DIEGO JOSÉ FERNANDES CABRAL

A investigação criminal nos crimes praticados na internet

Monografia apresentada como requisito para conclusão do curso de bacharelado em Direito do Centro Universitário de Brasília.

Orientadora: Eneida Orbage de Britto Taquary.

BRASÍLIA

2011

A todos os aplicadores do Direito e amantes da tecnologia que não veem uma separação entre essas duas ciências.

Agradeço, primeiramente, ao Senhor Jesus Cristo pela saúde e sabedoria a mim concedidas para que eu concluísse o trabalho.

Agradeço à minha namorada, Carol, que confiou em mim e me socorreu nos momentos mais difíceis demonstrando um amor incondicional.

Agradeço a meus pais, Cabral e Márcia, pelo suporte material e espiritual.

Agradeço a minha orientadora, por todo auxilio e paciência.

Agradeço, finalmente, a todos que de alguma maneira me ajudaram a concluir este trabalho.

“Os que desamparam a lei louvam o perverso, mas os que guardam a lei se indignam contra ele. Os homens maus não entendem o que é justo”

Provérbios 28:4-5a

RESUMO

O presente trabalho tem por objetivo analisar a investigação dos crimes ocorridos via internet a fim de se verificar se há violação de algum princípio constitucional quando da quebra do sigilo dos dados cadastrais dos usuários perante as empresas provedoras. Para tanto, foi estudado o caso concreto relativo ao Universo On Line (UOL), estudos doutrinários e o disposto na legislação e na jurisprudência pertinente ao tema. Tendo sido o mencionado caso o ponto de partida para o presente estudo, levou-se em consideração especialmente os princípios fundamentais da intimidade e do sigilo de dados, aliados ao princípio da supremacia do interesse público sobre o privado. De uma forma geral, foram analisados os aspectos de uma investigação de crimes cometidos via *websites* e como os princípios já citados interferem nessa inquirição. Deste modo, chegou-se a uma conclusão coerente, a qual obedece e respeita os princípios constitucionais, trazidos com tanto zelo pelo legislador constituinte, e também os interesses sociais, importantes para a manutenção do bem estar da sociedade.

PALAVRAS-CHAVE: crimes digitais, princípio da intimidade, princípio da inviolabilidade de dados, princípio da supremacia do interesse público, investigação.

LISTA DE ABREVIATURAS E SIGLAS

CF	Constituição Federal
CPP	Código de Processo Penal
GMT	Greenwich Mean Time
IG	Internet Grátis
IP	Internet Protocol
RISTF	Regimento Interno do Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal
UOL	Universo On Line
UTC	Coordinated Universal Time

SUMÁRIO

INTRODUÇÃO

Trata o presente trabalho de um estudo no âmbito do Direito Processual Penal, atinente à investigação criminal, com enfoque temático nos crimes cometidos via internet e a possível violação à intimidade no tocante à obtenção de dados cadastrais dos usuários junto aos provedores de internet durante a investigação criminal.

A internet e outras novas tecnologias que surgiram com o avanço das ciências eletrônicas permitiram às pessoas acesso universal aos computadores e às informações neles contidas. Assim, embora essa evolução tenha trazido várias contribuições para a sociedade em geral, ela trouxe também diversos impactos, principalmente para a área do Direito, a qual não se encontrava preparada para esse progresso digital.

Como se sabe, o aumento de pessoas usufruindo dos benefícios da rede mundial de computadores tem crescido a cada dia. Em contrapartida, aumenta-se também o número de crimes ocorridos no âmbito virtual.

O problema é que os usuários da internet não têm se preocupado com sua segurança no espaço cibernético, deixando de observar cuidados importantes e tornando-se, assim, alvos fáceis de internautas mal intencionados. Atualmente, há pouca instrução de como se proceder no uso das ferramentas digitais e a quem recorrer quando se for vítima da ação de criminosos.

Como consequência dessa desinformação, muitos usuários estão sendo pacientes de delitos no espaço cibernético. Depois de consumado o crime, é que começam a surgir as dúvidas e conflitos sobre como resolver o caso. Isso porque o crime virtual coloca em tensão direitos e princípios constitucionais como a intimidade do usuário e o interesse do Estado em exercer o *jus puniendi*.

Observe que a investigação policial nos delitos de internet não tem a mesma liberdade nem facilidade que aquelas realizadas fora do mundo virtual. Isso acontece porque,

para que se possa produzir essas provas, é necessário que os prestadores de serviços de acesso e de conteúdo à internet forneçam informações dos cadastros do usuário infrator para que a polícia consiga investigar de maneira eficiente.

Ademais, acaba-se criando uma divergência de interesses, onde de um lado se encontra o Estado, representado pela autoridade policial, que, de acordo com o princípio do interesse público, tem que fazer prevalecer os interesses da coletividade, exercitando suas prerrogativas, e de outro lado, tem-se os usuários da internet, os quais alegam que com a divulgação de seus dados cadastrais para a polícia o seu direito à intimidade estaria sendo violado.

Em primeiro lugar, será exposto um caso prático inspirador do presente trabalho, o qual trata da obtenção de dados de cadastro de determinado usuário perante o provedor Universo *On Line* (UOL) e sua necessidade de autorização judicial, respaldado pelo artigo 5º, incisos X e XII da Constituição Federal. Esse caso apresenta a controvérsia a ser solucionada: a quebra do sigilo dos dados do usuário implicaria uma violação aos direitos fundamentais? Mais precisamente, implicaria uma violação à intimidade e/ou ao sigilo de dados?

Após a exposição do caso, será estudado o inquérito policial, suas características e a sua aplicação no âmbito virtual, mais especificamente, sua utilização nos crimes cometidos via *websites.*

Por fim, será discutida a crise entre os direitos fundamentais criada por esses tipos de delitos com relação à fase investigativa quando da quebra de sigilo de dados pela autoridade policial, juntamente com uma proposta de eventuais conflitos entre esses direitos.

Em se tratando de caso cuja solução está prevista na Constituição da República, e sendo esta o ponto de partida para a pesquisa jurídica ora apresentada, foi necessária a utilização da técnica de pesquisa de levantamento de dados sobre legislação, doutrinas e jurisprudências especializadas que tratam do tema e ajudaram na resolução da questão.

A presente pesquisa foi desenvolvida segundo a forma estrutural de relatório indutivo, por meio do qual objetivou-se apresentar os resultados obtidos ao final do trabalho a partir da apresentação inicial de um caso concreto.

Para maior aprofundamento do tema, o trabalho contém uma ampla análise de doutrinas e jurisprudências especializadas, sendo estruturado em três capítulos, quais sejam: (1) Caso Universo On-Line (UOL); (2) A investigação criminal; e (3) Os princípios e direitos constitucionais envolvidos na decisão do STJ.

1 CASO UNIVERSO ON LINE (UOL)

Para entender melhor a problemática a ser resolvida pelo presente trabalho monográfico, é importante que se conheça o caso concreto que o inspirou. Assim, imperioso se faz o conhecimento do caso relatado na carta rogatória a seguir exposta.

1.1Definição de Carta Rogatória

Em primeiro lugar, cumpre-se definir o que vem a ser Carta Rogatória. A Carta Rogatória nada mais é do que um documento emitido/recebido por países soberanos, consistente em uma solicitação de diligências úteis para o andamento processual de uma ação judiciária em curso em outro país.[1]

Na Rogatória, como o próprio nome já indica, o *jusrogante* (país que emite a carta) roga ao *jusrogado* (país que recebe a carta) a realização de diligências, tais como citações, inquirições, depoimentos e quaisquer outros atos processuais impedidos de ser realizados no país rogante.[2]

Dispõe o artigo 782 do Código de Processo Penal (CPP) que "o trânsito, por via diplomática, dos documentos apresentados constituirá prova bastante de sua autenticidade."

Assim, todos os documentos relacionados à Carta Rogatória deverão tramitar pela via diplomática para que tenham sua autenticidade atestada.

Quando a Carta for expedida pelo Brasil, competirá ao Ministro da Justiça, também pela via diplomática, requerer o seu cumprimento às autoridades do país rogado, após a regular tramitação do processo.[3]

---

[1] OLIVEIRA, Eugênio Pacelli de. Curso de Processo Penal, Rio de Janeiro: Editora Lumen Juis, 2008, p. 772.
[2]Ibidem, p. 772,773.
[3]Ibidem, p. 773.

Ao revés, caso outro país expeça a Carta Rogatória, o cumprimento será feito pelo Presidente do Superior Tribunal de Justiça (STJ), o qual irá conceder o *exequatur* depois de verificada a validade dos documentos.

Nesse sentido, o artigo 784, §1º, do CPP dispõe que:

> As cartas rogatórias emanadas de autoridades estrangeiras competentes não dependem de homologação e serão atendidas se encaminhadas por via diplomática e desde que o crime, segundo a lei brasileira, não exclua a extradição.
> § 1º As rogatórias, acompanhadas de tradução em língua nacional, feita por tradutor oficial ou juramentado, serão, após *exequatur* do presidente do Supremo Tribunal Federal, cumpridas pelo juiz criminal do lugar onde as diligências tenham de efetuar-se, observadas as formalidades prescritas neste Código.

Aqui cabe uma observação no tocante ao órgão judicial competente para a concessão do *exequatur*. Apesar de o artigo acima transcrito fazer referência ao Supremo Tribunal Federal (STF), desde 2005, com a Emenda Constitucional nº 45, essa competência passou a ser do STJ, conforme se observa no artigo 105, I, i da Carta Magna:

> Art. 105. Compete ao Superior Tribunal de Justiça:
> I - processar e julgar, originariamente:
> i) a homologação de sentenças estrangeiras e a concessão de exequatur às cartas rogatórias.

Todavia, no entendimento de Eugênio Pacelli, o Regimento Interno do Supremo Tribunal Federal (RISTF) "deverá permanecer vigente, até que o Superior Tribunal de Justiça altere o seu Regimento, para o fim de incluir a aludida matéria".[4]

A Rogatória, pois, será acompanhada de tradução na língua nacional do país jus rogado, sendo feita por tradutor oficial ou juramentado. Entretanto, se a carta seguir o trâmite da via diplomática no local de origem e for vertida para o vernáculo pelas autoridades diplomáticas, não haverá a necessidade da exigência de um tradutor oficial ou juramentado.[5]

O cumprimento da rogatória, no âmbito das relações internacionais, será de competência da Justiça Federal (art. 109, X da Constituição da República), com a

[4] OLIVEIRA, Eugênio Pacelli de. Curso de Processo Penal, Rio de Janeiro: Editora Lumen Juris, 2008, p. 773.
[5] Ibidem, p. 773.

responsabilidade do Tribunal Regional Federal (TRF), de acordo com o artigo 784, §2º, do Código de Processo Penal. Concedido o *exequatur*, que significa uma ordem para cumprir o que foi determinado, a carta rogatória é remetida ao TRF, para depois ser encaminhada ao Juiz Federal do local de cumprimento.[6]

O artigo 227, parágrafo único, do Regimento Interno do Supremo Tribunal Federal (RISTF), diz que da decisão que conceder ou denegar o *exequatur* caberá agravo regimental. O agravo levará a decisão monocrática do Presidente do Tribunal ao Plenário da Corte. Além do artigo acima referido, o artigo 228, também do mesmo Regimento – RISTF – diz serem possíveis embargos em relação a quaisquer tipos de atos referentes ao andamento da rogatória, em um prazo máximo de dez dias.[7]

Destarte, como visto, em nosso ordenamento jurídico constitucional, para que os atos emanados de órgãos judiciários estrangeiros possam ser executados no Brasil eles dependem de uma prévia verificação do STJ, órgão nacional competente para homologar sentenças estrangeiras e conceder exequatur a cartas rogatórias, as quais, posteriormente, serão encaminhadas para os Juízes Federais para respectiva execução.[8]

1.2 O Caso "Universo On Line (UOL)"

Uma vez tendo elucidado o conceito de carta rogatória, pode-se expor com mais clareza seu conteúdo.

