CLAYTON DA SILVA BEZERRA
GIOVANI CELSO AGNOLETTO
Organizadores

COMBATE AO CRIME CIBERNÉTICO

doutrina e prática

(A visão do Delegado de Polícia)

Colaboradores

Alesandro Gonçalves Barreto
Carlos Eduardo Miguel Sobral
Clayton da Silva Bezerra
Coriolano Almeida Camargo
David Farias de Aragão
Diana Mann
Emerson Wendt
Erick Blatt
Giovani Celso Agnoletto
Higor Vinícius Nogueira Jorge
José Augusto Campos Versiani
José Navas Junior
Luiz Augusto Pessoa Nogueira
Pablo Barcellos Bergmann
Ruchester Marreiros Barbosa
Stenio Santos Sousa

Prefácio **Helcio Honda**

Mallet Editora

Polícia Cidadã

3

CLAYTON DA SILVA BEZERRA

O autor é Doutorando em Ciências Jurídica e Sociais pela Universidad Del Museo SocialArgentino - UMSA, **Especialista em Direito e Processo Penal – AVM-Universidade CândidoMendes – 2008**, Especialista em Direito Processual Civil – AVM Universidade Cândido Mendes - 2004, MBA em Gestão – Fundação Getúlio Vargas - 2003, Tutor da Academia Nacional de Polícia - ANP, É Delegado de Polícia Federal, Integrante do Grupo de Estudos da criminalidade cibernética Organizada - da Academia Nacional de Polícia - ANP - Presidente do Sindicato dos Delegados de Polícia Federal no Rio de Janeiro. Vice-Presidente da Federação Nacional dos Delegados de Polícia Federal. Coordenador Geral da Ação Social Federal Kids. Foi Gerente Operacional de **Segurança Cibernética** para a Copa das Confederações – FIFA 2013, Gerente Operacional de **Segurança Cibernética** para Encontro Mundial da Juventude - 2013, Gerente do Projeto de **Segurança Cibernética** no evento da Organização das Nações Unidas – ONU, Rio+20 – junho – 2012 – GEPNet.

GIOVANI CELSO AGNOLETTO

Aluno especial do curso de **Doutorado** da Escola de Comunicação e Artes da Universidade de São Paulo – USP, no Programa de Ciências da Comunicação, é **Mestre** pelo Instituto Mauá de Tecnologia (área de meio-ambiente), **pós graduado** em Investigação Criminal pela Academia Nacional de Polícia – ANP-DF, pós graduado em Administração de Empresas pela Escola Superior de Propaganda e Marketing - ESPM-SP, **graduado** em Direito pela Universidade Bandeirante - Uniban-SP e também, **graduado** em Comunicação Social pela Escola Superior de Propaganda e Marketing - ESPM-SP.
Certificador Oficial do INEP e professor universitário desde 1989, em diversas instituições de ensino superior e atualmente está vinculado à Academia Nacional de Polícia em Brasília, como Tutor de EAD, em disciplinas afetas a área de segurança pública.
É Delegado de Polícia Federal, lotado no Estado de São Paulo, já atuou como Policial Civil na cidade de São Paulo é também Oficial da Reserva da arma de Infantaria do Exército Brasileiro.

COMBATE AO CRIME CIBERNÉTICO

Doutrina e prática

(A Visão do Delegado de Polícia)

B574c

Bezerra, Clayton da Silva/Agnoletto, Giovani Celso
Combate ao Crime Cibernético / Clayton da Silva Bezerra
1.ed.- Rio de Janeiro; Mallet Editora, 2020.
269p.; 16 x 23 cm. (Doutrina e Prática – A visão do delegado de polícia 3)

Inclui bibliografia
ISBN 978-85-92842-00-0

1. Processo penal. 2. Direito penal..
I. Bezerra, Clayton da Silva. I. Agnoletto, Giovani Celso. III. Série

CDD: 340 CDU:343.1(81)

1.

Clayton da Silva Bezerra
Giovani Celso Agnoletto
Organizadores

COMBATE AO CRIME CIBERNÉTICO

Doutrina e prática

(A Visão do Delegado de Polícia)

1ª Edição – 2020 – Rio de Janeiro - RJ

Mallet Editora

Projeto Gráfico e Capa
Ana Carolina Mallet – malleteditora.com.br

Diagramação
Sandra Alves – M. Mallet Editora

Revisão
Mauro Mallet

Supervisão editorial
Clayton da Silva Bezerra
Giovani Celso Agnoletto

Editor
Mauro Mallet

1ª EDIÇÃO – 2020 – Rio de Janeiro

Rua Ferreira Sampaio 38 – Encantado
CEP 20756-010 – Rio de Janeiro – RJ
Tel./Fax (21) 4106-8235 celular 99613-0628
Site: www.malleteditora.com.br
e-mail: vendas@malleteditora.com.br

Impressão no Brasil

APRESENTAÇÃO

Este terceiro livro "Combate ao Crime Cibernético – Doutrina e Prática Policial. A visão do Delegado de Polícia" é o resultado do esforço acadêmico de vários estudiosos deste tema tão atual e inquietante.

Dada a relevância do tema, e o alto grau de "*expertise*" de estudiosos do Direito Cibernético no Brasil que nos últimos anos vem colaborando para fomentar discussões e para aprimorar a legislação sobre esta matéria, o Conselho Editorial pela primeira nesta coleção, convidou um profissional de renome deste ramo da ciências jurídicas e que faz parte dos quadros da OAB (Ordem dos Advogados do Brasil), para contribuir com seus estudos e engrandecer esta publicação.

Como coordenadores desta Coleção e os demais Delegados de polícia, lotados em diversos Estados da federação, nos sentimos honrados pelo fato do Dr. Coriolano Camargo ter aceito o convite e estar conosco dentre o nosso quadro de colaboradores, antes de tudo um profissional de valor reconhecido e um professor dedicado, mas sobretudo, um grande amigo (embora não seja policial...)

Buscamos também, para escrever o prefácio desta obra, outro amigo e profissional de destaque na área jurídica, o qual muito nos lisonjeia e que muito nos ajudou não só colaborando com este projeto editorial, mas também com o Projeto da Radio Polícia Cidadã (www.policiacidada.com.br), mais uma vez agradecemos ao Dr. Honda.

Assim, apresentamos a você leitor, o terceiro de uma série de estudos afetos ao trabalho daqueles que se interessam pela segurança pública e é, sobretudo, um relato prático do nosso dia-a-dia, é a forma como nós policiais e agora de outros profissionais - todos estudiosos do direito, colaboramos com a justiça deste país.

O objetivo desta coleção é apresentar um trabalho moderno, atualizado e, sobretudo, escrito principalmente a partir da visão de um Delegado de Polícia, àqueles que operam diariamente no direito criminal, seja como participante ou até mesmo responsável pela formulação de políticas públicas na área de segurança pública, ou até mesmo para estudiosos deste tema, como docente ou até mesmo, para o acadêmico do direito, aquele que na essência, todos somos e nunca deixaremos de ser.

Egon Bittner um grande pesquisador de temas da área de segurança pública, nascido na antiga Tchecoslováquia e que emigrou para os Estados Unidos após a Segunda Guerra Mundial, afirmou em um dos seus mais célebres trabalhos (Aspectos do trabalho policial, Editora da Universidade São Paulo - USP, 2003) que *... é diferente escrever sobre a atividade desenvolvida pela polícia, com uma visão de dentro ou de fora da polícia, ou seja, escrever sobre a polícia sem ser policial, possivelmente irá ter uma visão diferente da realidade praticada...* assim, mais uma vez, nós os coordenadores e todos os nossos colegas, nos esforçamos para trazer a visão de cada um a partir na nossa experiência cotidiana,

esperamos sinceramente que esta obra lhe seja útil e que a partir dele, você leitor, possa ver o trabalho policial, a partir dos nossos olhos...

Após o sucesso do lançamento dos dois primeiros livros desta série, temos a certeza de que trazer a discussão "Combate ao Crime Cibernético – Doutrina e Prática Policial", também irá despertar grande interesse, haja vista a enorme importância que as discussões jurídicas vêm tomando corpo nos últimos tempos.

Sabemos que nenhuma obra é perene, e certamente está (até mesmo pela impressionante evolução do tema) não o será, mas o que se apresenta a leitura é de suma importância para os dias atuais e ainda permanecerá em discussão por muito tempo, certamente, até mesmo quando da futura revisão para novos artigos, por isso, temos uma grande expectativa de que você leitor, irá apreciar bastante os novos e inquietantes temas que aqui são apresentados.

