeridas pelos aplicativos da categoria "*Comer e beber*"

PERMISSÕES	**Ifood**	**Zé Delivery**	**Rappi**	**Uber Eats**	**McDonalds**	**Tudo Gostoso**	**Foursquare**
PERMISSÕES DE HARDWARE							
(Des)Conectar da Wi-Fi	X			X		X	X
Acessar a internet	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*			X		X		X
Controlar a lanterna/*flash*			X				
Controlar NFC							X
Gravar áudio			X		X		
Manter o aparelho ativo	X	X	X	X	X	X	X
Modificar áudio			X				
Parear com *Bluetooth*			X		X		X
Realizar ligações			X	X			
Rodar ao ligar	X		X		X	X	X
Tirar fotos e gravar vídeos	X		X	X	X	X	
Vibrar	X		X	X		X	X
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO							
Acessar a localização aproximada	X	X	X	X	X		X
Acessar a localização precisa	X	X	X	X	X	X	X
Acessar as contas	X					X	X
Acessar os contatos	X		X	X		X	X
Editar fotos, mídia e arquivos	X		X	X	X	X	X
Editar memória externa USB	X		X	X	X	X	X
Ler configuração de serviço da Google	X						X
Ler fotos, mídia e arquivos	X		X	X	X	X	X
Ler memória externa USB	X		X	X	X	X	X
Ler o próprio cartão de contato			X				
Ler *status* do telefone e identidade	X		X		X		
Receber dados da internet	X	X	X	X	X	X	X
Recuperar aplicativos em execução						X	
Sobrepor outros aplicativos	X	X	X				
Usar contas do aparelho			X				
Ver conexões à internet	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X	X	X	X	X
Verificar licença da Google Play						X	

Tabela 6 – Lista de permissões requeridas pelos aplicativos da categoria "*Infantis e jogos*"

PERMISSÕES	Garena	Subway Surfers	Meu Talking Tom 2	Pou	Fifa	Angry Birds	Candy Crush	Demo Minecraft	Minecraft	Pokémon Go	Fruit Ninja	GTA	Paint Pop 3D	Buddy Toss	Hopping Ball
PERMISSÕES DE HARDWARE															
(Des)Conectar da Wi-Fi	X													X	
Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*				X						X					
Fazer transmissão	X														
Fechar outros aplicativos	X														
Gravar áudio	X		X	X											
Ler informações de bateria	X														
Manter o aparelho ativo	X	X	X	X	X	X	X			X	X	X	X	X	
Modificar áudio	X														
Modificar conectividade à rede	X													X	
Modificar configurações do sistema	X														
Parear com *Bluetooth*	X			X						X		X			
Programar alarme													X		
Rodar ao ligar	X									X	X				X
Tirar fotos e gravar vídeos										X					
Vibrar	X	X			X			X	X	X		X	X		X
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO															
Acessar a localização aproximada										X					
Acessar a localização precisa										X			X		
Acessar as contas					X	X		X	X	X		X			
Acessar os contatos								X	X						
Editar fotos, mídia e arquivos	X	X		X		X		X	X	X	X	X	X	X	
Editar memória externa USB	X	X		X		X		X	X	X	X	X	X	X	

Ler fotos, mídia e arquivos	X	X		X		X		X	X	X	X	X	X	X	
Ler memória externa USB	X	X		X		X		X	X	X	X	X	X	X	
Ler *status* do telefone e identidade	X			X				X	X		X				
Receber dados da internet	X	X	X		X	X	X	X	X	X	X		X	X	
Recuperar aplicativos em execução	X	X													
Reordenar aplicativos em execução															X
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X	X	X		X				X	X	X	X	X
Verificar licença da Google Play	X	X			X			X	X			X			

Tabela 7 – Lista de permissões requeridas pelos aplicativos da categoria "*Finanças e crédito*"

PERMISSÕES	**Banco do Brasil**	**Picpay**	**Caixa**	**Itaú**	**Bradesco**	**Serasa Consum.**	**Santander BR**	**Santander ESP**	**Santander UK**	**Nubank**	**Mercado Pago**	**Digio**	**PayPal**	**Banco Inter**	**Investing**
PERMISSÕES DE HARDWARE															
(Des)Conectar da Wi-Fi					X		X			X					
(Des)Instalar atalhos		X													
Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*		X			X						X				
Controlar a lanterna/*flash*	X														
Controlar NFC	X				X						X		X		
Desativar bloqueio de tela					X								X		
Fazer transmissão				X											
Gravar áudio				X	X		X				X			X	
Manter o aparelho ativo	X	X		X	X	X	X	X	X	X	X	X	X	X	X
Modificar áudio				X	X						X				
Parear com *Bluetooth*		X		X	X		X				X				
Realizar ligações				X	X		X	X			X	X			
Receber SMS							X								
Rodar ao ligar		X	X	X	X	X	X		X	X			X		
Tirar fotos e gravar vídeos	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Vibrar	X	X	X	X	X			X			X		X	X	X

PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO															
Acessar a localização aproximada	X	X	X	X	X	X	X	X		X	X	X	X	X	
Acessar a localização precisa	X	X	X	X	X	X	X	X		X	X	X	X	X	
Acessar as contas	X		X	X	X		X	X		X	X	X		X	X
Acessar os comandos adicionais de provedores de localização							X								
Acessar os contatos	X	X	X	X	X		X	X	X	X	X	X	X	X	X
Atualizar estatísticas de uso de componentes					X										
Criar contas e editar senhas													X	X	
Editar agenda e enviar e-mails sem conhecimento				X								X			
Editar as contas				X											
Editar configurações de exibição do sistema													X		
Editar fotos, mídia e arquivos	X		X	X	X		X	X	X	X	X	X	X	X	X
Editar memória externa USB	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ler a agenda e informações confidenciais												X			
Ler configuração de serviço da Google	X	X		X	X	X	X			X	X		X		
Ler fotos, mídia e arquivos	X		X	X	X		X	X	X	X	X	X	X	X	X
Ler memória externa USB	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ler o próprio cartão de contato											X		X		
Ler registro sensível de dados							X			X					
Ler SMS							X								
Ler *status* do telefone e identidade	X	X	X	X	X	X	X	X	X		X	X	X	X	X
Modificar configurações do sistema													X		
Modificar contatos							X						X		
Receber dados da internet	X	X		X	X	X	X	X	X	X	X	X	X	X	X
Recuperar aplicativos em execução					X		X								
Sobrepor outros aplicativos	X		X	X	X	X	X								
Usar contas do aparelho				X							X				
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X		X	X	X	X	X	X	X	X	X		X

Tabela 8 – Lista de permissões requeridas pelos aplicativos da categoria "*Compras*"

PERMISSÕES	Mercado Livre	Enjoei	Shopee	Wish	OLX	Magazine Luiza	AliExpress	Amazon	Americanas	Ebay
PERMISSÕES DE HARDWARE										
(Des)Conectar da Wi-Fi			X		X		X	X		
(Des)Instalar atalhos								X		
Acessar a internet	X	X	X	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*	X		X					X		
Controlar a lanterna/*flash*								X	X	
Controlar NFC			X	X						X
Gravar áudio			X				X	X		
Manter o aparelho ativo	X	X	X	X	X	X	X	X	X	X
Modificar conectividade à rede							X			
Parear com *Bluetooth*	X		X					X		
Permitir recepção por Wi-Fi Multicast										
Realizar ligações	X					X				
Rodar ao ligar		X	X	X	X		X		X	X
Tirar fotos e gravar vídeos	X		X	X		X	X	X	X	X
Vibrar	X	X	X	X	X	X	X	X	X	X
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO										
Acessar a localização aproximada	X		X			X		X		
Acessar a localização precisa	X	X	X	X	X	X		X	X	X
Acessar as contas		X		X				X	X	
Acessar os contatos	X		X	X				X	X	
Criar contas e editar senhas								X	X	
Editar agenda e enviar e-mails sem conhecimento		X								
Editar as contas								X	X	
Editar configurações de exibição do sistema							X			
Editar fotos, mídia e arquivos	X			X	X	X	X	X	X	X
Editar memória externa USB	X	X	X	X	X	X	X	X	X	X
Ler a agenda e informações confidenciais		X								
Ler configuração de serviço da Google	X		X	X	X	X			X	X
Ler configurações e atalhos da página inicial								X		
Ler fotos, mídia e arquivos	X			X	X	X	X	X	X	X
Ler memória externa USB	X	X	X	X	X	X	X	X	X	X
Ler *status* do telefone e identidade			X				X	X	X	
Modificar configurações do sistema							X			
Receber dados da internet	X	X	X	X	X	X	X	X	X	X
Recuperar aplicativos em execução							X			
Reordenar aplicativos em execução	X									
Sobrepor outros aplicativos			X				X		X	
Usar contas do aparelho								X	X	
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X		X		X	X	X	

Tabela 9 – Lista de permissões requeridas pelos aplicativos da categoria "*Notícias e revistas*"