Em 25 de fevereiro de 2004, às 3h20min (horário da Europa Central), um usuário de internet, de identificação desconhecida, cometeu um delito pela rede mundial de computadores, bloqueando o acesso aos sites atendidos pela empresa "Online-forum". Por meio de investigação criminal realizada pela Polícia local, descobriu-se a localização do

[6] OLIVEIRA, Eugênio Pacelli de. Curso de Processo Penal, Rio de Janeiro: Editora Lumen Juris, 2008, p. 773.
[7] Ibidem
[8] ZAVASCKI, Teori Albino. Cooperação Jurídica Internacional e a Concessão de Exequatur. Interesse Público, Belo Horizonte, n. 61, maio/jun. 2010, p. 16.

infrator após rastrearem o seu endereço IP, o qual era identificado pelo número 200.98.154.187.[9]

O IP – sigla de *Internet Protocol* – é um número dado pelo provedor de acesso ao computador quando este se conecta à internet[10]. A atribuição do endereço IP fica registrada nos sistemas do provedor de acesso durante todo o tempo em que o usuário permanece conectado à rede[11]. Esse número irá acompanhá-lo e monitorará a sua trajetória enquanto navegar na internet, possibilitando ao provedor de acesso identificar o momento em que o usuário se conectar e se desconectar da rede. O IP é composto por um conjunto de quatro grupos de três dígitos e no Brasil começa sempre com 200 ou 201. Ex.: IP 200.000.000.000.[12]

A identificação pelo número do IP, no caso acima citado, mostrou que o computador utilizado para o crime se encontrava no Brasil e que o autor do delito utilizava os serviços da provedora de conteúdo e acesso à internet Universo On-line (UOL), a qual foi solicitada a informar os dados cadastrais do infrator à justiça alemã. As informações, embora incompletas, permitem deduzir que o usuário fez o bloqueio dos sites quando usava algum dos serviços da provedora brasileira UOL.

O pedido da quebra de sigilo de dados do investigado foi requerido por meio da Carta Rogatória nº 297 pelo Tribunal da Comarca de Düsseldorf, sediado na República Federal da Alemanha. A investigação tratava de uma "sabotagem informática", conforme consta na tradução do texto rogatório.[13]

---

[9] BRASIL. Superior Tribunal de Justiça. *Carta Rogatória nº 297*, Relator Ministro Barros Monteiro, julgado em 18/09/2006, DJ 29/09/2006.

[10] NOGUEIRA, Sandro D'Amato. *Crimes de Informática*, 2ª Edição, BH Editora e Distribuidora, São Paulo: 2009, p. 72.

[11] BARBAGALO, Erica Brandini, *Contratos Formados por meio de redes de computadores: peculiaridades jurídicas da formação do vínculo*, Editora Saraiva, São Paulo: 2001, p. 34.

[12] Ibidem

[13] BRASIL. Superior Tribunal de Justiça. *Carta Rogatória nº 297*, Relator Ministro Barros Monteiro, julgado em 18/09/2006, DJ 29/09/2006.

Mesmo não estando explícito na decisão do Superior Tribunal de Justiça (STJ), pode-se inferir que a empresa se encontra em territórios germânicos, e por isso a competência para atuar neste caso seria justamente a do Tribunal Alemão.

A Carta Rogatória teve como objetivo auxiliar no inquérito policial que estava sendo realizado pela Polícia da Alemanha, requerendo elementos que apenas a empresa brasileira possuía. Houve a necessidade da cooperação do provedor de internet brasileiro, pois as informações que ele dispunha eram de extrema importância, já que o Universo On Line detinha dados de cadastro do autor, como endereço residencial, telefone, nome completo, registro geral, CEP, armazenados em seu banco de dados.

Porém, quando intimado, o provedor apresentou uma prévia impugnação, dizendo que não iria conceder as informações, pois seria "necessário, primeiramente, a homologação da sentença prolatada pela Justiça rogante, para que possa prestar informações relativas ao usuário em questão".[14]

Além disso, a empresa "invocou o princípio constitucional da inviolabilidade de dados, previsto no art. 5º, XII, da CF/88, que, segundo alega, impede a quebra do sigilo de dados cadastrais".[15]

A provedora Universo On Line alegou que o seu intuito não é obstar as investigações nem deixar de prestar as informações solicitadas, mas que fará isto apenas com expressa autorização judicial.[16]

Por fim, é importante ressaltar que a Carta Rogatória foi declarada pelo STJ como "devidamente motivada, contendo a exposição dos atos ilícitos praticados bem como a conduta da pessoa envolvida".[17]

---

[14]BRASIL. Superior Tribunal de Justiça. *Carta Rogatória nº 297*, Relator Ministro Barros Monteiro, julgado em 18/09/2006, DJ 29/09/2006.
[15]Ibidem
[16]Ibidem
[17]Ibidem

1.3 A Decisão da Carta Rogatória

Ao final, o STJ decidiu que o pedido do Tribunal Alemão de obter os dados cadastrais do usuário infrator não ofende a soberania nacional ou a ordem pública, pois a Constituição, no artigo 5º, incisos X e XII, na verdade veda a quebra do sigilo da comunicação dos dados e não o conhecimento dos dados em si.[18]

Observe-se, pois, que o conteúdo decisório da Rogatória analisada versa sobre uma questão polêmica que tem gerado divergências em alguns julgados da justiça brasileira. Isso porque os crimes cometidos pela internet trazem uma situação jurídica nova para o Direito, situação esta ainda não positivada.

Sabe-se que a sociedade é dinâmica e está em constante transformação, o que dificulta o acompanhamento do sistema jurídico. Sob o prisma dinâmico, o direito se encontra em constante mutação e é lacunoso, pois "não há possibilidade de conter, em si, prescrições normativas para todos os casos".[19] Destarte, é normal se deparar com a falta de regramentos específicos para delitos realizados no mundo virtual, pois "os criminosos são mais rápidos que os legisladores", fato que não é privilégio apenas do Brasil.[20]

Deve-se ressaltar que a maioria das infrações cometidas pela internet encontra tipificação no Código Penal, pois o que as diferenciam dos crimes do mundo físico é somente o meio pelo qual elas se materializam. Assim, torna-se possível usar a analogia em muitos casos, como acontece quando se utiliza analogicamente a tipificação dos crimes contra a honra quando um usuário faz uma injúria – artigo 140 do Código Penal – contra outro em uma rede social.[21]

---

[18]BRASIL. Superior Tribunal de Justiça. *Carta Rogatória nº 297*, Relator Ministro Barros Monteiro, julgado em 18/09/2006, DJ 29/09/2006.

[19] DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro, v. 1: teoria geral do direito civil, 23. ed. rev. e atual. De acordo com o novo Código Civil (Lei n. 10.406, de 10-1-2002) e o Projeto de Lei n. 6.960/2002*, São Paulo: Saraiva, 2006, p. 69.

[20] INELLAS, Gabriel Cesar Zaccaria de. *Crimes na Internet*, 2ª ed. atualizada e ampliada, São Paulo: Editora Juarez de Oliveira, 2009, p. 35.

[21] NOGUEIRA, Sandro D'Amato. *Crimes de Informática*, 2ª Edição, BH Editora e Distribuidora, São Paulo: 2009, p. 72.

Segundo a advogada Patrícia Peck Pinheiro, especialista em Direito Digital,

> não existe um Direito da Internet, assim como não há um direito televisivo ou um direito radiofônico. Há peculiaridades do veículo que devem ser contempladas pelas várias áreas do Direito, mas não existe a necessidade da criação de um Direito específico.[22]

O grande problema reside nas demais situações, como a invasão de computadores para furto de informações pessoais, que não possuem respaldo na legislação penal por falta de tipificação específica. Com isso, paira a dúvida de como serão tratados esses crimes e quais direitos estão sendo violados.

O caso UOL deixa explícita a incerteza gerada pela penalização dos crimes virtuais. A decisão traz a discussão sobre a existência ou não de uma violação da intimidade dos usuários com a quebra do sigilo de seus dados para investigações criminais.

Outra questão levantada é se a autoridade policial deveria ter autorização judicial para a solicitação dos dados ou se ela teria a prerrogativa de requerê-los sem a ordem do Judiciário. Esse questionamento se deve ao fato de as provas produzidas no mundo virtual serem mais frágeis e de mais fácil manipulação do que as provas dos crimes tradicionais, sendo imprescindível se proceder com a máxima celeridade. Nas palavras do delegado da Polícia Federal Elmer Vicente, "em crimes eletrônicos, precisamos dos dados para ontem. As provas materiais desaparecem em questão de horas e, por isso, temos de fazer a previsão do flagrante".[23]

Assim, a questão contida na Carta Rogatória é um assunto que está sendo bastante discutido nos tribunais do Brasil, não sendo ainda pacífico. A situação trazida na Carta Rogatória é um caso emblemático, que representa uma situação na qual muitos casos atuais se enquadram, e por essa razão demanda uma solução menos superficial do que a tratada na referida Carta.

---

[22] PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Saraiva, 2009, p. 30

[23] Por Evelin Ribeiro, do IDG Now!, Publicada em 04 de agosto de 2009 às 18h04, Atualizada em 05 de agosto de 2009 às 13h51. Disponível em < (http://idgnow.uol.com.br/seguranca/2009/08/04/delegados-defendem-acesso-rapido-a-dados-de-internautas-para-investigacoes) >. Acesso em 13 de abril de 2011 às 23h23min.

Observe-se que não se trata apenas de um mero pedido de autorização do juiz para a quebra dos dados. A questão vai além, e envolve o (aparente) conflito entre o direito particular e o direito público, ou seja, de um lado tem-se o direito da intimidade e o sigilo dos dados que protegem os usuários, e do outro se tem o Estado, cujo interesse de punir é refletido por meio do princípio da supremacia do interesse público. A solução deve ir mais afundo e elucidar se os incisos X e XII do artigo 5º podem ser invocados como uma alegação de que a quebra de dados cadastrais junto aos provedores viola a privacidade, devendo também esclarecer se há necessidade de ordem judicial para essa requisição nestes tipos de crimes, sem esquecer que os delitos computacionais possuem uma forma especial de investigação.