No primeiro livro desta coleção, "inquérito policial", reconhecia-se e destacava-se a merecida importância deste instrumento para a justiça e para a sociedade (.... *e não menos importante, também é através de inquérito policial, que aquilo que não é dito, ou declarado como verdadeiro... após um profundo trabalho investigado... vem a tona como verdade real, e os verdadeiros culpados aparecem... e aqui, cabe uma das máximas antigas, que poucos acreditam: o bem prevalece!)* tanto que foi escolhido para ser o primeiro título desta coleção

Já no segundo título "Temas processuais penais da atualidade", mais uma vez, até mesmo pela importância que se apresenta, e pela enorme responsabilidade que nos foi depositada, pelo sucesso desta coleção, escolhemos especialistas de diversas áreas de sua atuação, todos Delegados de Polícia, exercendo diuturnamente o trabalho de polícia judiciária, e com grande experiência na condução de investigações criminais e exercendo sua atividade nos mais diversos pontos deste imenso país.

Na medida em que cresce a sensação de insegurança e de impunidade, saber o que faz a polícia judiciária no Brasil cresce enormemente em importância.

O cidadão comum quer saber também como são empregados os recursos, qual (ou quais) a (s) técnica (s) utilizadas, o grau de profissionalismo de cada um dos profissionais de segurança pública envolvidos, tudo isso aumenta a sua relevância e principalmente, como trabalha a polícia a serviço dos valores de uma sociedade democrática, identificando autores de delitos, produzindo um conjunto probatório valioso, enfim, para a sociedade que se aflige diariamente, o que fica de importante deste trabalho: resolver o crime, punir o responsável, colaborar com a justiça!

Esperamos sinceramente que vocês apreciem este trabalho de pesquisa e que os inspire e incentive a discutir o que aqui está proposto.

Por fim, retomando o que já foi dito no primeiro livro sobre o inquérito policial, esperamos que esta obra também seja útil para todos os atores da "penosa" vida jurídica, de estudantes a magistrados, tornando claro o trabalho de investigação policial presidida pelo Delegado de Polícia que nas palavras do Ministro Marco Aurélio Melo é o "primeiro garantidor da legalidade e da justiça" (HC 84548/SP).

Lembrando as palavras do Delegado Federal Fábio Ricardo Ciavolih Mota ***"Ninguém quer o fim do Inquérito Policial, o que todos querem é O Inquérito Policial"***

PREFÁCIO

Gentilmente agraciado e convidado a escrever este prefácio da obra "Combate ao Crime Cibernético", organizado pelos Drs. Clayton da Silva Bezerra e Giovani Celso Agnoletto, tive a grata oportunidade de verificar o excelente conteúdo e abrangência de uma obra que não deve faltar em nenhuma biblioteca.

A abordagem ampla deste atualíssimo tema, agrada ao operador do direito e ao leigo, usuário de um sistema de informação digital ou de uma rede social.

O mundo sofreu uma grande alteração e o mundo cibernético da informação, tornou global a disseminação da informação pela internet e redes sociais, gerando problemas jurídicos até então nunca enfrentados. Nunca, na história, a vida privada ou corporativa, foram tão devassadas e violadas, disseminando-se sem permissão, a informação verdadeira, ou a falsamente maldosa, quebrando completamente os muros e barreiras de proteção.

Tema portanto, oportuno para esta obra, que avança com maestria sobre temais atuais do direito informático e suas implicações na segurança pública e jurídica.

O livro começa com um capítulo de História do Crime Cibernético escrito Pelos Delegado Clayton Bezerra e Carlos Eduardo Miguel Sobral para situar o leitor nos temas que serão debatidos no decorrer do texto.

O debate avança em temas atuais do Direito Informático e suas implicações na Segurança Pública Digital como os capítulos sobre as leis que englobam o tema Dos crimes cibernéticos como a lei 12.737/12, que ficou conhecida como a Lei Caroline Dieckmann, por ter sido aprovada pouco tempo depois da atriz que batiza a norma ter sido vítima de ataque de terceiros que violaram sua privacidade e intimidade, pelo modo cibernético, explicado com detalhes pelo Delegado Federal Luiz Augusto e os Aspectos Penais do Marco Civil da Internet, Lei 12.964/14 escrito pelo Delegado Federal Pablo Barcellos.

O trabalho de investigação do Delegado de Polícia foi abordado diretamente nos artigos: A contribuição crítica processo de investigação criminal da fraude bancária eletrônica do Delegado Federal Stenio e as Ferramentas de Investigação do Delegado Federal Erick Blatt e a Utilização de fontes abertas na investigação policial escrito pelo Delegado de Polícia Civil Alessandro.

Considerando a natureza específica do crime cibernético, teve-se o cuidado de abordar a questão das provas escrito pelos Delegados Federais Clayton Bezerra e Giovani Agnoletto, além de um capítulo sobre Perícia computacional e investigação de delitos informáticos: importância e desafios contemporâneos,

escrito pelos Delegados de polícia Civil do Rio Grande do Sul Emerson Emerson Wandit do e o Delegado de Polícia Civil de São Paulo Igor Jorge

A discussão nesta obra extrapola a esfera formal e traz uma contribuição na doutrina jurídica de assuntos de vanguarda neste tipo de crime quando discute o Stalkink (Perseguição virtual) que esteve como manchetes de jornal no caso da apresentadora Ana Hickman que foi ameaçada de morte por um "perseguidor". Este capítulo foi escrito pelo Delegado Federal José Navas Junior. A Infiltração Cibernética no Processo Penal Brasileiro é discutida pela Delegada Federal Diana Mann.

Outro assunto que mereceu destaque foi a Cooperação Internacional na Investigação de crimes Cibernéticos do Delegado Federal Versiani.

A Obra traz também, uma discussão doutrinária construtiva a luz da Ciência Policial e da Policiologia com os capítulos sobre: A Inconstitucionalidade da lei 12.965 (Marco Civil da Internet), capítulo escrito pelo Delegado de Polícia civil Ruchester Marreiros Barbosa e o tema Limites Constitucionais E Efetividade Da Investigação Criminal De Delitos Cibernéticos escrito pelo Delegado Federal David Farias de Aragão.

Os organizadores da obra tiveram a sensibilidade de convidar o Advogado Dr Coriolano Aurélio de Almeida Camargo Santos para escrever sobre Ciberameaças e o Registro de Controle da Produção e do Estoque – Bloco K do SPED Fiscal, para mostrar que o perigo de violação de dados corporativos ou segredos industriais de produtos e formulação, podem ocorrer também no ambiente corporativo das empresa, emprestando uma visão da advocacia sobre o assunto.

Enfim, esta é uma pequena amostra do grande universo que se abre sobre o assunto e recomendo o leitor a uma atenta leitura desta obra que com certeza auxiliará muito nos grandes debates e soluções desta nova área do direito.

Helcio Honda.
Vice Presidente do Conselho Jurídico de Assuntos Jurídicos e Legislativos da FIESP e CIESP. Diretor Titular do Departamento Jurídico da Federação das Indústrias do Estado de São Paulo.

Caiu um avião?!... aparecem os “especialistas” em queda de avião...

Copa do mundo?!... surgem os especialistas em futebol...

Manifestações de rua?! materializam-se os especialistas em manifestações...

Alta da inflação?!... instantaneamente os especialistas em economia...

Baixa da inflação, ajuste fiscal, *impeachment*?!... especialistas em política...

Maioridade penal, liberação de drogas, refugiados, sim, também temos especialistas; e por aí afora...

E como não poderia deixar de ser, quando se discute “segurança pública”, também há uma oportunidade única para aqueles que se autodenominam “especialistas em segurança pública”, mas que na verdade, em sua maioria ou quase a totalidade, são oportunistas!

O inquérito policial – atacado e criticado por muitos desses especialistas – é o principal instrumento utilizado para se chegar à justiça no Brasil, senão o único!

A luta fundamental pelo poder é a batalha pela construção de significado na mente das pessoas, o que explica em grande medida a luta desenfreada desses “especialistas” em criticar a polícia e o trabalho policial, sobretudo, o inquérito.

É possível haver um trabalho investigativo sério, com cadeia de custódia probatória preservada, com organização temporal, com exposição crítica e técnica dos fatos, com sigilo, com ciência, com tecnicidade... se não houver um inquérito?

Todos aqueles que colaboraram para que esta obra existisse são policiais! Se não somos especialistas, ao menos somos aqueles que fazem do inquérito a razão da nossa existência e lutamos para que este instrumento fique melhor, buscando aprimorar e melhorar a cada dia que entramos em uma Delegacia em qualquer parte deste vasto país.

Nós, os policiais, quando acordamos cedo (ou por vezes, nem dormimos), para ir às ruas e realizar o trabalho que escolhemos por vocação e por orgulho de pertencer a uma instituição policial, certamente podemos resumir em três palavras o nosso dia-a-dia e a nossa expectativa: força, coragem e honra!

Há justiça sem polícia?