PERMISSÕES	G1	Folha de SP	UOL Notícias	El País	CNN	Fox News	NY Times	Le Figaro	Le Monde	BBC	Der Spiegel	The Guardian	Flipboard
PERMISSÕES DE HARDWARE													
(Des)Ativar sincronização	X								X	X			
Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*									X				
Ler configurações de sincronização	X								X	X			
Manter o aparelho ativo	X	X	X	X	X	X	X	X	X	X	X	X	X
Modificar áudio					X								
Parear com *Bluetooth*			X						X				
Rodar ao ligar		X	X	X	X	X	X	X					
Tirar fotos e gravar vídeos							X						
Transmitir infravermelho					X								
Vibrar	X	X	X		X	X	X	X	X	X	X	X	
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO													
Acessar a localização aproximada	X		X			X	X	X				X	
Acessar a localização precisa	X		X										
Acessar as contas	X	X	X	X				X	X	X		X	X
Acessar os contatos	X	X	X	X				X	X	X		X	X
Criar contas e editar senhas	X								X	X		X	
Deletar aplicativos													
Editar as contas	X								X			X	
Editar fotos, mídia e arquivos			X	X	X	X		X	X		X		X
Editar informações sobre programa ou canal de TV						X							
Editar memória externa USB			X	X	X	X		X	X		X		X
Ler configuração de serviço da Google	X												X
Ler fotos, mídia e arquivos			X	X	X	X		X	X		X		X
Ler informações sobre programa ou canal de TV						X							
Ler memória externa USB			X	X	X	X		X	X		X		X
Ler *status* do telefone e identidade								X					
Receber dados da internet	X	X	X	X	X	X	X	X	X	X	X	X	X
Recuperar aplicativos em execução	X							X					
Reordenar aplicativos em execução					X							X	
Sobrepor outros aplicativos	X												
Usar contas do aparelho	X												
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X	X	X	X	X	X		X		X	

Tabela 10 – Lista de permissões requeridas pelos aplicativos da categoria "*Turismo, locais, mapas e navegação*"

PERMISSÕES	Uber	99	Cabify	Google Maps	Maps.ME	Waze	Trivago	Decolar	Booking	TripAdvisor	Airbnb	Skyscanner	Street View	Google Earth
PERMISSÕES DE HARDWARE														
(Des)Ativar sincronização				X		X			X					
(Des)Conectar da Wi-Fi	X	X		X	X				X	X	X		X	
(Des)Instalar atalhos				X					X					
Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*	X	X		X		X								
Controlar a lanterna/*flash*		X	X											
Controlar NFC				X					X		X			X
Desativar bloqueio de tela		X		X										
Download de arquivos sem conhecimento		X		X					X					
Enviar notificações de *download*		X												
Enviar SMS	X			X										
Fazer transmissão		X		X		X								
Gravar áudio	X	X		X		X		X			X			
Ler configurações de sincronização				X		X			X					
Ler estatísticas de sincronização						X								
Ler informações de bateria					X									
Manter o aparelho ativo	X	X	X	X	X	X	X	X	X	X	X	X	X	
Medir tamanho aplicativo				X									X	X
Modificar áudio	X	X				X		X						
Modificar conectividade à rede		X											X	
Parear com *Bluetooth*	X	X		X		X								
Programar alarme									X					
Realizar ligações	X			X										
Realizar ligações SIP								X						
Receber SMS	X													
Rodar ao ligar		X	X	X	X	X	X	X	X	X	X			
Tirar fotos e gravar vídeos	X	X	X	X		X		X	X	X	X	X	X	
Vibrar	X	X	X	X		X		X	X		X	X	X	X
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO														
Acessar a localização aproximada	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar a localização precisa	X	X	X	X	X	X	X	X	X	X	X		X	X
Acessar as contas	X			X		X			X	X	X		X	X
Acessar funções avançadas do gerenciador de *downloads*		X												

Acessar o gerenciador de *downloads*		X												
Acessar os comandos adicionais de provedores de localização						X								
Acessar os contatos	X	X		X		X			X	X	X		X	X
Criar contas e editar senhas						X			X	X	X			
Editar as contas	X	X		X		X			X	X	X		X	
Editar fotos, mídia e arquivos	X	X	X	X	X	X	X	X	X	X	X		X	X
Editar memória externa USB	X	X	X	X	X	X	X	X	X	X	X		X	X
Editar registro de chamadas				X										
Ler a agenda e informações confidenciais	X					X	X		X					
Ler configuração de serviço da Google	X		X	X				X	X	X	X		X	X
Ler fotos, mídia e arquivos	X	X	X	X	X	X	X	X	X	X	X		X	X
Ler memória externa USB	X	X	X	X	X	X	X	X	X	X	X		X	X
Ler o próprio cartão de contato	X					X								
Ler registro de chamadas				X										
Ler registro sensível de dados		X												
Ler SMS	X													
Ler *status* do telefone e identidade	X	X		X		X					X			
Modificar configurações do sistema						X								
Modificar contatos				X		X								
Receber dados da internet	X	X	X	X	X	X	X	X	X	X	X	X	X	
Recuperar aplicativos em execução		X		X				X						
Sobrepor outros aplicativos	X	X	X								X			
Usar contas do aparelho	X			X		X		X	X	X	X		X	
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X		X	X		X	X	X	X	X	X	X	