2 A INVESTIGAÇÃO CRIMINAL

O Direito Penal tem como objetivo tutelar os bens jurídicos mais importantes, agindo apenas nos casos em que houver lesão aos bens jurídicos fundamentais para a vida em sociedade.[24] O Direito Penal é, pois,

> o ramo do ordenamento jurídico que se ocupa dos mais graves conflitos existente, devendo ser utilizado com a última opção do legislador para fazer valer as regras legalmente impostas a toda comunidade, utilizando-se da pena como meio de sanção, bem como servindo igualmente para impor limites à atuação punitiva estatal, evitando abusos e intromissões indevidas na esfera da liberdade individual.[25]

Como consequência lógica da tutela dos bens jurídicos mais relevantes, cabe ao Estado também promover o esclarecimento dos fatos e das circunstâncias que deram causa a esta infração penal, para que se possa aplicar a sanção ao respectivo delinquente.[26]

Conforme disposição da Carta Magna, compete à polícia civil a realização dessa tarefa, como se percebe no artigo 144, §4º do respectivo Diploma:

> Art. 144.§ 4º - às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a **apuração de infrações penais**, exceto as militares.

Assim, deve as Polícias Civis, dirigidas por Delegados de Polícia de carreira, investigar as infrações penais e sua respectiva autoria, ressalvada a competência da União, além de fornecer às Autoridades Judiciárias os elementos informativos necessários à instrução e julgamento do processo penal.[27]

À essa investigação, dá-se o nome de inquérito policial, o qual, além da previsão constitucional, têm previsão no artigo 4º do Código de Processo Penal - CPP:

> Art. 4º. A polícia judiciária será exercida pelas autoridades policiais no território de suas respectivas circunscrições e terá por fim a apuração das infrações penais e da sua autoria.

---

[24] JESUS, Damásio E. de. *Direito Penal, volume 1: parte geral*. 28. ed. rev. São Paulo: Saraiva, 2005, p. 4.
[25] NUCCI, Guilherme de Souza. *Manual de direito penal: parte geral: parte especial*. 3. ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2007, p. 55.
[26] OLIVEIRA, Eugênio Pacelli de. Curso de Processo Penal, Rio de Janeiro: Editora Lumen Juris, 2008, p. 41.
[27] TOURINHO FILHO, Fernando da Costa. *Manual de Processo Penal*. 11. ed. rev. e atual. São Paulo: Saraiva, 2009, p. 65

Trata-se de procedimento persecutório de caráter administrativo instaurado pela autoridade policial[28], o qual, no entanto, é peça meramente informativa e, por esse motivo, não absolutamente indispensável[29], já que, conforme o artigo 27 do CPP, "qualquer pessoa do povo poderá provocar a iniciativa do Ministério Público, nos casos em que caiba a ação pública, fornecendo-lhe, por escrito, informações sobre o fato e a autoria e indicando o tempo, o lugar e os elementos de convicção".

O inquérito policial – IP, se caracteriza por ser um procedimento escrito, sigiloso, feito por órgãos oficiais (oficialidade), independente de qualquer espécie de provocação (oficiosidade), presidido por uma autoridade pública (autoritariedade), indisponível e inquisitivo.[30]

Importante destacar, dentre todas as características, que o IP é inquisitivo, pois "as atividades persecutórias concentram-se nas mãos de uma única autoridade, a qual, por isso, prescinde, para a sua atuação, da provocação de quem que seja".[31] Além disso, cabe frisar que o IP "é secreto e escrito" e a ele "não se aplicam os princípios do contraditório e da ampla defesa, pois, se não há acusação, não se fala em defesa".[32]

Dispõe ainda o artigo 155 do Código de Processo Penal que:

> Art. 155. O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, **ressalvadas as provas cautelares, não repetíveis e antecipadas**. (**grifou-se**)

Assim, mesmo aquelas provas realizadas sem a observância do contraditório e da ampla defesa, caso sejam cautelares e não repetíveis terão função mais que meramente informativas, possuindo alto valor probatório para a ação penal.

---

[28] CAPEZ, Fernando. Curso de Processo Penal. 16. Ed. São Paulo: Saraiva, 2009, p. 67
[29] TOURINHO FILHO, Fernando da Costa. *Manual de Processo Penal*. 11. ed. rev. e atual. São Paulo: Saraiva, 2009, p. 69
[30] CAPEZ, Fernando. Idem, p. 73-4
[31] Ibidem, p. 74-5
[32] Ibidem, p. 75

2.1 O Inquérito Policial nos Crimes Digitais

Com exceção dos crimes cometidos por hackers - que, de certa forma, podem ser enquadrados nos crimes contra o patrimônio previstos no Código Penal Brasileiro -, os crimes eletrônicos não ficam restritos ao ambiente virtual, e por essa razão não são crimes de fim. Assim, pode-se dizer que os crimes telemáticos são, em princípio, crimes de meio, isto é, utiliza-se de um meio virtual. Isso significa que o meio de materialização do delito pode ser virtual; contudo, em certos casos, o crime não.[33]

A grande parte dos crimes que acontece na rede também acontece no mundo real, com a diferença de que no ambiente virtual a internet é usada como um meio facilitador, pois permite que o infrator permaneça anônimo. Assim a definição para delito é idêntica tanto no Direito Penal quanto no Direito Penal Digital. As novidades na área digital dizem respeito à territorialidade e à investigação probatória, bem como à necessidade de uma legislação especial para tratar de crimes específicos, que, devido às particularidades cibernéticas, merecem uma codificação própria.[34]

Assim como nos crimes comuns, os crimes de informática possuem modalidades diferentes, variando de acordo com o bem jurídico protegido. Pode-se citar como exemplo o crime de interceptação telefônica e de dados, o qual tem como bem jurídico tutelado as informações, vez que estas podem servir de subsídios para o envio de "e-mail bombing"[35], um

[33] PINHEIRO, Patrícia Peck. *Direito Digital*, São Paulo: Saraiva, 2009, p. 225-6.
[34] Ibidem, p. 226.
[35] "Mensagem de correio eletrônico enviada anonimamente ou por um endereço falso, que: (1) Contém códigos que podem bloquear ou danificar dados no computador do usuário que a recebe. (2) É enviada em grande quantidade, podendo travar ou até causar problemas maiores para o computador do usuário que a recebe." (BIANCHI, Adriano Smid. E-dictionary: dicionário de termos usados na internet, São Paulo: Edicta, 2001, p. 117)

"e-mail com vírus", o "spam"[36]. Esse tipo penal também visa proteger a inviolabilidade das correspondências eletrônicas.[37]

Um grande entrave para uma investigação efetiva dos crimes virtuais é a insuficiente quantidade de denúncias e o despreparo dos peritos, policiais e delegados para resolução dessas delinquências, muito embora já seja possível até mesmo a realização de boletins de ocorrência via internet.[38]

Assim, apresenta-se como soberana preocupação a falta de conhecimento a respeito das implicações da informática em questões jurídicas no país ou, talvez, do descaso que as provedoras manifestam a respeito da necessidade de proteção aos bens jurídicos mais relevantes socialmente por meio da crucial atuação da polícia e do Ministério Público no combate aos crimes informacionais.[39] Um exemplo do desapreço dessas empresas é citado pelo promotor de justiça criminal Gabriel Zaccaria de Inellas, ao dizer que

> É de pasmar que a FAPESP[40] bloqueie, *sponte sua*, um registro de domínio, por falta de pagamento, mas crie empecilhos de toda sorte, para efetuar tal bloqueio, diante de um delito praticado através da Internet, exigindo um Mandado Judicial, para efetuá-lo.[41]

Deve-se ainda atentar para o fato de que hoje em dia os delinquentes da rede não serem mais aqueles sujeitos que possuem uma inteligência acima da média, pois hoje em dia a própria *web* fornece os elementos necessários para o cometimento destes delitos,[42] sendo os motivos que levam uma pessoa a cometer estes crimes computacionais diversos: espionagem profissional, quando uma empresa contrata pessoas para invadir os sistemas de seus

---

[36] "ato de enviar indiscriminadamente artigos para grupos de discussão ou e-mails, geralmente com mensagens publicitárias, piadas, correntes de fé, sorte ou dinheiro (sendo que esta última é caracterizada como crime de estelionato) ou informativos, sem a solicitação ou autorização do destinatário." (BIANCHI, Adriano Smid. E-dictionary: dicionário de termos usados na internet, São Paulo: Edicta, 2001, p. 207-208)
[37] PINHEIRO, Patrícia Peck. *Direito Digital*, São Paulo: Saraiva, 2009, p. 226.
[38] Ibidem, p. 228-9.
[39] INELLAS, Gabriel Cesar Zaccaria de. *Crimes na Internet*, 2ª ed. atualizada e ampliada, São Paulo: Editora Juarez de Oliveira, 2009, p. 37.
[40] Fundação de Amparo à Pesquisa do Estado de São Paulo – Órgão responsável pelos registros de domínios no Brasil. Os registros de domínio não feitos através do site Registro.br, mantido pela FAPESP. O Registro.br é o único responsável por registros de domínios brasileiros (.br) e não tem representantes pelo país. (BIANCHI, Adriano Smid. E-dictionary: dicionário de termos usados na internet, São Paulo: Edicta, 2001, p. 123)
[41] PINHEIRO, Patrícia Peck. *Direito Digital*, São Paulo: Saraiva, 2009, p. 37.
[42] Ibidem, p. 228-9.

concorrentes; proveito próprio, que são os crimes mais comuns, como roubo de dinheiro, cancelamento de dívidas e fraude em concursos; vingança, de um ex-funcionário contra uma empresa, por exemplo; curiosidade e aprendizado, justificativa alegada por muitos *Hackers*; busca de aventura, que é o ataque a sistemas avançados; ou mesmo maldade, pelo simples prazer de causar um mal.[43]

Os ciberdelitos, de uma forma geral, demandam a quebra de sigilo dos dados, pois a testemunha destes ilícitos é justamente aquela pessoa que detém os protocolos IP – registros que contêm os elementos das transações realizadas eletronicamente. Além disso, apesar de muitos não aceitarem juridicamente as provas eletrônicas sob a alegação de que são altamente manipuláveis, para serem aceitas em processo são capazes de passar por perícias e análises extremamente rigorosas.[44]

Pelo fato de apresentarem vantagens tais como redução de custos, otimização de decisões e fornecimento de logística, muitos empreendimentos criminosos têm se utilizado dos meios eletrônicos assim como fazem as empresas legalmente constituídas. Uma das primeiras organizações criminosas a perceber o grande potencial das transações eletrônicas foi a Máfia, que utilizou a rede para lavagem de dinheiro, seguida de cartéis de tráfico de drogas, os quais aproveitam as vantagens da *web* para fechar negócios bilionários, sem deixar de fora o "ciber-terrorismo", já praticado por grupos terroristas.[45]

Além do assunto sobre provas visto nos parágrafos acima, outro ponto que gera polêmica é a territorialidade no que tange os crimes telemáticos. O Direito Penal está limitação à uma ação interna em um determinado território, somente podendo atuar externamente se houver acordos entres os países envolvidos. Ademais, mesmo a melhor das investigações pode ser frustrada caso não haja como julgar o autor do delito, seja pelo

[43] NOGUEIRA, Sandro D'Amato. Crimes de Informática, Leme/SP: BH Editora e Distribuidora, 2009, p. 33-4.
[44] PINHEIRO, Patrícia Peck. *Direito Digital*, São Paulo: Saraiva, 2009, p. 230.
[45]Ibidem, p. 232-3.

impedimento de sua extradição ou mesmo pela impossibilidade de julgamento no próprio país de origem.[46]