Giovani Celso Agnoletto

SUMÁRIO

Capítulo I

Introdução ao estudo Do crime cibernético

Carlos Eduardo Miguel Sobral[1] *e Clayton Bezerra*[2]

Com o mundo globalizado e cada vez mais interconectado, com o número de usuários de novas tecnologias crescendo de forma exponencial, as legislações neste ramo do direito precisam estar atualizadas para nos proteger dessa nova modalidade delitiva que a cada dia coloca em risco integridades físicas, morais e financeiras de pessoas físicas, pessoas jurídicas e até mesmo de governos, como vimos nas revoltas do Egito, Síria, Líbano, etc.

Neste estudo, temos como objetivo avaliar a evolução histórica do uso do computador e da internet e suas influências no mundo jurídico, tendo como enfoque o Crime Cibernético e a evolução das normas penais no que tange esta modalidade delituosa, que está em franco crescimento.

Abordaremos a história da informática, assim como a evolução da internet e sua consequência inevitável que é o crime no ciberespaço ou a utilização deste meio para atividades criminosas, ou seja, a internet como meio para a efetivação de um delito. Como se pode ver, o alvo central de nosso estudo sempre será a história dos delitos informáticos. O Direito Informático é defendido como ramo autônomo do Direito.

Para Pinheiro[3] (2010): "A capacidade de adaptação do Direito determina a própria segurança do ordenamento, no sentido de estabilidade do sistema jurídico por meio da atuação legítima do poder, capaz de produzir normas válidas e eficazes."[4]

As sociedades mudam[5], seus integrantes e também seus pensamentos. As

---

[1] Delegado de Polícia Federal, foi Chefe do Serviço do Serviço de Repressão a Crimes Cibernéticos (2007 a 2013), Chefe do Serviço de Inteligência da Coordenação Geral de Polícia Fazendária (2013), Consultor para assuntos relacionados a "crimes cibernéticos" do Escritório das Nações Unidas, Professor Universitário Convidado da UnB, CEUT, Mackenzie/SP e da Academia Nacional de Polícia e Presidente da Associação Nacional dos Delegados de Polícia – ADPF.

[2] O autor é Doutorando em Ciências Jurídica e Sociais pela Universidad Del Museo Social Argentino - UMSA, **Especialista em Direito e Processo Penal – AVM-Universidade Cândido Mendes – 2008,** Especialista em Direito Processual Civil – AVM Universidade Cândido Mendes - 2004, MBA em Gestão – Fundação Getúlio Vargas - 2003, Tutor da Academia Nacional de Polícia - ANP, É Delegado de Polícia Federal.

[3] - Pinheiro, Patricia Peck Direito Digital, São Paulo: Saraiva, 2010

[4] "O Direito é responsável pelo equilíbrio da relação comportamento-poder, que só pode ser feita com a adequada interpretação da realidade social, criando normas que garantam a segurança das expectativas mediante sua eficácia e aceitabilidade, que compreendam e incorporem a mudança por meio de uma estrutura flexível que possa sustentá-la no tempo. Esta transformação nos leva ao Direito Digital." - Pinheiro, Patricia Peck. Direito Digital, São Paulo: Saraiva, 2010.

[5] "A sociedade humana vive em constante mudança: mudamos da pedra talhada ao papel, da pena com tinta ao

inovações tecnológicas atingem todas as atividades humanas. Junto conosco convivem as leis e estas precisam se adaptar as novas necessidades de cada época.[6]

Para Catala (2010): "Este crecimiento de la sociedad de nuestro tiempo, impulsado por un progreso técnico más veloz que el avance de las ciencias sociales, requierem una respuesta inmediata para preservar sua armonía, pues, de lo contrario, puede vaticinarse, habrá de volverse contra el indivíduo, em cuanto su inorgannicidad acelera también sua ineficiencia para servilo."[7]

Uma coisa é certa, quanto mais demorarmos em nos proteger com medidas legais para o combate a este tipo de delito, mais ele crescerá e como possui uma característica de auto renovação e desenvolvimento de tecnologias, mais difícil será acabar com a impunidade dos crimes cibernéticos que já possuem uma geração econômica no patamar do tráfico internacional de entorpecentes, mas que não possuem o mesmo viés de violência nem o estereótipo dos guetos e favelas.

1. A HISTÓRIA DO COMPUTADOR

1.1 ENIAC (Eletronic Numerical Integrator and Calculator)

Muitos consideram ser o ENIAC, criado em 1946 pelos cientistas norte-americanos John Eckert e John Mauchly, como o primeiro computador a ser fabricado, contudo, o mesmo era imenso e ocupava diversas salas da Universidade da Pensilvania e consumia uma quantidade grande de energia.[8]

A partir deste ponto as evoluções ocorrem de forma acelerada com destaque para as principais:

- 1951 - lançamento do UNIVAC - primeiro computador vendido comercialmente;
- Anos 60 - o transistor substitui as válvulas, proporcionando uma redução no tamanho das máquinas;
- Anos 70 - Microprocessador;

---

tipógrafo, do código morse à localização por Global Positioning System (GPS), da carta ao e-mail, do telegrama à videoconferência. Se a velocidade com que as informações circulam hoje cresce cada vez mais, a velocidade com que os meios pelos quais essa informação circula e evolui também é espantosa". Pinheiro, Patricia Peck. Direito Digital, São Paulo: Saraiva, 2010.

[6] "... em las postrimerías del siglo XIX la aparición de la fotografia instantánea y el avance de la tecnologia que permitió multiplicar las ediciones de los medios masivos de comunicación, trajeron como consecuencia la difusión con una qamplitud hasta el momento desconecida de hechos y eventos, los cuales afectaban la intimidad de las personas. Lhevando a que la doctrina y luego la jurisprudencia tuvieran que forzosamente redefinir el concepto de ïntimidad". Anzit Guerrero, Ramiro El derecho informático y sus aspectos fundamentales, Buenos Aires: Catedra 2010.

7 Tobares Catala, Gabriel H. Delitos Informáticos, Cordoba: Advovatus, 2010 pag.

[8] *"..los científicos Eckert y Mauchly desenrrollaron em 1946 una máquina electronica a la cual nombraran ENIAC (Eletronic Numerical Integrator and Calculator), la cual si bien era quinientas veces má rápida que sus antecesoras, ocupaba un espacio de casi 150 kilómetros cuadrados, y utilizaba un absurdo consumo de energía, a tal punto que un director de IBM, em alguna oportunidad, llegó a decir que era inaudito pensar em computadores u ordenadores hogareños. Más tarde reconocería su gran error".* Rosende, Eduardo E. Derecho penal e informática, Buenos Aires: Fabián J. Di Placido, Editor, 2007.

- 1981 - Computador com “mouse”e interface gráfica;
- 1982 - Computador pessoal;
- 1989 - Linguagem HTML (Hyper Text Markup Language);
- 1996 - Google (buscador);
- 2001 - Wikipedia (enciclopédia on line);
- atualmente - Facebook - Iphone - Ipad - Tweeter, Skype, WhatsApp.

Para ilustrar o avanço tecnológico, utilizaremos um quadro esquemático da obra de Eduardo R. Rosende (2007)[9]:

Generación	Nombre	Componentes
Primera (1951-1959) Caracterizada por el uso de tubos de vácio	Univac 1	Compuesta po un procesador de mercurios y unidades de cintas magnéticas, utilizado por el gobierno de Estados Unidos y por la caderna de noticias CBS News.
	IBM 701	Procesador de memoria electrostática y cintas magnéticcas
	IBM 650	Com esta máquina, IBM se convertió em lider del sector Informático
Segunda (1959 - 1962) Caracterizada por el uso de transistores	IBM 1400 y 1700 y la UNIVAC 1107 entre otras	El mercado em esta época era liderado por dos sectores. IBM por un lado, y el denominado BUNCH (conformado por las empresas Bourougs, UNIVAC. CDC y Hineywell)
Tercera (1963-1971) Caracterizada por el uso de circuitos integrados.	IBM 360, serie 600 da General Eletric, 1108 da UNIVAC. Intel introdujo el primer chip de RAM em 1970 y tenia una capacidad de 1 Kb	Em esta etapa comezaron a aparecer nuevos productores, y los costos de fabricación fueron haciendose menos onerosos, com la consecuente disminución del precio de venta, comenzándose a utilizar el TELEPROCESO (conexión entre terminales Ubicadas a distancia)
Cuarta (desde 1971) Circuitos integrados em gran escala	IBM lanza la serie PC (personal com-puter), vendiendo 830.000 entre 1981 y 1982 com el sistema operativo de disco (DOS) de Microsoft	Com la utilización de los sistemas VLSI(Very Large ScaleIntegration), se permitió comenzar a trabajar com palabras de 8 bits, llhegando hoy días las posibilidades hasta 128 bits, y lo importante es la miniaturización. Em esta etapa, aparecieron las maquinas Apple

[9] - Rosende, Eduardo E. Derecho penal e informática, Buenos Aires: Fabián J. Di Placido, Editor, 2007, pág. 38.
:

2. INTERNET E A REGULAMENTAÇÃO BRASILEIRA

Durante a curta, mas intensa história da internet[10], tem sido possível cometer crimes e permanecer impune. Isto dá mais coragem e incentivo para que criminosos migrem para esta modalidade delituosa, o que só faz aumentar a cibercriminalidade.