Tabela 11 – Lista de permissões requeridas pelos aplicativos da categoria "*Educação*"

PERMISSÕES	**Duolingo**	**Brainly**	**Babbel**	**TED**	**Khan Academy**	**Khan Academy Kids**	**Google Classroom**	**Kahoot!**	**Google Tradutor**
PERMISSÕES DE HARDWARE									
(Des)Instalar atalhos						X			
Acessar a internet	X	X	X	X	X	X	X	X	X

Acessar as configurações do *Bluetooth*									X
Controlar NFC									X
Gravar áudio	X		X			X			X
Manter o aparelho ativo	X	X	X	X	X	X	X	X	
Medir tamanho aplicativo							X		X
Modificar áudio	X			X					X
Modificar conectividade à rede		X							
Parear com *Bluetooth*									X
Rodar ao ligar	X	X	X	X	X			X	X
Tirar fotos e gravar vídeos	X	X						X	X
Vibrar	X	X	X				X		
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO									
Acessar as contas	X	X	X		X		X		X
Acessar os contatos	X		X		X		X		X
Criar contas e editar senhas	X								
Editar as contas							X		X
Editar fotos, mídia e arquivos	X		X	X	X		X		X
Editar memória externa USB	X	X	X	X	X		X		X
Ler configuração de serviço da Google		X	X				X		X
Ler configurações e atalhos da página inicial						X			
Ler fotos, mídia e arquivos	X		X	X	X		X	X	X
Ler memória externa USB	X	X	X	X	X		X	X	X
Ler SMS									X
Receber dados da internet	X	X	X	X	X		X	X	
Sobrepor outros aplicativos					X				X
Usar contas do aparelho			X		X		X		X
Ver conexões à internet	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X		X	X				X	X

Tabela 12 – Lista de permissões requeridas pelos aplicativos da categoria "*Produtividade e antivírus*"

PERMISSÕES	**MS Word**	**Polaris Office**	**WPS Office**	**Google Docs**	**Google Drive**	**4Shared**	**Dropbox**	**Share It**	**Adobe Reader**	**Clean Master**	**Avast**	**Kaspersky**	**AVG**	**McAfee**
PERMISSÕES DE HARDWARE														
(Des)Ativar sincronização			X	X	X	X	X				X	X	X	X
(Des)Conectar da Wi-Fi		X	X					X		X	X	X	X	X
(Des)Instalar atalhos	X		X	X	X			X		X				
Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar as configurações do *Bluetooth*		X						X			X		X	X
Alterar ou interceptar configurações de rede e tráfego												X		
Controlar NFC			X		X									

Definir aplicativos preferidos												X		
Definir papel de parede								X		X				
Desativar bloqueio de tela								X		X	X		X	X
Download de arquivos sem conhecimento				X	X	X								
Editar barra de *status*								X		X	X	X	X	
Enviar SMS												X		
Excluir dados *cache* do aplicativo								X		X	X		X	
Fazer transmissão						X		X		X				
Fechar outros aplicativos								X		X	X	X	X	X
Gravar áudio								X			X	X	X	
Interagir com o administrador														X
Ler configurações de sincronização				X	X	X	X				X	X	X	X
Ler estatísticas de sincronização				X	X	X								X
Ler informações de bateria										X	X	X	X	X
Manter o aparelho ativo	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Medir tamanho aplicativo	X			X	X			X		X	X		X	X
Modificar as configurações de segurança do sistema											X		X	X
Modificar áudio								X		X	X	X	X	
Modificar conectividade à rede			X					X		X	X	X	X	X
Modificar configurações do sistema								X		X	X	X	X	X
Modificar estado do telefone												X		X
Parear com *Bluetooth*		X						X			X		X	X
Permitir recepção por Wi-Fi Multicast						X								X
Programar alarme	X									X				
Realizar ligações											X	X	X	X
Receber SMS												X		
Redefinir ao padrão de fábrica											X		X	
Reinicializar o aparelho											X		X	
Rodar ao ligar	X	X				X	X	X			X	X	X	X