2.1.1 A investigação criminal dos cibercrimes

Como os crimes informacionais diferem dos demais no seu modo de execução, sua investigação também é diferente e difícil.[47]

As evidências e informações inicialmente coletadas representam o início de toda investigação, seja ela processada em meio físico ou virtual. Embora a hierarquia de provas não faça parte da legislação processual brasileira, a prova pericial acaba prevalecendo no conjunto probatório, o que decorre do fato de a prova pericial ser produzida fundamentada em rigores científicos, sem depender de qualquer tipo de interpretações subjetivas.[48]

Deve-se atentar que a prova eletrônica deverá obedecer a cinco regras: (a) admissibilidade, isto é, a possibilidade de ser utilizada no processo; (b) a autenticidade, que significa a prova ser certa e de importância para o caso investigado; (c) a completude, já que a prova não poderá causa ou levar a suspeitas alternativas; (d) a confiabilidade, pois não devem existir dúvidas quanto a veracidade e autenticidade da prova; e (e) a credibilidade, que representa a clareza, o fácil entendimento e a interpretação dos dados obtidos pericialmente.[49]

O primeiro passo no inquérito policial nos crimes digitais, pois, é identificar o meio utilizado para o delito ocorrido, podendo ser: *website*, mensagens instantâneas, *chats*, grupos de discussão, comunidades virtuais. Essa primeira determinação tem relevância para se restringir as providências a serem tomadas.[50]

---

[46]PINHEIRO, Patrícia Peck. *Direito Digital*, São Paulo: Saraiva, 2009, p. 235-236.
[47]INELLAS, Gabriel Cesar Zaccaria de. *Crimes na Internet*, 2ª ed. atualizada e ampliada, São Paulo: Editora Juarez de Oliveira, 2009, p. 35.
[48] PINHEIRO, Patrícia Peck. Idem, p. 172.
[49] Ibidem, p. 172-3.
[50] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 15.

As evidências dos crimes cibernéticos possuem como características o caráter complexo, a volatilidade, ou seja, fácil alterabilidade, e, a mais importante, o número IP[51], já explicado anteriormente. Por ser uma rede global de computadores, a internet em seus registros indica a hora local e a referência à hora GMT ou UTC[52], sendo que, em alguns casos, apenas é feita menção ao GMT[53]. Quando na solicitação da quebra de sigilo de dados telemáticos feita aos provedores é necessário que o pedido mencione pelo menos três indicadores, que são "a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos".[54]

Dentre os vários meios possíveis para a prática de delitos cibernéticos, sabendo que cada meio demanda uma inquirição distinta, no presente trabalho será considerada a investigação utilizada nos crimes cometidos via *website*, que é o caso do delito relatado na Carta Rogatória em análise.

Para iniciar a investigação criminal, não é suficiente apenas o endereço URL do site que sofreu o ataque, pois, como dito anteriormente, as evidências nos crimes cibernéticos são de fácil manipulação, podendo ser apagadas, modificadas ou perdidas facilmente. Desse modo, é de extrema importância que a *notitia criminis* não esteja desacompanhada da página impressa, e, por isso, deve-se providenciar de maneira urgente sua impressão ou, se possível, o *download* do seu conteúdo.[55]

---

[51]MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 15.

[52] "Coordinated Universal Time (abreviado UTC, e portanto frequentemente escrito como Universal Time Cordinated e às vezes Universal Coordinated Time), ou horário universal coordenado, é o horário padrão comum a todos os lugares no mundo. Anteriormente e ainda amplamente chamado de Greenwich Mean Time (GMT) ou horário médio de Greenwich, e também de World Time (horário mundial), o UTC reflete nominalmente o horário solar médio ao longo do meridiano primo da terra." (THING, Lowell (edição). Tradução de Bazán Tecnologia e Linguistica e Texto Digital. Dicionário de Tecnologia. São Paulo: Futura, 2003, p.183)

[53]MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 15.

[54]Ibidem, p. 15.

[55] Ibidem, p. 18-19.

Quanto aos *downloads*, é importante frisar que já existem programas que facilitam este tipo de trabalho. Um exemplo é o programa HTTrack o qual permite baixar o conteúdo de um site inteiro, inclusive textos e fotos publicadas, quando o sítio possuir um grande volume de dados.[56] Além desse artifício, o programa também gera um arquivo de log[57] (hts_log), o qual registra a data, hora e endereço do site salvo. Isso serve para que se defina o tempo do crime.[58]

Realizados esses procedimentos, todo o conteúdo recolhido pelo referido programa poderá ser encaminhado para o órgão competente por meio de e-mails ou, de preferência, em mídia não regravável.[59]

É importante também manter a integridade dos dados coletados, pois, ao longo da instrução processual penal a defesa poderá impugnar as provas, questionando sua autenticidade. Para prevenir essa problemática, é indicado o uso de softwares como o MD5Sum[60], que garante a integridade dos dados gravados no momento em que a prova foi produzida, com o objetivo de assegurar que nenhum tipo de adulteração ocorreu durante o a persecução penal.[61]

É ainda recomendável que se faça a duplicação da mídia de prova, a fim de que os originais permaneçam conservados até o final do processo para que, em caso de dúvida, estes possam ser reexaminados. Assim, a perícia deverá ser realizada nas cópias e não nas originais,

---

[56] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 19.

[57] "Arquivos de *log*: [...] permitem a reconstituição de fatos que ocorreram no sistema computacional (...). Registram, por exemplo: as atividades do usuário, dos processos e do sistema, as conexões de rede, as atividades da rede e informações específicas dos aplicativos e serviços" (PINHEIRO, Patrícia Peck. *Direito Digital*, São Paulo: Saraiva, 2009, p. 173).

[58] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 19.

[59] Ibidem, p. 19.

[60] "MD5 é um algoritmo (algorithm) usado para verificar a integridade dos dados (data integrity) por meio da criação de uma mensagem 128-bit de entrada de dados (que pode ser uma mensagem de qualquer tamanho) com uma identificação única, como se fosse uma impressão digital de um indivíduo específico." (THING, Lowell (edição). Tradução de Bazán Tecnologia e Linguística e Texto Digital. Dicionário de Tecnologia. São Paulo: Futura, 2003, p. 518)

[61] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 20-21.

para a preservação do que se chama, na computação forense, de *timeline* – ou linha de tempo – que é uma cronologia de eventos relacionados ao caso sob avaliação, pois somente o fato de abrir um arquivo de computador já é capaz de alterar seu estado.[62]

Vale frisar que na internet já se encontram disponíveis não apenas os programas aqui citados, mas também muitos outros de mesma ou melhor qualidade, gratuitos ou pagos.[63]

Depois de obter a prova e assegurar sua inteireza, o próximo passo é identificar o servidor que hospeda, ou hospedou, o site investigado. O imprescindível é saber se o sítio é nacional – se possui a identificação final do ".br" – ou estrangeiro.[64]

No caso dos domínios nacionais, uma pesquisa feita no site www.registro.br ajudará a encontrar informações tais como o nome do responsável por administrar o domínio, o responsável pela área de segurança e o provedor *backbone*[65], que é a empresa que possui o bloco de endereços de IP.[66]

De outro lado, nos domínios estrangeiros há muitas possibilidades de se descobrir o servidor hospedador por meio de serviço de Whois[67], dentre eles http://www.arin.net/ e http://www.internic.net/whois.html, dentre outros.[68] A competência da polícia e da justiça brasileira para investigar os delitos digitais cujo site esteja hospedado em um servidor estrangeiro só será justificável se houver algum brasileiro envolvido.[69] Caso o delito não seja praticado por um brasileiro ou o site não estiver hospedado em provedores nacionais,

---

[62] INELLAS, Gabriel Cesar Zaccaria de. *Crimes na Internet*, 2ª ed. atualizada e ampliada, São Paulo: Editora Juarez de Oliveira, 2009, p. 145-6.
[63] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 22.
[64] Ibidem, p. 23.
[65] "'espinha dorsal, a parte mais importante' (*Michaelis*) – conforme a definição, o backbone é o cabeamento mais importante da Internet, uma infraestrutura de alta velocidade que é a via principal de passagem de informações. Geralmente, temos um backbone ligando um servidor a outro." (BIANCHI, Adriano Smid. E-dictionary: dicionário de termos usados na internet, São Paulo: Edicta, 2001, p. 79)
[66] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. Idem, p. 23.
[67] "Cadastro de um conjunto de usuários com informações pessoais e endereço eletrônico. O nome surgiu da expressão *who is*? (quem é?)." (BIANCHI, Adriano Smid. E-dictionary: dicionário de termos usados na internet, São Paulo: Edicta, 2001, p. 234)
[68] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. Idem, p. 24.
[69] Ibidem, p. 25.

recomenda-se que o fato criminoso seja encaminhado à Interpol[70] ou a um dos *hotlines* ligados à Inhope[71], pois, fazendo isso, a associação filiada será responsável por comunicar o ocorrido à polícia local.[72]

No que diz respeito à Carta Rogatória analisada, a empresa cujo site foi atacado era hospedado em um provedor estrangeiro e seu domínio também o era, no entanto, o suspeito era brasileiro, o que justificou sua emissão e a colaboração da justiça brasileira na resolução do caso.

Após os passos anteriores, chega-se na etapa mais polêmica da investigação: a quebra de dados telemáticos. A etapa seguinte dependerá de o hospedeiro ser um provedor conhecido, o qual pode ou não cobrar remuneração para essa hospedagem, ou de a página estar registrada, no órgão competente para o registro, no nome de uma empresa não conhecida, sendo que, nesse caso, seria necessário analisar cada situação para saber se seria possível requerer a quebra de sigilo de dados sem que o autor da página tomasse conhecimento disto.[73]

Se o hospedeiro, além de conhecido, for brasileiro, a violação de sigilo das informações do usuário infrator deverá ser requerida judicialmente, para que assim ele forneça uma cópia em mídia não regravável das páginas objetos da investigação criminal, assim como os *logs*, ou seja, os registros de criação e alteração da página. O *log* também será importante

[70] "Sigla de *Organization Internaionale de Police Criminelle*, sediada em Paris, é a polícia internacional; o organismo policial que age em vários países, sob uma direção central." (DINIZ, Maria Helena. Dicionário Jurídico, São Paulo: Saraiva, 1998, p. 885.)

[71] É uma associação internacional de linhas de atendimento de denúncias de conteúdos suscetíveis de serem considerados ilegais. Por fim, o inhope presta ainda auxílio à instalação e desenvolvimento de novas linhas de denúncia. <http://www.internetsegura.pt/pt-PT/Sobre/MissaoVisao/ContentDetail.aspx> Acesso em 18/04/2011>. Acesso em 18.04.2011, 9:30.

[72] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 25.

[73] Ibidem, p. 26.

para se encontrar informações referentes ao número IP, à data e à hora da comunicação e à referência ao horário, inclusive com o fuso horário GMT ou UTC.[74]

No caso das páginas *web*, no momento de fornecer o conteúdo solicitado, os provedores costumam apresentar uma lista de IP's e datas, a qual contém a indicação de todas as vezes que a página foi alterada, pois há possibilidade de que outros computadores tenham sido utilizados com o intuito de adulterar o conteúdo da página.[75] É justamente isso que foi solicitado à empresa UOL – provedor conhecido – através da Carta Rogatória em análise.