A impunidade no mundo virtual muito se dá a problemas nas legislações existentes, como a falta de previsão legal para a tipificação do delito, a falta de uma previsão de cooperação penal e processual entre estados soberanos. A soberania que antes era a proteção de um estado passou a ser aliada dos cibercriminosos para a garantia de sua impunidade.

No Brasil, Pinheiro (2010) destaca dois fatos essenciais para o amadurecimento de várias questões jurídica. "1990, ano da criação do primeiro

---

[10] Durante a Guerra Fria buscou-se um sistema de interligação de redes, tendo como objetivo o uso militar.

Segundo Pinheiro[10] **"Esse método revolucionário permitiria que, em caso de ataque inimigo a alguma de suas bases militares, as informações lá existentes não se perderiam, uma vez que não existia uma central de informações propriamente dita".**

Inevitavelmente, este sistema passou a ser utilizado por civis, inicialmente no meio acadêmico, mas avançando para o lado comercial no final da década de 80. "Fue entonces cuando, bajo el auspicio de la Agencia de Programas Avanzados de Investigación (ARPA) em un programa dirigido por Robert Khan, Vinton Cerf desarrolló em 1973 los protocolos TCP/IP (protoloco de control de la transmisión/protocolo entre redes), base de la actual Internet." (Tobares Catala:2010).

Apresentando grandes atrativos, como por exemplo o correio eletrônico, a expansão da Internet era inevitável e ganhou inigualável impulso com o desenvolvimento do World Wide Web ou WWW, como é conhecido. Para Pinheiro:

"Tecnicamente, a Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos IP (abreviação de Internet Protocol), ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra ótica, satélite, ondas de rádio ou infravermelho, A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na Internet por meio de um browser, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do website indicado, exibindo na tela do usuário textos, sons e imagens".

O autor argentino Tobares Catala entende que a Internet não é um corpo físico ou tangível, senão uma rede gigante que interconecta uma inumerável quantidade de redes locais de computadores.

Para a doutrina policial adotada pela Academia Nacional de Polícia (ANP – Brasil) "'A Internet é um local de crime real e, portanto, deixa vestígios como registros de conexão à Internet, registros de utilização de serviços na Internet (envio e recebimento de e-mails, registros de trocas de mensagens, download de arquivos, entre outros), além, obviamente, dos próprios computadores utilizados para a prática criminosa". Este pensamento é discutível e ainda busca uma solidificação, dependendo de seu posicionamento final, muito deverá ser rediscutido, como vemos na obra Direito Digital:

"Se entendermos que a Internet é um lugar, então muitas questões do Direito devem ser redesenhadas, uma vez que o próprio território ou jurisdição deveria ser a própria Internet. Se entendermos que a Internet é um meio, então voltamos a ter de resolver a questão da territorialidade para a aplicação da norma, já havendo como referência a atuação do Direito Internacional".

Podemos destacar ainda, e cada vez mais recente e de presentes e futuros impactos, o Cloud Comput que trata da virtualização no armazenamento de informações, e o advento das redes sociais como **Orkut** e **Facebook,** para citar apenas algumas que estiveram ou estão com papel determinante em diversos tipos de mobilização, quer seja de cunho político ou não. SOBRAL e BEZERRA, In Inquérito Policial, Doutrina e Prática, AGNOLETO e BEZERRA Organizadores, São Paulo, Letras Jurídicas, 2015.

Código Brasileiro de Defesa do Consumidor e 1995, quando o Ministério das Comunicações publicou a norma 001, que regula o uso de meios da rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à internet, marcando o nascimento comercial do sistema no país".

A origem da tentativa de regulamentação legislativa sobre os assuntos ligados a internet começa com a Ordem dos Advogados do Brasil (OAB) em 1999 com uma comissão criada especialmente para redigir um modelo para a lei a ser apresentada ao Congresso Nacional. Contudo, tratava-se de uma regulamentação de comércio eletrônico (validade de documentos eletrônicos e assinatura digital).

A falta de regulamentações da internet no cenário brasileiro transfere ao poder judiciário a sua regulamentação através de decisões judiciais, ou seja, o judiciário acaba legislando em cima de casos concretos, como explica Lemos[11] "Com isso, a regulamentação da internet brasileira é feita primordialmente por "regras gerais" que têm como consequência transferir a decisão do equilíbrio de interesses ao Poder Judiciário, mas sem dotá-lo de regras claras para tanto, o que aumenta ainda mais a incerteza". Tal procedimento é perigoso e pouco prático, pois em matéria penal o juiz encontra-se amarrado ao princípio da legalidade e nos outros campos do Direito a demora da resposta jurídica pode fazer uma decisão tornar-se completamente inócua.

Em 2003 foi criado o Comite Gestor da Internet (CGI.br) com o objetivo de administrar recursos da rede. Tal organismo é composto por membros do governo, setor empresarial, da comunidade acadêmica, etc.

Especificamente sobre a nossa área de atuação e enfoque do estudo, existiam em tramitação no congresso brasileiro o projeto de lei 89/2003, de autoria do Deputado Luiz Piauhylino e com substitutivo do relator Senador Eduardo Azeredo, que definia os crimes de informática, e o projeto do Deputado Paulo Teixeira que foram votados e transformados em lei no ano de 2012, leis 12.737/2012 e 12.735/2012, além do Marco Civil da internet, que serão abordados em capítulos adiante.

Apesar das críticas quanto a demora da aprovação das leis brasileiras que definiram os critérios e as novas tipificações dos crimes cibernéticos, sabemos que a tarefa não é fácil e que estas entraram em vigor com alguns defeitos, contudo, não podemos deixar de melhorá-las, pois estamos desamparados e dependemos de analogia e arremedos por parte do judiciário.

Nos valemos da tabela elaborada por Pinheiro (2010)[12] para demonstrar as principais inovações ou modificações jurídicas propostas nos diversos projetos de lei em tramitação no Congresso Nacional Brasileiro:

[11]Lemos, Ronaldo. Direito Tecnologia e cultura, Rio de Janeiro: FGV, 2006.
[12] Pinheiro, Patricia Peck. Direito Digital, São Paulo: Saraiva, 2010, pág 295.

NOVA CONDUTA	NOVA TIPIFICAÇÃO DE CRIME
Disseminar phishing scam (e-mails fraudulentos contendo malweres e outros códigos maliciosos)	ESTELIONATO ELETRÔNICO
Roubar senhas bancárias por meio de phishing scam	ESTELIONATO ELETRÔNICO
Falsificar cartões de crédito	FALSIFICAÇÃO DE DADO ELETRÔNICO OU DOCUMENTO PARTICULAR
Destruir, inutilizar ou deteriorar dado eletrônico alheio	DANO
Inserir ou difundir códigos maliciosos (vírus, worms, trojans, etc) em dispositivos de comunicação, rede, sistemas	INSERÇÃO OU DIFUSÃO DE CÓDIGO MALICIOSO
Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida	ACESSO NÃO AUTORIZADO
Inserir ou difundir códigos maliciosos (vírus, worms, trojans, etc) em dispositivos de comunicação, rede, sistemas causando dano	INSERÇÃO OU DIFUSÃO DE CÓDIGO MALICIOSO SEGUIDO DE DANO
Obter ou transferir dado ou informação sem autorização (ou em desconformidade à autorização)	OBTENÇÃO NÃO AUTORIZADA DE INFORMAÇÃO
Divulgar, sem autorização, informações pessoais disponíveis em banco de dados	DIVULGAÇÃO NÃO AUTORIZADA DE INFORMAÇÕES PESSOAIS
Atentado contra segurança de serviço de utilidade pública	ATAQUES A REDES E INVASÕES
Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistemas informatizados	ATAQUES A REDES E INVASÕES
Falsificação de dado eletrônico ou documento público	FALSA IDENTIDADE FALSIDADE IDEOLÓGICA DIGITAL FRAUDE
Falsificação de dado eletrônico ou documento particular	FALSA IDENTIDADE FALSIDADE IDEOLÓGICA DIGITAL FRAUDE
Preconceito	PRECONCEITO DIGITAL
Pedofilia	PRECONCEITO DIGITAL

3. DEFINIÇÕES

3.1 Definição e Classificação dos crimes cibernéticos[13].

[13] Heriberto Simon Hocsman define o delito informático como "aquellaa acciones tipicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien juridico de naturaleza colectiva o macrosocial, em cualquieira de las fases que tienen vinculación com su flujo o intercambio".