Tirar fotos e gravar vídeos	X		X		X		X	X	X	X	X	X	X	X
Vibrar	X	X		X	X		X	X	X	X	X	X	X	X
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO														
(Des)Ativar componentes de aplicativos														X
Acessar a localização aproximada						X		X		X	X	X	X	X
Acessar a localização precisa			X			X		X		X	X	X	X	X
Acessar as contas	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar o gerenciador de *downloads*						X								
Acessar os contatos	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Acessar todos os *downloads* do sistema						X								
Acessar todos os serviços Google				X	X									
Atualizar estatísticas de uso de componentes								X		X	X		X	X
Criar contas e editar senhas	X	X		X	X	X	X		X		X		X	
Deletar aplicativos														X
Editar agenda e enviar e-mails sem conhecimento											X	X	X	
Editar as contas	X	X		X	X	X	X		X		X	X	X	
Editar configurações e atalhos da página inicial								X		X				
Editar dicionário				X										
Editar estatísticas de aplicativos														X
Editar favoritos e histórico da Web										X	X	X	X	X
Editar *feeds* assinados				X	X									
Editar fotos, mídia e arquivos	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Editar memória externa USB	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Editar registro de chamadas												X		
Editar SMS												X		
Gerenciar usuários		X												
Ler a agenda e informações confidenciais												X		

Ler configuração de serviço da Google			X	X	X	X					X	X	X	X
Ler configurações e atalhos da página inicial								X		X				
Ler dicionário				X										
Ler favoritos e histórico da Web										X	X	X	X	X
Ler *feeds* assinados				X	X								X	
Ler fotos, mídia e arquivos	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ler memória externa USB	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ler registro de chamadas												X		
Ler registro sensível de dados								X			X	X	X	X
Ler SMS												X		
Ler *status* do telefone e identidade	X					X		X	X	X	X	X	X	X
Modificar os contatos								X			X	X	X	X
Receber dados da internet	X	X	X		X	X	X	X	X	X	X	X	X	X
Recuperar aplicativos em execução		X						X		X	X	X	X	X
Recuperar estatísticas de aplicativos														X
Reordenar aplicativos em execução												X		X
Sobrepor outros aplicativos	X		X					X		X	X	X	X	X
Usar contas do aparelho	X	X		X	X	X			X		X		X	X
Ver conexões à internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Ver conexões Wi-Fi	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Verificar licença da Google Play	X													X

Tabela 13 – Lista de permissões requeridas pelos aplicativos da categoria "*Governamentais*"

PERMISSÕES	**FGTS**	**Coronavírus**	**C. Auxílio Eme.**	**Sisu**	**C. Trabalhador**	**Meu Imposto**	**Bolsa Família**	**e-Título**	**CNH Digital**	**DigiSUS**	**Sine**	**Caesb**	**CEB**	**Novacap Buraco**	**SNE Denatran**	**Meu INSS**
PERMISSÕES DE HARDWARE																

Acessar a internet	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Controlar a lanterna/*flash*								X								
Download de arquivos sem notificação											X					
Licença completa para interagir entre usuários															X	
Manter o aparelho ativo	X	X		X	X	X	X		X	X	X	X	X	X	X	
Parear com *Bluetooth*		X														
Realizar ligações	X											X		X		
Rodar ao ligar		X		X		X				X	X				X	
Tirar fotos e gravar vídeos								X	X		X	X		X		
Vibrar		X		X					X	X	X					
PERMISSÕES DE INFORMAÇÕES PESSOAIS DO USUÁRIO																
Acessar a localização aproximada	X							X		X		X		X		X
Acessar a localização precisa	X				X		X	X		X		X		X	X	X
Acessar as contas	X				X	X	X			X						
Acessar os contatos	X				X	X	X			X						
Editar agenda e enviar e-mails sem conhecimento					X		X									
Editar fotos, mídia e arquivos	X			X	X	X	X	X		X	X	X	X	X	X	X
Editar memória externa USB	X			X	X	X	X	X		X	X	X	X	X	X	X
Ler a agenda e informações confidenciais					X		X									
Ler fotos, mídia e arquivos	X			X	X	X	X	X		X	X	X	X	X	X	X
Ler memória externa USB	X			X	X	X	X	X		X	X	X	X	X	X	X
Ler *status* do telefone e identidade	X					X	X			X	X					
Modificar os contatos										X						
Receber dados da internet	X	X		X	X	X	X		X	X	X	X	X	X	X	
Sobrepor outros aplicativos											X					
Usar contas do aparelho	X				X		X									

Ver conexões à internet	X	X		X	X	X	X	X	X	X	X	X	X	X	X	
Ver conexões Wi-Fi	X				X		X	X		X			X			