A identificação dos computadores é feita por meio dos IP's, os quais podem ser estáticos – quando pertencem a pessoas determinadas durante um período determinado de tempo – ou dinâmicos – quando são distribuídos de forma aleatória aos usuários. Para exemplificar o primeiro caso, tem-se as empresas e universidades que possuem uma faixa de IP próprios. No que tange aos usuários domésticos, o usual é a utilização do IP dinâmico, cujo fornecimento será feito por uma operadora de comunicação, que, na maioria das vezes, são provedores de acesso, como UOL, Globo, IG. As informações referentes ao dia e horário em que um endereço IP foi utilizado deverão ser buscadas nas operadoras de comunicação.[76]

Na prática, há muitos questionamentos sobre a quem ou a qual instituição dever-se-á pedir informações sobre a quem pertence o endereço IP. Sabe-se que os números IP's que começam com "200" geralmente pertencem a concessionárias brasileiras. Ao se digitar o número *Internet Protocol* investigado no site www.registro.br o próprio sítio informará o meio pelo qual o usuário se conectou pela internet, o nome do responsável e o endereço para onde o ofício judicial deverá ser remetido[77], se assim for o caso.

---

[74] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 26.
[75] Ibidem, p. 26.
[76] Ibidem, p. 27.
[77] Ibidem, p. 27.

De qualquer forma, caso seja necessária uma futura busca e apreensão do computador, o investigador, de posse dessas informações, poderá requerer a expedição de um mandado judicial para esse fim.[78]

No caso UOL, a investigação foi apenas iniciada. Observe que, provavelmente, a polícia alemã já copiou e salvou o conteúdo do site violado de forma segura. Também já conseguiu identificar o provedor de acesso que forneceu o endereço IP para que o infrator se conectasse a internet, que é o Universo On Line. No entanto, apesar de já ter o número IP, a justiça germânica requereu à brasileira a quebra dos dados telemáticos a fim de se obter o último dado necessário à conclusão do inquérito: a localização do "dono" do referido número *Internet Protocol*.

Importante, por fim, fazer uma pequena observação. Com o advento das redes *Wi-Fi*, que são os sistemas de transmissão de dados sem fio, se tornará mais difícil a identificação do computador utilizado para acessar a rede. Assim, qualquer pessoa que estiver na área de abrangência da rede de conexão emitida pelo ponto de acesso poderá praticar de forma anônima um número incontável de delitos. Isso dificultará cada vez mais o trabalho de investigação policial nos crimes eletrônicos.[79]

Ainda quanto à investigação, cabe destacar a responsabilidade dos provedores quanto ao armazenamento dos *logs* de acesso de seus usuários. Pela completude da discursão, convém citar a opinião do Ministério Público Federal quanto ao tema:

> Para que seja possível identificar qual usuário estava ligado a determinado endereço de IP, num determinado dia e hora, os provedores de acesso e também de hospedagem devem manter um banco de dados eletrônico, uma lista de cada endereço de IP utilizado, juntamente com a correspondente data, horário e região de conexão. A *International Association of Prosecutors* recomenda que os provedores mantenham os *logs* de acesso pelo prazo mínimo de um ano, de forma que, quando forem formalmente requisitados, tenham disponível a informação de interesse do órgão solicitante, inclusive para instruir os casos envolvendo cooperação

[78] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 27.
[79] Ibidem, p. 28.

> internacional, em cujo âmbito as investigações demandam maior tempo para sua conclusão.[80]

Por fim, cite-se que o Brasil já segue neste sentido, tendo elaborado um Projeto de Lei sobre a importância desse armazenamento de dados, o qual facilitará futuras investigações criminais em crimes cometidos via internet, conforme se observa no artigo 22, I, do Projeto de Lei de autoria do Deputado Federal Eduardo Azevedo:

> Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:
> I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

Essa tipificação demonstra um avanço no pensamento do Legislativo nacional, o qual acarretará uma celeridade e maior confiabilidade na justiça brasileira.

[80] MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*, p. 43.

3 OS PRINCÍPIOS E DIREITOS CONSTITUCIONAIS ENVOLVIDOS NA DECISÃO DO STJ

Após saber como se procede a investigação nos crimes digitais, convém analisar os princípios constitucionais nela envolvidos a fim de saber se há violação a alguma deles, que é justamente o problema que o presente trabalho busca solucionar.

3.1 O Direito à Intimidade

Reza o inciso X do artigo 5º da Constituição Federal, que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Note-se que a intimidade recebeu uma especial proteção constitucional, visto que o artigo 5º trata dos direitos fundamentais. Assim, a Carta Magna resguardou um espaço íntimo da vida do indivíduo, intangível por influências ilícitas externas.[81]

Anote-se ainda que a proteção constitucional abrange tanto a intimidade das pessoas físicas quanto das pessoas jurídicas.[82]

É importante, no entanto, diferenciar os conceitos de vida privada, de intimidade e de segredo. Para essa explicação, é útil valer-se da teoria das esferas, a qual ilustra, através de três círculos concêntricos, que a vida privada – relacionada a aspectos específicos da pessoa – seria representada pelo círculo maior, a intimidade – de natureza espiritual – pelo círculo imediatamente menor, e, por fim, no círculo menor, estaria representado o segredo – informações secretas. Para essa teoria, o círculo verdadeiramente intransponível seria o círculo do segredo, da confiabilidade. [83]

---

[81] MORAES, Alexandre de. Direito Constitucional, 26. ed. rev. e atual. São Paulo: Atlas, 2010, p. 53.
[82] Ibidem, p. 53.
[83] RODRÍGUEZ, Victor Gabriel. *Tutela Penal da Intimidade: Perspectivas da Atuação Penal na Sociedade da Informação*. São Paulo: Atlas, 2008, p. 25.

Para a correta divisão dessas esferas, as quais são flexíveis, deve-se analisar aspectos particulares da vida da pessoa. Para a crítica mais atual, a teoria não deveria ser considerada de forma rígida, pois, se assim o fosse, estar-se-ia diante de um indivíduo com grau de sociabilidade zero, e não é admissível conceber uma esfera de âmbito individual não social.[84]

Prosseguindo na análise, cumpre-se diferenciar os dois círculos menores: a intimidade – círculo intermediário – e o segredo – círculo menor. A intimidade não está diretamente vinculada à ideia de informação confidencial, nem é, por si, uma questão apenas de segredo ou de ocultação, ainda que este possa vir a fazer parte dela. A intimidade, como modo de manifestação da personalidade, é forma de expressão de liberdade.[85]

O segredo, diferentemente, "atrela-se ao desejo de ocultar, ou seja, aquilo que cada pessoa guarda para si, com a firme intenção de não revelar aos demais". [86] Representa "aquele conjunto de informações que não pode sequer ser de conhecimento daquele que não detenha o sigilo". [87]

Para se saber quais informações ou dados devam fazer parte deste círculo intangível, pode-se usar duas tendências: a primeira subjetiva, relacionada à vontade; a segunda objetiva, relacionada ao interesse. Pela tendência subjetiva, a situação de segredo seria definida a partir do momento que seu titular manifestasse a vontade de que determinadas informações permanecessem em segredo. Pela tendência objetiva, só seria admitido o segredo se houvesse um interesse sério, que também fosse legítimo e juridicamente relevante, no sentido de ser justificável que outras pessoas não tivessem acesso à esses dados. [88]

---

[84] RODRÍGUEZ, Victor Gabriel. *Tutela Penal da Intimidade: Perspectivas da Atuação Penal na Sociedade da Informação*. São Paulo: Atlas, 2008, p. 25-26.
[85] Ibidem, p. 27.
[86] Ibidem, p. 27.
[87] Ibidem, p. 28.
[88] Ibidem, p. 28-29.

Os conceitos de intimidade e vida privada também não se confundem. Enquanto que a intimidade trata de questões íntimas, como as relações familiares e de amizade, a vida privada envolve os demais relacionamentos humanos, inclusive as relações comerciais.[89] Portanto, "entende-se que a vida privada tem uma maior amplitude de significado".[90]

A intimidade e a vida privada estão, então, elevadas ao *status* de direito fundamental. A intimidade é, mais ainda, entendida como um direito da personalidade, uma qualidade do próprio sujeito. Não há que se falar, dessa forma, em direito subjetivo, pois os atributos da personalidade não seriam direitos dessa dimensão, já que unificam-se no próprio indivíduo. Como previsão constitucional, outrossim, mais do que um direito de personalidade previsto no Código Civil, a intimidade é um direito fundamental.

Como os direitos da personalidade formam um conjunto indissociável, a intimidade está relacionada diretamente com a dignidade da pessoa humana, como se pode perceber em quase todos os documentos internacionais atuais que cuidam do tema. Dessa forma, a intimidade seria um dos elementos da dignidade humana do qual surgem os demais direitos da personalidade.[91]

No mesmo sentido, trazendo estes conceitos para o contexto da sociedade tecnológica, a intimidade também é considerada, além de um bem jurídico consagrado como direito fundamental, como atributo da personalidade. Tal raciocínio torna legitima sua tutela penal, a qual protege inclusive a mera potencialidade de sua exposição ao risco.[92]

---

[89] MORAES, Alexandre de. Direito Constitucional, 26. ed. rev. e atual. São Paulo: Atlas, 2010, p. 53.
[90] RODRÍGUEZ, Victor Gabriel. *Tutela Penal da Intimidade: Perspectivas da Atuação Penal na Sociedade da Informação*. São Paulo: Atlas, 2008, p. 32.
[91] Ibidem, p. 38.
[92] Ibidem, p. 134.

Em verdade, a internet tem se mostrado um campo não mais teórico e futuro, mas totalmente atual. Dessa forma, deve-se analisar a aplicação do direito à intimidade também neste âmbito.[93]

Embora inicialmente fosse idealizado um ciberespaço livre de qualquer norma, esse ideal anarquista não persistiu. Entre os fatores que fizeram naufragar essa ideia podemos citar os mais diversos delitos praticados via internet: racismo, pornografia infantil, terrorismo, fraudes, crimes contra o consumo e várias outras formas de crimes contra o patrimônio.[94]

A intimidade no mundo dos computadores não se resume a uma ideia de direito ao controle de dados pessoais; ao contrário, vai além desse tipo de conceito, pelo fato de tais dados não estarem em circulação em redes fechadas sobre as quais se possam determinar uma confidencialidade e uma regulação estrita.[95]

A internet fez com que os juristas formulassem um conceito menos pretensioso para intimidade. Assim, este direito ficaria restrito ao simples anonimato, o qual, por sua vez, não significa o controle dos dados pessoais. A definição daquele direito se transformou em um suave conceito de anonimato, o qual é entendido por um direito de circular sem ser notado.[96]

Desse modo, o anonimato fica definido, em seu uso na rede, como uma grande garantia da intimidade que impede a colheita ou a identificação dos dados pessoais. Assim, a impossibilidade da identificação do usuário que acessou tais e quais páginas, ou que realizou uma compra, ou, até mesmo, postou um comentário em uma rede social, figura como proteção da vida privada, dada a função específica da rede mundial de computadores.[97]

---

[93] RODRÍGUEZ, Victor Gabriel. *Tutela Penal da Intimidade: Perspectivas da Atuação Penal na Sociedade da Informação*. São Paulo: Atlas, 2008, p. 85.
[94] Ibidem, p. 86-87.
[95] Ibidem, p. 87-88.
[96] Ibidem, p. 88.
[97] Ibidem, p. 88.