Existem vários autores que classificam os crimes cibernéticos de diversas maneiras, como o prof. Anzit Guerreo

A internet pode ser utilizada como meio para cometimento de um delito como estelionato14, por exemplo, ou pode ser o próprio. Para Tobares Catalá:15 "El problema de las actividades delictivas que implicam modernas tecnologias de computadoras, redes informática y telecomunicaciones supone um desafío importante em la justicia penal, que debe valerse de un derecho penal que no contemplan em sus normas los adelantos tecnológicos y científicos que evolucionaram com posteridad a la sanción de la ley."

3.1.1) Crimes cibernéticos próprios quando o objetivo do crime é o próprio sistema, tendo como exemplo mais específico os ataques de negação de serviço.

3.1.2) Crimes cibernéticos impróprios são aqueles que utilizam a internet ou os meios tecnológicos apenas como uma ferramenta para sua concretização. Exemplos:

- Falsificação de documentos;
- Furto;
- Estelionato.

4 .DIREITO COMPARADO E CONVENÇÃO DE BUDAPESTE

Diversos países já possuem legislações específicas para tratar as demandas relacionadas a crimes cibernéticos. Certamente contam com a expertise de ações no sentido de tentar punir o delinquente deste tipo de delito, proporcionando um sentimento de segurança em sua sociedade. Observar, criticar, aprender e adaptar tais legislações é o caminho para se buscar a resposta ao crescimento vertiginoso do cibercrime.[16]

"...toda ación (ación u omisión) culpable realizada por un se humano, tipificada por la ley, que se realiza em el entorno informático mediante el elementos informáticos, y está sancionado com una pena".

Outra classificação interessante é descrita *por Tobares Catalá (página 31)* onde transcreve a classificação elaborada por *Maria de la Luz Lima* de acordo com a utilização da tecnologia eletrônica utilizada, sendo:

- Como método – quando os métodos eletrônicos são utilizados pelos indivíduos para chegar ao resultado do ilícito;
- Como meio – quando utilizam o computador ou Internet como meio ou ferramenta para a realização de um delito;
- Como fim – quando as condutas criminosas são dirigidas contra o hardware ou seu software.

No Brasil, para a Academia Nacional de Polícia (ANP) existem ainda os **Crimes cibernéticos mistos** que se assemelham aos crimes cibernéticos impróprios, com a diferença que são potencializados pela tecnologia, a qual cria um novo *modus operandi*. Ex.: fraude bancária eletrônica.[13]

Evolução dos crimes cibernéticos no Brasil

- 1996 – Primeiros casos de pornografia infantil pela Internet;
- 1998 – Primeiros casos de clonagem de cartão;
- 2000 – Primeiros casos de fraude bancária pela Internet;
- 2002 – *Phishing*: cavalo de tróia;
- 2009 – Explosão do número de Fraudes Bancárias via cartão crédito clonado e Internet banking, chagando-se a cifra de um bilhão de dólares em prejuízos segundo a FEBRABAN (Federação Brasileira de Bancos);
- 2011 – Ataques a páginas eletrônicas do governo brasileiro como, IBGE, Receita Federal, etc.

[14] *Art 171 CPB* -

[15] Tobares Catala Gabriel H. Delitos Informáticos, Cordoba: Advovatus, 2010

[16] A Convenção de Budapeste:

A convenção de Budapeste foi firmada pelo Conselho da Europa em 23 de novembro de 2001 e entrou em vigor no ano de 2004.

Tal convenção, em seus quarenta e oito artigos, formaliza a intenção da Comunidade Europeia em unificar uma legislação visando combater o cibercrime ao uniformizar terminologias, definições e prever a cooperação

Podemos citar os seguintes países seguindo a obra de Eduardo E. Rosendo[17]

País	Ano	Assunto
Alemanha	1986	Pirataria informática, dano , alteração de dados, sabotagem de computadores etc.
Espanha	1995	Ataques que se produzem contra o direito de intimidade
Áustria	1987	Destruição de dados pessoais
Chile	1993	Lei n. 19223 (Lei de delitos informáticos, de 28 de maio de 1993)
França	1988	Lei n. 88-19 de 5 de janeiro de 1998
Estados Unidos	1986	Ata de Fraude e Abuso Computacional
Itália	1993	Art. 615 Código Penal Italiano
Venezuela	2001	Lei Especial contra Delitos Informáticos (Diário Oficial n. 37.313 de 30 de outubro de 2001)
México	1999	Reforma do Código Penal Mexicano, Artigos 210 e 2011
Bolívia	1997	Reforma do Código Penal Boliviano, Artigo 363
Costa Rica		Lei 8148 que adicionou os artigos 196 bis, 217 bis e 229 bis ao Código Penal Costarriquenho
Peru	2001	Capítulo especial sobre delitos informáticos no Código Penal Peruano, Art. 207 e seguintes
Equador	2002	Lei de Comércio, Mensagens Eletrônicas e Mensagens Eletrônicas de Dados incorpora os artigos 184, 185, 186, 415 e 416 ao Código Penal Equatoriano
Grã Bretanha	1991	Lei de Abusos Informáticos
Portugal	1991	Lei Especial 109/1991
Japão	1987	Artigos 161 bis e seguintes

internacional, fundamental em uma possibilidade de crimes que avançam por diversas fronteiras. Destacamos alguns pontos de seu preâmbulo.

- - "Convictos da necessidade de prosseguir, como caráter prioritário, **uma política criminal comum**, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional"; (grifo nosso)
- - "Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas." (grifo nosso)
- - "Preocupados com o risco de que as redes informáticas e a informação eletrônica sejam igualmente utilizadas para cometer infrações criminais e **de que as provas dessas infrações sejam armazenadas e transmitidas** através dessas redes"; (grifo nosso)
- - "Reconhecendo a necessidade de uma **cooperação entre Estados e a indústria privada** no combate à cibercriminalidade..."; (grifo nosso)
- - "... Convictos de que a presente Convenção é necessária para... e da adoção de poderes suficientes pra **combater eficazmente essas infrações, facilitando a detecção, a investigação e o procedimento criminal** relativamente às referidas infrações, tanto a **nível nacional com internacional**, e estabelecendo disposições materiais com vista a um **cooperação internacional rápida e viável**"; (grifo nosso)
- - "Tendo presente a necessidade de garantir um **equilíbrio** adequado entre os interesses da **aplicação da lei** e o respeito pelos **direitos fundamentais do ser humano**...". (grifo nosso)

Corrobora com este entendimento as palavras do professor Anzit Guerrero "La ONU considera que el problema de los delitos informáticos se eleva a la escena internacional, por cuanto éstos constituyen una nueva forma de crimen transnacional y su combate reueiere de una eficaz cooperación internacional concertada."[16]

[17] Rosende Eduardo E. Derecho penal e informática, Buenos Aires: Fabián J Di Placido Editor 2007 pag 218 / 282:

5. O FUTURO: CRIME CIBERNÉTICO X SOBERANIA X IMPUNIDADE

Granillo Ocampo (2007)[18] em sua obra Derecho Público de la Integarcion faz um resumo dos principais pensadores sobre o conceito de Estado[19], seu surgimento e finalidade. Destaca que atualmente existe uma simbiose forte entre o conceito de Estado e Soberania.

Para o renomado professor argentino, o conceito de soberania elaborado por Jean Bodin[20] em 1576 está atualmente em crise "consecuencia natural y logica de que nos constituye una categoria absoluta sino historica y que tal como fueira concebida (absoluta) no puede funcionar ni em el aspecto interno ni em el externo de un Estado".[21] [22]

Aref[23], citandoWeinert, (2007 p.28) entende que a soberania é relativa à justiça e ao bem-estar coletivo, de modo a defender a individualidade de todos os cidadãos, neste diapasão e entendendo o Cybercrime como possibilidade de ser um crime transnacional, vê-se a importância crucial de uma investigação ágil, com cooperação entre os estados ou províncias de um país e até mesmo de uma cooperação internacional eficiente.

Para Azambuja (2003):

> Quando se diz que o Estado é soberano, deve entender-se que, na esfera da sua autoridade, na competência que é chamado a exercer para realizar a sua finalidade, que é o bem público (...) a soberania de um Estado é considerada geralmente sob dois aspectos: interno e externo. A soberania interna quer dizer que o poder do Estado, nas leis e ordens que edita para todos os indivíduos que habitam seu território e as sociedades formadas por esses indivíduos (...) o termo soberania significa que o poder do Estado é o mais alto

[18] Granillo Ocampo, Raul, Derecho público de la integrción/ Raúl Granilo Ocampo; com prólogo de Julio M. Sanguinetti – 1ª ed. Buenos Aires: Ábaco de Rodolfo Depalma, 2007

[19] Platão (427-347 AC), Aristóteles (384-322 AC), Maquiavel (1469-1527), Jean Bodin, Thomas Hobbes, John Locke, Jean Jacques Rousseau, Montesquieu, Emanuel Kant,

[20] O estado é uma suma potestas, ou seja, o poder absoluto e perpétuo de uma república que se exerce nesses termos tanto dentro do Estado (em relação a seus habitantes) como internacionalmente, não se limitando nem em poder nem responsabilidades, nem tempo.

[21] Granillo Ocampo (2007), pag 73

[22] La realidad es que el siglo XIX el concepto de soberania se va separando de la pessoa del monarca y va perdiendo sus caracteristicas de absoluto, como consecuencia de que la nacion e Estado por un lado se despersonaliza y por le outro y al mismo tiempo, se constitucionalizaceandose cada vez mayor cantidad de restriciones para la administracion del viejo concepto de soberania absoluta o de poder absoluto. Estos procesos se aceleran marcadamente em el siglo XX, sobre todo despues de las grandes guerras mundiales.

Como síntesi podriamos decir que si bien estamos lejos del Estado universal, el nuevo orden internacional tiene, como caracteristica principal, la erosion del concepto de soberania, em favor del acrecentamiento de las competencias dos organismos internacionales."

[23] Aref, Flavia Regina Rebelo: O enfraquecimento da impunidade soberana: A revitalização da Soberania frente à Universidade dos Direitos Humanos e Humanitários no Cenário Pós-Guerra Fria: Cadernos Relações Inetrnacionais, V4, n. 1, 2011.

existente dentro do Estado. A soberania externa significa que nas relações recíprocas entre os Estados não há subordinação nem dependência, e sim, igualdade.

A doutrina policial adotada pela Academia Nacional de Polícia (ANP - Brasil) entende que "A internet é um local de crime real e, portanto, deixa vestígios como registros de conexão à internet, registros de utilização de serviços na internet (envio e recebimento de e-mails, registros de trocas de mensagens, download de arquivos, entre outros), além, obviamente, dos próprios computadores utilizados para a prática criminosa". [24]

Para o combate ao cibercrime transnacional é fundamental a coleta, armazenamento, lapidação e análise das diversas condutas criminosas perpetradas, visto que vários são os crimes cometidos de forma conexa e acompanhada, restando nesta ferramenta a maneira mais eficiente de se buscar os elos de ligação para a captura de criminosos e quadrilhas especializadas no cibercrimes, onde quer que eles se encontrem, no território pátrio ou estrangeiro.

6. CONCLUSÃO

Nossas vidas mudam, assim como nossos pensamentos, inclusive repercutindo sobre nosso modo de falar e escrever. O que era importante hoje, já não o é amanhã. O que é indecente aqui, é fato normal no estado vizinho, a grafia atual não é a mesma de outrora. Cada dia trará um fato prático novo, isto obrigará o "julgador" a interpretar a norma ou a falta desta.

Um novo mundo se apresentou para a humanidade e teremos que lidar com suas características, tanto as benignas quanto as malignas. O mundo "virtual" é uma realidade e necessitamos interpretar e ajustar nossas legislações para aplicarmos a essa realidade, pois os conflitos neste novo cenário já se fazem presentes e possuem características não pensadas em nossa realidade pretérita. Alguns dos paradigmas do nosso mundo "concreto" não são aplicáveis, ou o são de maneira ineficaz no caso concreto.

Com um mundo (virtual), completamente novo e diferente, tipos penais, locais de crime, assim como jurisdição e competência de juízos precisam ser interpretados sob novos princípios de Direito.

[24] Este pensamento é discutível e ainda busca uma solidificação, dependendo de seu posicionamento final, muito deverá ser rediscutido. Muito se deve ao desconhecimento dos operadores do direito, juízes e promotores de justiça. Como exemplo tem-se a obra Direito Digital[24]: "Se entendermos que a Internet é um lugar, então muitas questões do Direito devem ser redesenhadas, uma vez que o próprio território ou jurisdição deveria ser a própria Internet. Se entendermos que a Internet é um meio, então voltamos a ter de resolver a questão da territorialidade para a aplicação da norma, já havendo como referência a atuação do Direito Internacional". BEZERRA E SOBRAL in Inquérito Policia,l Doutrina e Prática, São Paulo: Letras Jurídicas, 2015

O Direito Penal e Processual Penal, precisam ser repensados visando adequar a legalidade das ações com a realidade mundial, integrando os objetivos de prevenção e repressão da criminalidade, além da busca de uma maior eficiência por parte dos Estados. Tal caminho já foi iniciado pela República da Argentina e diversos países da América Latina e também de outros continentes do mundo. O Brasil precisa acelerar a sua caminhada.

Até mesmo a soberania, antes entendida como o poder dos Estados de ter política exclusiva dentro de seus territórios, começa a dar lugar a um novo conceito de responsabilidade nacional e internacional em que os direitos humanos e outros fatores forçam o Estado a ceder parte de sua soberania para o bem maior. Acreditamos que a internet e a necessidade de se combater os cibercriminosos em delitos transnacionais irão acelerar tal processo de mudança. "La nueva realidad global, caracterizada por una creciente interdependencia mundial a nível ecológico, politico, militar, económico etc., requiere una ruptura com el paradigma realista".[25]

[25] - Salmón, Elizabeth. El crimen de agresión despues de Kampala: soberania de los estados y lucha contra la impunidad: Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú 2011

7. REFERÊNCIAS

ANZIT GUERRERO, Ramiro, El derecho informático y sus aspectos fundamentales, Buenos Aires: Cathedra Jurídica 2010

AREF, Flavia Regina Rebelo, O enfraquecimento da impunidade soberana: A revitalização da soberania frente à universidade dos direitos humanos e humanitários no cenário pós-guerra fria: Caderno de relações Internacionais, V4, n. 1, 2011

BEZERRA e AGOLETTO, Clayton da Silva e Giovani Celso, Org. Inquérito Policial: Doutrina e prática; São Paulo; Letras Jurídica, 2015

GRANILLO OCAMPO, Derecho público de la integración, Buenos Aires: Ábaco de Rodolfo Depalma 2007

LEMOS, Ronaldo, Direito tecnologia e Cultura, Rio de Janeiro: FGV 2005

PINHEIRO, Patricia Peck, Direito digilal, São Paulo: Saraiva 2010

ROSENDE, Eduardo E., Derecho penal e informática, Buenos Aires: Fabián J Di Placido Editor 2007

SUEIRO, Carlos, Analisis integrado de la criminalidade informática, Buenos Aires: Fabián J Di Placido Editor 2007

TOBARES CATALA, Gabriel H, Delitos informáticos, Cordoba: Advocatus 2010

Capítulo II

Dos crimes cibernéticos (Lei 12.737/12)

Luiz Augusto Pessoa Nogueira[26]

Com o crescimento da internet no Brasil, é cada vez mais comum nos depararmos com crimes cujos atos preparatórios ou executórios são realizados por meio do ambiente cibernético.

Nesse sentido, em 2013 passou a vigorar a Lei 12.737, que alterou o Código Penal trazendo a tipificação criminal das condutas que a própria lei denomina de delitos informáticos. Com isso, condutas que até então eram consideradas atípicas ou ilícitos civis passaram a ser tipificadas criminalmente:

> **"Invasão de dispositivo informático**
> **Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

[26] O Autor é Especialista em Inteligência de Estado pela Escola Superior do Ministério Público de Minas Gerais, Delegado de Polícia Federal e foi Chefe da Delearm (2005/2007), Chefe da Delepat (2007/2009), Chefe do NIP (2010) e chefe do Grupo de Repressão a Crimes Cibernéticos de 2012 à 2015.

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Além disso, a nova lei altera os artigos 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, que passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

"Falsificação de documento particular
Art. 298
Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR)

Referido dispositivo legal, conhecido como Lei Carolina Dieckmann, em virtude da lei ter sido aprovada pouco depois de atriz de mesmo nome ter sido vítima de invasão de seu computador por terceiros não autorizados, entrou em vigor no dia 02 de abril do ano de 2013, portanto, 120 dias após sua publicação no Diário Oficial da União (03/12/2012).

Apesar disso, referida lei já vinha sendo discutida há anos no congresso nacional, sendo uma resposta do Estado brasileiro a uma demanda social para condutas que há muito necessitavam de tipificação penal.

Com efeito, não se trata de simples percepção coletiva, estatisticamente o crime vem, há algum tempo, migrando do mundo virtual para o mundo real. Ou seja, paradigmas sociais em mudança e evolução exigem um aprimoramento da legislação penal, a fim de evitar, ou pelo menos mitigar, a impunidade dos chamados crimes cibernéticos próprios (aqueles que só podem ser praticados através da internet) e impróprios.

Se levarmos em consideração que o direito penal é a "ultima ratio" do direito, em que a intervenção mínima é critério para o legislador discutir, votar e aprovar regras na seara penal, podemos concluir que o Estado brasileiro, através de seus representantes no congresso nacional, entendeu que determinados direitos e bens virtuais ou cibernéticos do cidadão brasileiro merecem grande proteção do Estado, daí a razão de serem tutelados pelo direito penal após a entrada em vigor da Lei 12.737/12. E isto se justifica pela grande adesão da sociedade brasileira ao mundo digital. Qual pessoa, física ou jurídica, inserida dentro de um contexto de cidadania total no Brasil, não depende de algum dispositivo informático, desde um simples "pendrive", aos mais complexos smartphones (pessoa física) ou poderosos servidores de dados (pessoa jurídica)?