No entanto, esse anonimato que se pretende como uma redefinição da intimidade para a rede, também não é uma realidade, "tendo em vista a identificação, pelos provedores da *web*, dos pontos de acesso à internet, e a partir daí, de seus usuários".[98]

Nesse ponto, leva-se em consideração o fato de que a garantia de anonimato não quer dizer, de forma direta, liberdade pessoal ou, menos ainda, satisfaz o conceito de intimidade. A Constituição Federal estabeleceu a liberdade de expressão e a vedação ao anonimato no mesmo inciso com o intuito de evitar a impunidade dos registros anônimos.[99]

A garantia do anonimato interessa à intimidade enquanto o usuário não possui o registro de todas as suas atividades praticadas no mundo virtual. Porém, poderá haver um efeito reverso, na medida em que não se possibilite a identificação – e logo a persecução – daqueles que, utilizando a internet como instrumento de publicação, atinjam a vida privada de outras pessoas.[100]

O anonimato absoluto, entretanto, não pode ser praticado, seja (1) porque encontra, no ordenamento jurídico vigente, vedação da constituição, seja (2) porque a própria dificuldade de se identificar um usuário de internet já constituir um fator delituoso. Daí a justificativa da possibilidade de os provedores identificarem seus usuários e guardarem as suas informações em sigilo, o qual poderá ser violado em caso de extrema necessidade.[101]

Mesmo quando relacionado apenas ao acesso à internet, o direito ao anonimato não pode representar um aspecto do direito à intimidade. Embora os usuários busquem justifica-lo, eles mesmos reconhecem que seus pontos de coincidência com o mundo físico – como, por exemplo, seu alto potencial de divulgação/publicação e a possibilidade de

[98] RODRÍGUEZ, Victor Gabriel. *Tutela Penal da Intimidade: Perspectivas da Atuação Penal na Sociedade da Informação*. São Paulo: Atlas, 2008, p. 88.
[99] Ibidem, p. 89.
[100] Ibidem, p. 90.
[101] Ibidem, p. 91-92.

cometimento de crimes digitais – o impedem de ser entendido como um direito a ser consagrado, pelo menos neste momento, no qual vigora a vedação constitucional a ele. [102]

3.2 A Inviolabilidade de Dados

Preconiza o inciso XII do artigo 5º da Lei Maior que:

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal

A garantia do sigilo de dados é matéria de proteção constitucional recente, tendo sido prevista somente no texto da Carta de 1988. Essa inviolabilidade representa um complemento ao direito de intimidade, sendo ambas previsões de defesa da privacidade.[103]

Observe que, embora a constituição estabeleça uma exceção apenas para o último caso – sigilo das comunicações telefônicas –, deve-se entender que também os demais direitos admitem exceções, pois nenhum direito é absoluto. Analisando-se um caso concreto no qual outros valores constitucionais igualmente protegidos também estejam em jogo, poderá haver violação aos outros tipos de sigilo.[104]

Nesse diapasão, já apresenta o STF jurisprudência no sentido de permitir a interceptação das correspondências e comunicações telegráficas e de dados sempre que tais direitos estiverem sendo invocados para encobrir práticas ilícitas:

> A administração penitenciária, com fundamento em razões de segurança pública, de disciplina prisional ou de preservação da ordem jurídica, pode, sempre excepcionalmente, e desde que respeitada a norma inscrita no art. 41, parágrafo único, da Lei 7.210/1984, proceder à interceptação da correspondência remetida pelos sentenciados, eis que **a cláusula tutelar da inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguarda de práticas ilícitas**.[105] (**grifou-se**)

---

[102] RODRÍGUEZ, Victor Gabriel. *Tutela Penal da Intimidade: Perspectivas da Atuação Penal na Sociedade da Informação*. São Paulo: Atlas, 2008, p. 92-93.
[103] MORAES, Alexandre de. Direito Constitucional, 26. ed. rev. e atual. São Paulo: Atlas, 2010, p. 70.
[104] PAULO, Vicente e ALEXANDRINO, Marcelo. Direito Constitucional Descomplicado, 5 ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: Método: 2010, p. 131.
[105] BRASIL. Supremo Tribunal Federal. HC 70.814/SP, Relator Ministro Celso de Mello, julgado em 01/03/1994, DJ 24/06/1994.

Note ainda que o Poder Público obtém dados relativos à vida privada e aos negócios de todos os contribuintes, por meio de declarações de rendas anuais enviadas à Receita Federal, sejam pessoas físicas ou jurídicas.[106] Assim, apesar das informações a respeito da situação de riqueza dos respectivos contribuintes estarem resguardada de qualquer interferência externa, a simples obtenção de dados cadastrais não implica em violação ao sigilo de dados.

Isso porque, ao prever a inviolabilidade do sigilo de dados, a Constituição está proibindo, na verdade, que se abram cartas e outras formas de correspondência escrita, se interrompa o seu curso e se escutem e interceptem telefonemas, não abrangendo os meros dados cadastrais em si.[107]

Nesse sentido, cumpre-se utilizar de um exemplo, no qual a comunicação telefônica protegida pelo sigilo difere-se dos dados cadastrais telefônicos, estes representando informações mínimas sobre o dono da linha telefônica com a finalidade de reconhecer o consumidor do serviço, e aqueles acessíveis somente mediante autorização judicial. Como visto acima, a mencionada proteção constitucional resguarda tão somente a comunicação.[108]

Pode-se assim definir dados cadastrais como as informações objetivas, armazenadas em bancos de dados de pessoas jurídicas de direito privado, fornecidas por consumidores. Como exemplo pode-se citar: nome completo, CPF, RG, endereço e número de telefone.[109]

As informações relativas a esses dados não estão protegidas pelo sigilo, pois a finalidade essencial do armazenamento dos dados de cadastro é a identificação do consumidor para utilização para fins de cobrança, venda de produtos via telemarketing e envio de mala-

[106] MORAES, Alexandre de. Direito Constitucional, 26. ed. rev. e atual. São Paulo: Atlas, 2010, p. 72.
[107] SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 21. ed. rev. e atual. São Paulo: Malheiros, 2002, p. 436.
[108] REZENDE, Bruno Titz de. *A requisição de dados cadastrais pela autoridade policial.* Jus Navigandi, Teresina, ano 13, n. 1967, 19 nov. 2008. Disponível em: <http://jus.uol.com.br/revista/texto/11985>. Acesso em: 19 abr. 2011.
[109] Ibidem.

direta, na maioria dos casos. Observe que tais informações não revelam qualquer aspecto da vida privada ou mesmo da intimidade do indivíduo, razão pela qual a melhor doutrina sustenta que não há que se falar em proteção constitucional nesse caso.[110]

Contudo, existem cadastros específicos que não se enquadram no conceito aqui trazido. Tratam-se de verdadeiros arquivos sobre o comportamento de clientes, e para a doutrina, por conseguinte, estes dossiês estão sob a tutela constitucional. De qualquer forma, o conhecimento de tais dados pela Autoridade Policial, que deve restringir seu uso apenas para fins de persecução penal, não representa publicização de informações mantidas sob o manto de proteção da Constituição.[111]

3.3 O Princípio da Supremacia do Interesse Público

O princípio da supremacia do interesse público, também chamado de princípio da finalidade pública, não apenas inspira o legislador, como também vincula a atuação da Administração Pública, ou seja, deve o princípio estar presente também no momento da aplicação da lei ao caso concreto.[112] Ele está previsto no *caput* do artigo 2º da Lei n. 9.784/99:

> Art. 2º A Administração Pública obedecerá, dentre outros, aos princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, **interesse público** e eficiência. (**grifou-se**)

Quanto à influência deste princípio na elaboração das leis, diz-se que, suscintamente, o direito público visa proteger o interesse público, enquanto que o direito privado contém normas de caráter eminentemente individual.[113]

Ademais, o objetivo primeiro das normas de interesse público é o bem estar coletivo, embora proteja invariavelmente também os interesses individuais. O individualismo,

---

[110] REZENDE, Bruno Titz de. *A requisição de dados cadastrais pela autoridade policial.* Jus Navigandi, Teresina, ano 13, n. 1967, 19 nov. 2008. Disponível em: <http://jus.uol.com.br/revista/texto/11985>. Acesso em: 19 abr. 2011.
[111] Ibidem.
[112] DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 20. ed. São Paulo: Atlas, 2007, p. 59.
[113] Ibidem, p. 59.

que via o homem como fim único do direito, foi substituído pelo princípio que os interesses públicos têm supremacia sobre os individuais. [114]

Nos dizeres de Maria Sylvia Di Pietro, o "Direito deixou de ser apenas instrumento de garantia dos direitos do indivíduo e passou a ser visto como meio para consecução da justiça social, do bem comum, do bem-estar coletivo".[115]

Os preceitos que surgiram no plano constitucional em nome da primazia do interesse público demonstram a intervenção crescente do Estado na vida econômica e, inclusive, no direito de propriedade, existindo, outrossim, normas que permitem ao Poder Público intervir no funcionamento e até mesmo na propriedade das empresas.[116]

É no âmbito do Direito Constitucional e Administrativo que o princípio da supremacia do interesse público tem a sua aplicação principal.[117]

Nesse momento, é oportuno lembrar que o Direito Constitucional é um ramo do direito público, essencial à organização, ao funcionamento e à estruturação política do Estado.[118] Nas palavras do ilustre jurista José Afonso da Silva, trata-se de um "Direito Público fundamental, por referir-se diretamente à organização e funcionamento do Estado, à articulação dos elementos primários do mesmo e ao estabelecimento das bases da estrutura política".[119]

Visando atender ao interesse social, o qual não poderá ser negligenciado diante do individual, permite-se que a lei outorgue à Administração poderes dentre os quais o de policiar e punir. Consequentemente, essa prerrogativa não poderá ser usada para a persecução

[114] DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 20. ed. São Paulo: Atlas, 2007, p. 60.
[115] Ibidem, p. 60.
[116] Ibidem, p. 60.
[117] Ibidem, p. 61.
[118] PAULO, Vicente e ALEXANDRINO, Marcelo. Direito Constitucional Descomplicado, 5 ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: Método: 2010, p. 2.
[119] SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 21. ed. rev. e atual. São Paulo: Malheiros, 2002, p. 34.

de objetivos pessoais, sendo que nesse caso o ato será ilegal pelo vício de desvio de poder ou desvio de finalidade.[120]

Ainda ligado a este princípio, pode-se citar o princípio da indisponibilidade do interesse público, que está intimamente ligado ao primeiro. De acordo com esse princípio, não cabe à Administração dispor dos direitos da coletividade, devendo o órgão público apenas tutelá-lo e aplica-lo.[121] É por essa razão que se diz que o poder da Administração é na verdade um poder-dever, pois ela tem o dever, a obrigação, de agir. A Administração não pode, por conseguinte, renunciar ao exercício das competências que lhe foram atribuídas, não pode deixar de punir após a constatação do ilícito e muito menos pode deixar de exercer o poder de polícia para restringir o exercício de direitos individuais em conflito com o bem-estar coletivo.[122]