Como primeira medida, a Lei 12.737/12 criou o delito de "invasão de dispositivo informático", assim definido no caput do Art. 154-A:

> **Art. 154-A** Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
>
> Bem jurídico protegido: privacidade, gênero do qual são espécies a intimidade e a vida privada.
> Sujeito ativo: qualquer pessoa (crime comum).
> Sujeito passivo: titular do dispositivo informático.

Em relação ao sujeito passivo, cabem algumas observações. Via de regra, a vítima será o proprietário do dispositivo informático, seja ele pessoa física ou jurídica. Todavia, em algumas situações, na verdade bem comuns de acontecer, o sujeito passivo poderá ser a pessoa que efetivamente faz uso do dispositivo informático para armazenar informações ou dados pessoais. Por exemplo, em um desktop utilizado por uma família, o principal usuário é o filho mais velho do casal (que é o real proprietário do computador), que armazena arquivos e dados pessoais no computador invadido. Ainda que não seja o proprietário do dispositivo informático invadido, o jovem foi vítima do crime de invasão de dispositivo, pois como visto acima, o bem jurídico tutelado pela norma é a privacidade e não a propriedade.

Elementares do tipo:

Já no que diz respeito às elementares do tipo penal, a par da obviedade de algumas, outras merecem alguns comentários.

Nossa primeira observação diz respeito ao conceito de "invasão" e sua abrangência. Em nosso entendimento, "invadir", no sentido virtual ou cibernético, "é todo ato, sem autorização, que, de forma física ou virtual, consegue acessar dispositivo informático, quer seja pelo uso da força ou coação, quer seja de modo ardiloso". Resumindo, entrar em um dispositivo ou um sistema sem autorização do (s) proprietário (s).

A expressão "dispositivo informático" deve ser entendida como qualquer equipamento passível de ser conectado a uma rede ou a um computador, HDs, pendrives, smartphone, inclusive os chamados equipamentos periféricos, como uma impressora.

A elementar "conectado ou não à rede de computadores", aumenta a abrangência da conduta criminosa, deixando claro que um tablet ou uma impressora, mesmo não estando conectados à internet, podem ser objeto do crime de invasão de dispositivo.

Observação importante acerca desse tipo penal, que o difere de outros crimes, é a elementar "mediante violação indevida de mecanismo de segurança". Isto implica afirmar que só haverá o crime de "invasão de dispositivo informático" caso exista algum mecanismo de segurança no referido dispositivo, por mais simples que seja.

Vale dizer que acessar o computador de um colega de trabalho durante sua ausência, mesmo tendo acesso a dados ou informações íntimas do titular do dispositivo, não configurará o crime analisado. Em nosso entendimento, trata-se de um equívoco, pois a privacidade alheia estará sendo violada da mesma maneira, todavia, a conduta, ainda que moralmente reprovável, não será penalmente punível.

"Com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo...". A situação prevista nesta elementar pode ser ilustrada com o caso da atriz Carolina Dieckmann, pois seu computador foi invadido para a obtenção de fotos íntimas!

CUIDADO: se uma empresa contrata um hacker para testar a vulnerabilidade de seus sistemas, não haverá crime, obviamente, pois caso a invasão ao dispositivo do tipo penal seja autorizada, o fato é atípico!!!

Da mesma maneira, professores de cursos de informática/computação ou funcionários de empresas que desenvolvam softwares espiões para testar segurança de redes e a defesa contra ataques ou invasões não autorizadas, não estarão cometendo o crime de invasão de dispositivo informático em virtude da ausência do elemento subjetivo do crime (com o fim de obter, adulterar ou destruir dados ou informações...).

"Ou com o fim de instalar vulnerabilidades para obter vantagem ilícita". Situação que pode ser ilustrada através do envio de e-mails contendo o malware "trojan horse", onde o objetivo do agente criminoso é obter senhas e usuários da vítima em sites de bancos e outros dados pessoais.

Elemento subjetivo: O dolo com especial fim de agir, ou seja, é um crime com dolo específico (com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou "instalar vulnerabilidades para obter vantagem ilícita").

Considerações gerais sobre o "caput" do Art. 154-A:

Trata-se de infração de menor potencial ofensivo, portanto, a competência para julgamento de eventual crime será do Juizado Especial Criminal (Art. 61 da Lei 9.099/95). Em princípio, consoante regra prevista no Art. 69 da Lei 9.099/95, a investigação deverá ser feita através da lavratura de Termo Circunstanciado, entretanto, a complexidade na apuração da autoria e materialidade do delito de invasão de dispositivo informático, que muitas vezes irá demandar requisição de dados cadastrais, perícia em computadores, busca e apreensão, interrogatórios de testemunhas, etc, provavelmente ensejará a instauração de Inquérito Policial.

Consumação: por tratar-se de crime formal, consuma-se com a invasão. Sendo assim, a obtenção, adulteração ou destruição de dados ou a instalação de vulnerabilidades serão mero exaurimento do delito informático "invasão de dispositivo".

Tentativa: Admite-se a tentativa. Ex. agente inicia os atos executórios para invasão do equipamento (computador), todavia, por razões alheias a sua vontade, não consegue violar os dispositivos de segurança.

Pena: A pena para o delito informático previsto no "caput" do Art. 154-A (detenção de 03 meses a 01 ano, e multa) é baixa, apresentando mais um componente de caráter psicológico para a prevenção do crime do que uma efetiva punição ao autor.

Condutas equiparadas:

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

No parágrafo primeiro, o legislador equiparou ao crime de "invasão de dispositivo informático" a conduta de produzir softwares maliciosos (malwares) e sua disponibilização.

Outra observação importante acerca do parágrafo em análise, é que ele fala em "dispositivo ou programa de computador", ou seja, em hardware e software. Vale dizer que a produção e a disponibilização de hardwares utilizados para a invasão não autorizada de dispositivos ou sistemas informáticos, como o simulacro conhecido como "chupa-cabra", também é punida.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

Entendemos que o prejuízo econômico resultante da invasão de dispositivo informático diz respeito aos danos materiais (formatação, troca de equipamentos, etc) e aos lucros cessantes de quem trabalha com o dispositivo ou nele guardou dados e informações que iriam ser utilizadas para atividade profissional (apresentação de uma palestra remunerada, por exemplo).

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Invasão qualificada de dispositivo informático

Em relação ao parágrafo 3º da Lei 12.737, cabe observar que, diferentemente das informações ou dados de caráter genérico previstos no "caput", o dispositivo em foco está tutelando segredos comerciais ou industriais e informações sigilosas definidas em lei, daí a razão da conduta ser qualificada.

Este parágrafo qualifica, ainda, a invasão que resultar em controle remoto do dispositivo invadido. Exemplo clássico são os dispositivos controlados remotamente a serviço de uma "botnet".

Por derradeiro, cumpre diferenciar o crime de "obtenção de conteúdo de comunicações eletrônicas privadas" previsto no § 3º da Lei 12.737/12, do crime de interceptação de comunicações telefônicas, de informática ou telemática, tipificado pelo Art. 10 da Lei 9.296/96.

Enquanto o crime de "obtenção de conteúdo de comunicações eletrônicas privadas" diz respeito a comunicações já realizadas e arquivadas em dispositivo informático (ou seja, do momento da obtenção das comunicações para trás, passado), o crime de interceptação de comunicações telefônicas, de informática ou telemática, diz respeito a comunicações realizadas a partir da implementação da interceptação (ou seja, do momento da interceptação para frente, futuro).

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

O § 4º é uma causa de aumento de pena específica do delito descrito no § 3º, bastando, para tanto, a divulgação, comercialização ou transmissão, a terceiro, das comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal".

Outra causa de aumento de pena prevista para o crime de invasão de dispositivo informático é a descrita no parágrafo 5º do Art. 154-A. Trata-se de aumento de pena para o caso do crime ser praticado contra determinadas autoridades. Neste caso, o que se quer tutelar é a função desempenhada pela autoridade e não o indivíduo.

Esta causa de aumento de pena vale tanto para o "caput" quanto para o § 3º. Desta maneira, o crime de invasão de dispositivo informático, que em sua forma simples tem pena de 03 meses a 01 ano, em sua forma qualificada (§ 3º), com a causa de aumento prevista no § 4º e cometido contra determinadas autoridades (§ 5º), poderá ter pena de até 60 meses (05 anos).

> **Art. 154-**B. Nos crimes definidos no Art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos".