Dentre todos os bens protegidos pelo Estado, existem alguns, no entanto, que demandam um resguardo maior e mais rigoroso, eis que sua violação afeta sobremaneira as condições de vida em sociedade. Estes bens mais importantes são definidos pelo legislador e tutelados pelo Direito Penal, sendo que a violação a qualquer deles é o que se chama de ilícito ou infração penal.[123]

Como os bens tutelados pelas regras penais são públicos no mais alto grau, o direito de punir os infratores pertence à sociedade, visto que todos sabem que a prática de delitos transtorna a ordem pública, e a sociedade é a principal vítima. Destarte, tem a sociedade o direito de prevenir e reprimir atos lesivos à sua existência e manutenção.[124] Essa

[120] DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 20. ed. São Paulo: Atlas, 2007, p. 61.
[121] Ibidem, p. 61.
[122] Ibidem, p. 61.
[123] TOURINHO FILHO, Fernando da Costa. Manual de Processo Penal, 11. ed. rev. e atual, São Paulo: Saraiva, 2009, 5.
[124] Ibidem, 5.

função de reprimir os crimes, no entanto, conserva-se nas mãos do Estado, o qual a exerce por intermédio de órgãos competentes, já que a sociedade é uma entidade abstrata.[125]

Por fim, ressalte-se que o direito à persecução penal (*persecutio criminis*), que é o direito de investigar o tipo criminal violado e pedir a solução do litígio, é mais do que um mero poder do Estado; é um dever, uma obrigação funcional, a fim de que o Estado possa alcançar um dos fins cruciais para o qual foi criado: segurança e reintegração da ordem jurídica.[126]

Sobre essa obrigação policial, preconiza o artigo 6º, inciso III do Código de Processo Penal:

> Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
> [...]
> III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias

Ainda com relação à atuação da polícia na fase inquisitiva, vale citar o seguinte julgado do Tribunal Regional Federal da 4ª região:

> MANDADO DE SEGURANÇA. GARANTIA CONSTITUCIONAL. SIGILO TELEFÔNICO. PEDIDO DE INFORMAÇÃO. CADASTRO DE USUÁRIO DE OPERADORA DE TELEFONIA MÓVEL. DELEGACIA DE POLÍCIA FEDERAL. INQUÉRITO. DESNECESSIDADE DE AUTORIZAÇÃO JUDICIAL. DIREITO DE INTIMIDADE. NÃO-VIOLAÇÃO. DIREITO LÍQUIDO E CERTO. INEXISTÊNCIA.
> **1. Havendo inquérito policial regularmente instaurado e existindo necessidade de acesso a dados cadastrais de cliente de operadora de telefonia móvel, sem qualquer indagação quanto ao teor das conversas, tal pedido prescinde de autorização judicial.**
> 2. Há uma necessária distinção entre a interceptação (escuta) das comunicações telefônicas, inteiramente submetida ao princípio constitucional da reserva de jurisdição (CF, art. 5º, XII) de um lado, e o fornecimento dos dados (registros) telefônicos, de outro.
> 3. O art. 7º da Lei nº 9296/96 - regulamentadora do inciso XII, parte final, do art. 5° da Constituição Federal - determina poder, a autoridade policial, para os procedimentos de interceptação de que trata, requisitar serviços e técnicos especializados às concessionárias de serviço público. Se o ordenamento jurídico confere tal prerrogativa à autoridade policial, com muito mais razão, confere-a, também, em casos tais, onde pretenda-se, tão-somente informações acerca de dados cadastrais.

---

[125] TOURINHO FILHO, Fernando da Costa. Manual de Processo Penal, 11. ed. rev. e atual, São Paulo: Saraiva, 2009, 5.
[126] Ibidem, 7.

> 4. Não havendo violação ao direito de segredo das comunicações, inexiste direito líquido e certo a ser protegido, bem como não há qualquer ilegalidade ou abuso de poder por parte da autoridade apontada como coatora.[127] (**grifou-se**)

Desse modo, apesar de o poder de polícia não prevalecer quando a Constituição ou outra lei expressamente exigir ordem judicial para a realização de determinada diligência, ele permite à Autoridade Policial determinar quaisquer providências tendentes a elucidar o fato criminoso e suas circunstâncias, inclusive a requisição de dados cadastrais.[128]

3.4 A interpretação dos princípios

A matéria de interpretação dos princípios se mostra de suma utilidade, uma vez que delimitará o alcance e os limites que cada princípio representa concretamente. Assim, é importante compreender a eficácia de cada direito e princípio acima relatado, para que se possa resolver a problemática de forma racional e fundamentada.

A normatividade dos direitos fundamentais contidos no texto constitucional apresenta uma eficácia considerada ainda em nível abstrato, ou seja, uma potencialidade de eficácia. Isso porque a eficácia somente deixará de ser uma possibilidade quando o caso concreto for colocado perante a Constituição para se buscar uma solução, ou seja, quando a norma-texto passar a ser uma norma decisória.[129]

Para que se percorra esse caminho – da norma-texto para a norma decisória – deve-se, em primeiro lugar, analisar os argumentos linguísticos da norma (perquirição verbal), seguida da análise da realidade concreta. Após ambas as análises, será feito um raciocínio interpretativo buscando integrar a norma ao caso concreto apresentado. A norma

---

[127] BRASIL. Tribunal Regional Federal da 4ª Região. MS nº 2004.71.00.022811-2/RS, Relator Desembargador Federal Néfi Cordeiro, julgado em 07/06/2005, DJU 22/06/2005.
[128] REZENDE, Bruno Titz de. *A requisição de dados cadastrais pela autoridade policial*. Jus Navigandi, Teresina, ano 13, n. 1967, 19 nov. 2008. Disponível em: <http://jus.uol.com.br/revista/texto/11985>. Acesso em: 19 abr. 2011.
[129] BONAVIDES, Paulo. Curso de Direito Constitucional, 19. ed. São Paulo: Malheiros, 2006, p. 636.

constitucional no campo do "dever ser" somente será, de fato, "dever ser" após absorver a dimensão da realidade.[130]

A partir destas primeiras considerações, pode-se avaliar especificamente a aplicação dos princípios citados. Sabendo que tanto o direito à intimidade quanto o direito à inviolabilidade de dados constituem direitos fundamentais explicitamente contidos no texto constitucional, deve-se passar a próxima análise: saber se esses direitos recebem ou não proteção absoluta.[131]

Prescreve o § 4º do artigo 60 da Carta Magna:

> § 4º - Não será objeto de deliberação a proposta de emenda tendente a abolir:
> I - a forma federativa de Estado;
> II - o voto direto, secreto, universal e periódico;
> III - a separação dos Poderes;
> IV - **os direitos e garantias individuais**.(**grifou-se**)

Assim, do ponto de vista hermenêutico, uma primeira forma de análise seria considerar os direitos e garantias fundamentais expressões gramaticalmente compreendidas como o texto constitucional os apresenta sem qualquer tipo de intermediação doutrinária, do formalismo jurídico da Constituição-lei e dos códigos onde se analisam o conteúdo de forma mais minuciosa.[132]

Nessa visão, a norma estaria isenta de outros conteúdos valorativos, não sendo considerado nem mesmo a natureza social dos direitos individuais.[133]

Observe-se, no entanto, que se assim fosse considerado, o constitucionalismo seria eternamente inconformado com o surgimento de novos direitos e interpretações que penetram na consciência jurídica de nosso tempo.[134] Os direitos e garantias fundamentais protegidos pelo artigo 60, em grau máximo de intangibilidade, seriam apenas aqueles previstos pelo legislador constituinte originário, sem qualquer adaptação da realidade,

---

[130] BONAVIDES, Paulo. Curso de Direito Constitucional, 19. ed. São Paulo: Malheiros, 2006, p. 636.
[131] Ibidem, p. 637.
[132] Ibidem, p. 637.
[133] Ibidem, p. 637.
[134] Ibidem, p. 638.

lembrando que, de qualquer modo, nesses direitos estariam compreendidos também os direitos de segunda geração, que são os direitos sociais. [135] Uma pequena observação quanto aos direitos sociais é quanto a sua previsão taxativa no artigo 6º da Constituição da República:

> Art. 6º São direitos sociais a educação, a saúde, o trabalho, a moradia, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição.

Uma segunda forma de analisar os direitos e garantias fundamentais seria refutar a ideia de compreensão destes com base unicamente em valores e princípios que outrora os regiam, os quais, muitas vezes, nem mesmo correspondem mais à conjuntura atual.[136] Também nessa concepção considera-se que os direitos sociais são abrangidos pela proteção do tal artigo 60.[137]

Finalmente, tenha-se claro que não há hierarquia, de grau ou de valor, entre os direitos sociais e os individuais. Tanto um quanto o outro buscam a efetivação da proteção constitucional a um bem maior: a dignidade da pessoa humana.[138]

Com efeito, o reconhecimento e a garantia dos bens prezados pela sociedade visa justamente legitimar e preservar a dignidade da pessoa humana, não tendo os direitos fundamentais sido expostos de forma aleatória pelo legislador constituinte. Por essa razão, tais direitos devem constituir a base essencial para a resolução das questões jurídico-constitucionais.[139]

Tal como o caso apresentado no início do presente trabalho, existem situações em que pode ocorrer o que a doutrina denomina de colisão ou conflito de direitos fundamentais. Esse conflito ocorre quanto o exercício de um direito fundamental de um titular colide com o

---

[135] BONAVIDES, Paulo. Curso de Direito Constitucional, 19. ed. São Paulo: Malheiros, 2006, p. 640/641.
[136] Ibidem, p. 641.
[137] Ibidem, 2006, p. 642.
[138] Ibidem, p. 642/643.
[139] BRAZ, Graziela Palhares Torreão. Crime Organizado X Direitos Fundamentais, Brasília: Brasília Jurídica, 1999, p. 103.

de outro. Pode ainda ocorrer em relação aos direitos fundamentais entre si ou mesmo em relação a outros bens jurídicos constitucionais. [140]

Seja como for, na resolução da controvérsia deve-se ter claro que um direito não deverá ser suprimido por outro para sua resolução. Ao revés, "a colisão será solucionada a partir da análise das circunstâncias especiais do caso, que determinará uma relação de precedência condicionada de um direito em relação ao outro."[141]

[140] BRAZ, Graziela Palhares Torreão. Crime Organizado X Direitos Fundamentais, Brasília: Brasília Jurídica, 1999, p. 107.
[141] Ibidem, p. 108.

CONCLUSÃO

A Carta Rogatória inicialmente trazida ao trabalho trata de uma requisição feita pela justiça alemã à justiça brasileira para a quebra do sigilo dos dados cadastrais do usuário infrator mantidos no provedor de conteúdo e acesso à internet Universo On-Line (UOL). A investigação policial germânica culminou neste estágio após constatar que o suspeito era brasileiro, invocando assim a colaboração da justiça brasileira na resolução do referido caso.

Nessa Rogatória foi discutida uma questão polêmica: seria essa quebra de dados cadastrais uma violação aos direitos fundamentais da intimidade e do sigilo de dados, ambos previstos na Constituição?

Para se responder com exatidão e coerência a problemática exposta, constatou-se que, durante a investigação policial – inquérito policial – a autoridade deverá realizar todas as diligências cabíveis na coleta de provas.

Nos crimes digitais, como no caso narrado na Rogatória, as provas são realizadas da seguinte maneira. Primeiramente é necessário realizar a cópia do site vítima - ou meio - do ataque. Depois, deve-se salvar o conteúdo de forma segura, com o objetivo de não ser adulterado, para que, assim, esses dados possam ser usados no processo penal sem terem sua autenticidade questionada. Após, deve-se identificar o servidor que hospeda a página, que no caso em análise, era um servidor estrangeiro. Posteriormente, deve ser localizado o "dono" do IP, para que, por fim, possa ser feita a quebra do sigilo de dados telemáticos, tal como solicitada na Carta Rogatória.

Findadas as considerações sobre a investigação, procedeu-se à análise sobre os direitos fundamentais envolvidos na fase do inquérito. Em primeiro lugar, foi trazido à baila o direito à intimidade, previsto no inciso X do artigo 5º da Constituição Federal. Quando na análise deste direito, verificou-se que apenas a esfera mais íntima, ligada ao segredo, é que é protegida contra as intervenções de terceiros. As demais esferas, como a intimidade e a vida

privada, as quais não guardam informações secretas sobre o individuo, permitem certa flexibilização, visto que nenhum direito é absoluto.

Com esta análise, já podemos asseverar que o fornecimento de dados cadastrais, por não serem informações confidenciais, não viola este direito. Do contrário, afirmar-se-ia que o nome de uma pessoa, seu endereço e demais dados comuns seriam dados secretos, de conhecimento exclusivo do usuário, o que não corresponde à verdade e nem o que a constituição considera inviolável.

Ainda com relação a este inciso, tem-se afirmado que, no âmbito virtual, o direito à intimidade tem-se manifestado no anonimato. No entanto, também se verificou que não se pode falar em anonimato absoluto, pois existe uma vedação constitucional a ele, além de o fato de existir uma dificuldade de identificação de usuário na internet constituir um fator delituoso. A possiblidade de cometimento de crimes digitais impede o anonimato de ser considerado uma faceta do direito à intimidade, mesmo porque tal direito não poderá ser invocado para encobrir atos criminosos.

Quanto ao direito à inviolabilidade de dados, também estudado, constatou-se que a proteção constitucional veda sua comunicação, mas não os dados comumente cadastrais. As informações cadastrais mantidas junto aos provedores de acesso à internet não estão protegidas pelo sigilo constitucional, pois sua finalidade crucial é a identificação do usuário, e não revelam qualquer aspecto de sua vida privada ou mesmo de sua intimidade.

Foi trazido ainda ao trabalho o princípio da supremacia do interesse público, pois a polícia, juntamente com os demais órgãos públicos, atua com a observância desse princípio. De acordo com ele, o interesse público sempre deverá prevalecer em face do interesse individual, seja na elaboração ou na aplicação da lei.

Ligado a este princípio está o da indisponibilidade do interesse público, segundo o qual o órgão não poderá se eximir de suas competências institucionais, pois são elas que

permitem que o interesse coletivo seja garantido. Assim, a polícia não poderá simplesmente deixar de investigar um fato com base em um direito individual, tendo a obrigação, por meio do *jus puniendi*, de fazer com que a segurança e o bem-estar – interesses coletivos – prevaleçam. Assim, tem-se mais um argumento no sentido de permitir a quebra dos dados telemáticos.

Foi ainda sugerida uma forma de interpretação dos direitos fundamentais, a qual, na sua forma mais racional, propõe que os direitos sejam analisados de forma conjunta e com sua implicação atual e não mais a noção engessada do constituinte. Também não deverá haver supressão de nenhum direito quando entre eles houver conflito.

Assim, pode-se resolver o problema tratado por meio das interpretações já expostas. Em primeiro, quanto ao direito à intimidade, o acesso a dados cadastrais do usuário não implicaria violação a este, pois, na sua interpretação mais atual, os dados cadastrais não estão contidos na esfera de confidencialidade do indivíduo. Em segundo lugar, não há que se falar em violação ao sigilo de dados, pois, como visto, os dados meramente cadastrais não estão protegidos pelo dispositivo constitucional, o qual só se aplica em relação à sua comunicação, pois se assim não fosse, não seria possível qualquer tipo de investigação.

Por fim, ainda que essa não fosse a interpretação de tais direitos, tendo em vista que tais direitos são individuais, o direito coletivo à segurança deveria prevalecer, tendo em vista o princípio da supremacia do interesse público que deverá ser observado pela polícia. Essa solução representaria uma interpretação considerando os direitos fundamentais como um todo – os individuais e os coletivos – sem supressão de qualquer deles.

Por tudo aquilo que foi explanado, não há como concluir de forma diversa daquela que permite acesso aos dados cadastrais mantidos nos provedores de acesso à internet, conforme acertada decisão do STJ na Carta Rogatória estudada, a qual considera que a vedação constitucional abrange apenas a comunicação dos dados e não a ciência dos dados

em si. Também pelo exposto, como não há violação aos direitos previstos no artigo 5ª, não há que se falar em necessidade de autorização judicial para esse acesso.

Com o presente trabalho também ficou explícito que muitos internautas só estão interessados em consumir conteúdo, expondo sem nenhum limite sua privacidade em redes socais para terceiros desconhecidos, sem saber das possíveis consequências desses atos. Pensam que estão imunes de sofrerem qualquer golpe na *web.*

Os tempos mudaram e a sociedade precisa urgentemente buscar conhecer esse novo meio de comunicação, o qual é utilizado com muita frequência. Do mesmo modo que se procura cuidar da segurança no mundo físico, também se deve fazer no virtual.

Sabe-se que o conceito de privacidade não é o mesmo de anos atrás, e isso precisa ser levando em consideração. Hoje invadir a intimidade de alguém se tornou um fetiche, como é o caso do programa televisivo, Big Brother Brasil, da rede Globo, onde os telespectadores ficam sentados, assistindo passivamente o dia a dia de um grupo de desconhecidos. É necessária uma reflexão sobre o que é de fato uma violação a intimidade de um indivíduo ou uma quebra de sigilo de dados dentro de um contexto em que os clientes de empresas como Google e Facebook confiam a elas informações sigilosas de si próprio.

O problema, como visto, não está no ordenamento jurídico. Aliás, pode-se até dizer que a questão pode ser resolvida sem muita controvérsia jurídica. A verdadeira controvérsia encontra-se na mentalidade hipócrita dos próprios usuários de internet, que expõem suas informações pessoais, e até as mais íntimas possíveis, em redes de relacionamento sociais, visíveis a qualquer um, e, no entanto, não são capazes de permitir à polícia acesso aos dados mais ínfimos possíveis quanto a sua pessoa, sendo que o objetivo da polícia é manter a segurança do próprio usuário.

Na mesma linha, encontram-se os provedores de acesso à internet, os quais não querem a exposição dos seus clientes, mas acabam, por outro lado, abrindo mão da própria

segurança deles e, consequentemente, colocando em risco a imagem da referida empresa perante a sociedade.

REFERÊNCIAS

BARBAGALO, Erica Brandini, *Contratos Formados por meio de redes de computadores: peculiaridades jurídicas da formação do vínculo*, Editora Saraiva, São Paulo: 2001

BONAVIDES, Paulo. *Curso de Direito Constitucional*, 19. ed. São Paulo: Malheiros, 2006

BRASIL. *Constituição da República Federativa do Brasil de 1988*. DOU de 05/10/1988.

BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. *Código de Processo Penal*. DOU de 13/10/1941.

BRASIL. Lei nº 9.784, de 29 de janeiro de 1999. *Regula o processo no âmbito da Administracao Pública Federal.* DOU de 11/03/1999.

BRASIL. Superior Tribunal de Justiça. *Carta Rogatória nº 297*, Relator Ministro Barros Monteiro, julgado em 18/09/2006, DJ 29/09/2006.

BRAZ, Graziela Palhares Torreão. *Crime Organizado X Direitos Fundamentais*, Brasília: Brasília Jurídica, 1999

CAPEZ, Fernando. *Curso de Processo Penal*. 16. Ed. São Paulo: Saraiva, 2009

DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 20. ed. São Paulo: Atlas, 2007

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro, v. 1: teoria geral do direito civil, 23. ed. rev. e atual. De acordo com o novo Código Civil (Lei n. 10.406, de 10-1-2002) e o Projeto de Lei n. 6.960/2002*, São Paulo: Saraiva, 2006

DINIZ, Maria Helena. *Dicionário Jurídico*, São Paulo: Saraiva, 1998

Evelin Ribeiro, do IDG Now!, Publicada em 04 de agosto de 2009 às 18h04, Atualizada em 05 de agosto de 2009 às 13h51. Disponível em < (http://idgnow.uol.com.br/seguranca/2009/08/04/delegados-defendem-acesso-rapido-a-dados-de-internautas-para-investigacoes) >. Acesso em 13 de abril de 2011 às 23h23min.

INELLAS, Gabriel Cesar Zaccaria de. *Crimes na Internet*, 2ª ed. atualizada e ampliada, São Paulo: Editora Juarez de Oliveira, 2009, p. 35

JESUS, Damásio E. de. *Direito Penal, volume 1: parte geral*. 28. ed. rev. São Paulo: Saraiva, 2005

MINISTÉRIO PÚBLICO FEDERAL, PROCURADORIA DA REPÚPLICA DO ESTADO DE SP, GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. *Crimes Cibernéticos: Manual Prático de Investigação*

MORAES, Alexandre de. *Direito Constitucional*, 26. ed. rev. e atual. São Paulo: Atlas, 2010

NOGUEIRA, Sandro D'Amato. *Crimes de Informática*, 2ª Edição, BH Editora e Distribuidora, São Paulo: 2009

NUCCI, Guilherme de Souza. *Manual de direito penal: parte geral: parte especial*. 3. ed. rev. atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2007

OLIVEIRA, Eugênio Pacelli de. *Curso de Processo Penal*, Rio de Janeiro: Editora Lumen Juis, 2008

PAULO, Vicente e ALEXANDRINO, Marcelo. *Direito Constitucional Descomplicado*, 5 ed. rev. e atual. Rio de Janeiro: Forense; São Paulo: Método: 2010

PINHEIRO, Patrícia Peck. *Direito Digital*, São Paulo: Saraiva, 2009

REZENDE, Bruno Titz de. *A requisição de dados cadastrais pela autoridade policial*. Jus Navigandi, Teresina, ano 13, n. 1967, 19 nov. 2008. Disponível em: <http://jus.uol.com.br/revista/texto/11985>. Acesso em: 19 abr. 2011.

RODRÍGUEZ, Victor Gabriel. *Tutela Penal da Intimidade: Perspectivas da Atuação Penal na Sociedade da Informação*. São Paulo: Atlas, 2008

THING, Lowell (edição). Tradução de Bazán Tecnologia e Linguistica e Texto Digital. *Dicionário de Tecnologia*. São Paulo: Futura, 2003

TOURINHO FILHO, Fernando da Costa. *Manual de Processo Penal*. 11. ed. rev. e atual. São Paulo: Saraiva, 2009

ZAVASCKI, Teori Albino. *Cooperação Jurídica Internacional e a Concessão de Exequatur*. Interesse Público, Belo Horizonte, n. 61, maio/jun. 2010.