A fim de preservar a intimidade da vítima, ordinariamente, o crime de invasão de dispositivo informático será de ação pública condicionada a representação. Ora, a intimidade e a vida privada, ainda que protegidos constitucionalmente, são bens disponíveis do indivíduo/vítima, que mais que qualquer pessoa, tem melhores condições de avaliar se deseja ou não uma investigação policial e um eventual processo penal em virtude do crime de invasão de dispositivo informático que sofreu, que poderá ensejar outros constrangimentos a partir da divulgação para investigadores, delegado, serventuários, juiz e promotor, das circunstâncias que envolvem o crime, inclusive fotos, mensagens eletrônicas, dados sigilos, etc., é o chamado *streptus iudici*.

Sendo assim, é imprescindível que seja oferecida representação pela vítima, a fim de iniciar qualquer investigação sobre o fato tido por criminoso (Art. 5º, § 4º do CPP).

As exceções estão previstas na 2ª parte do Art. 154-B, que decretou ação pública incondicionada para os casos em que o crime de invasão de dispositivo informático seja cometido contra "a administração pública direta ou indireta de

qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos".

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

> **Art. 266**. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um (01) a três (03) anos, e multa.
> § 1 Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)

Além de criar os delitos informáticos vistos acima, a Lei 12.737/12 inseriu os parágrafos 1º e 2º ao artigo 266 do Código Penal, tipificando penalmente a conduta daquele que interromper serviço **telemático ou de informação de utilidade pública**.

Interessante observar no parágrafo 1º que o ato de interromper o serviço telemático ou de informação de utilidade pública passou a ser considerado crime, todavia, em atendimento ao princípio do *Nullum crimen, nulla poena sine praevia lege poenali*, positivado no Art. 1º do Código Penal (*"Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal."*), o ato de perturbar o serviço telemáticou ou de informação de utilidade pública **não é**, o que, em nosso entendimento, foi um lapso cometido pelo legislador.

Ainda analisando o § 1º, temos que definir o que podemos entender como "serviço de informação de utilidade pública". Segundo a melhor doutrina do Direito Administrativo pátrio, serviços de utilidade pública são aqueles em que a Administração, admitindo sua utilidade e conveniência (não é essencial nem necessário) para a coletividade, os presta diretamente ou concorda que terceiros o façam, através da concessão, permissão ou autorização de determinado serviço ou atividade. Ademais, a corroborar este entendimento, o tipo penal em apreço foi inserido no Título VIII - Dos Crimes Contra a Incolumidade Pública, capítulo II - Dos Crimes Contra a Segurança dos Meios de Comunicação e Transporte e Outros Serviços Públicos, do Código Penal, ou seja, podemos ler o tipo penal da seguinte maneira: " § 1º Incorre na mesma pena quem interrompe serviço **público** telemático ou de informação de utilidade pública....". Já por serviço de informação leia-se veículo oficial de informação de serviço público (dependendo de norma regulamentadora, pode ser sítio eletrônico oficial).

“Falsificação de documento particular
Art. 298. Falsificar no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.
Falsificação de cartão
Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito”. (NR)

Por fim, a Lei 12.737/12 acrescentou o parágrafo único ao artigo 298 do CP equiparando o cartão de crédito ou débito a documento particular. Isto vale dizer que a mera falsificação de um cartão, seja ele de débito ou de crédito, é considerada crime, não havendo necessidade, portanto, de o cartão falsificado ser utilizado para outros delitos para imputação penal ao agente. É CRIME AUTÔNOMO!

Observações acerca do uso de cartões clonados

Conforme já pacificado na jurisprudência do STJ e do STF, a conduta do indivíduo que utiliza cartão de débito falsificado (clonagem) para realizar saques ou transferências a partir da conta bancária do titular, configura o delito de furto qualificado previsto no Art. 155, § 4º, II do Código Penal. Por outro lado, o uso de cartões clonados para a realização de compras em estabelecimentos comerciais configura o delito de estelionato (Art. 171 do CP), consoante recentes julgados do STJ.

Apesar de parecer estranha esta distinção, na realidade, o que diferencia estes crimes é a participação ou não da vítima na entrega de seu patrimônio ao fraudador. Enquanto no crime de furto qualificado através de cartões clonados o agente simplesmente subtrai ou retira o valor da conta da vítima, sem qualquer participação desta última, no caso de compra em estabelecimento, o agente induz o comerciante/vítima a erro, fazendo com que este entregue seu patrimônio ou produto ao fraudador.

Portanto, a principal diferença entre o delito de furto qualificado mediante fraude e o estelionato é a de que naquele (crime de furto qualificado) não há a participação e concordância da vítima para que a fraude seja perpetrada, ou seja, a vítima não concorre para o crime. Já no estelionato, a vítima, voluntariamente, entrega os seus dados sigilosos ao criminoso, pois tem convicção de que está agindo da maneira correta.

Esta distinção é importante para fins de fixar a competência jurisdicional e a circunscrição da Polícia Judiciária. Isto porque, no crime de furto qualificado mediante fraude a consumação do delito será o local onde está situada a agência bancária da vítima, no estelionato, a consumação da infração será o local em que foi praticada a fraude, sendo, portanto, indiferente a localização da agência bancária da vítima.

De certa maneira, para fins de inquérito policial, esta discussão restou ultrapassada a partir da implementação do Projeto Tentáculos (que será estudado adiante), em que são analisadas, tratadas e contextualizadas várias ações delituosas praticadas por uma quadrilha a fim de determinar o melhor local para se promover a investigação, ao contrário da forma tradicional, em que era investigada a prática de apenas um fato criminoso, de forma isolada e descontextualizada das demais ações criminosas praticadas pela quadrilha.

Outra questão interessante acerca dos crimes de estelionato e furto qualificado através do uso de cartões (falsificados) diz respeito ao concurso material com o crime do artigo 298, após a inserção do parágrafo 1º pela Lei 12.737/12.

Ainda que sejam crimes que protegem bens jurídicos distintos (o crime de falsidade protege a fé pública e os crimes de furto qualificado e de estelionato protegem o patrimônio), quando o mesmo agente cometer ambos os crimes (falsidade documental e uso de cartão clonado, seja para furto, seja para estelionato), entendemos ser o caso de aplicação do princípio da consunção expresso na Súmula 17 do STJ: "Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido".

Exemplificando: O agente que falsifica ou clona um cartão de débito ou de crédito e posteriormente o utiliza para realização de compras em estabelecimento comercial estará cometendo apenas o crime de estelionato, caso não haja maior potencialidade lesiva.

Importante destacar que algumas condutas já estavam amparadas no Código Penal, como a divulgação de informações públicas de caráter sigilosas ou reservadas é punida com penas que variam de 01 a 04 anos de detenção, nos termos do § 1º -A do Artigo 153 do Código Penal. Assim, um "hacker" que invadir uma base de dados do governo e divulgar informações classificadas estará praticando o delito previsto no artigo abaixo transcrito:

> **Divulgação de segredo**
> § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000)
> Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa.

No caso do ataque de negação de serviço, convém transcrever o artigo 265 do Código Penal o qual prevê uma pena de 01 a 05 anos de reclusão a quem atentar contra o funcionamento ou segurança de qualquer serviço de utilidade pública que coloque em risco a incolumidade pública:

Atentado contra a segurança de serviço de utilidade pública
Art. 265 - Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública:
Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.
Também é crime a alteração de dados promovida pelo servidor público em base de dados da própria administração, nos termos do artigo 313-A do Código Penal:

Inserção de dados falsos em sistema de informações
Art. 313 - A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000).
Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.

Assemelham-se aos crimes cibernéticos impróprios, com a diferença de que o uso da tecnologia não é meramente circunstancial ou acidental. A informática, nesse caso, potencializa a ofensividade e alcance de tais delitos, o que leva ao surgimento de um *modus operandi* especial, tanto para a prática do crime, quanto para a sua investigação.

Os dois exemplos, por excelência, deste tipo de crime são a fraude bancária eletrônica (artigo 155, § 4.º, II, CP) e os delitos relativos à pornografia infantil na internet (ECA - Artigo 241 e ss).

Capítulo III

Aspectos penais do Marco Civil da Internet

Pablo Barcellos Bergmann [27]

1. INTRODUÇÃO

Após longa discussão no Congresso Nacional, no dia 24/04/2014 foi publicada a Lei 12.965/2014, conhecida como "Marco Civil da Internet", que "*estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil*". O Art. 32 estabeleceu que a lei entraria em vigor após transcorridos 60 dias da publicação, o que ocorreu em 23/06/2014.

Pretendemos aqui discorrer sobre as implicações do Marco Civil nas investigações criminais, especialmente quanto a obtenção de dados cadastrais e de conteúdo mantidos por empresas nacionais e estrangeiras, analisando as dificuldades e resistências que se apresentam nesse processo.

Consideraremos que o leitor possui entendimento básico dos conceitos relativos ao funcionamento da internet. O Art. 5º do marco civil descreve a terminologia utilizada pela lei para alguns desses conceitos. O "*log de IP"*, por exemplo, é chamado de "registro de conexão" ou "registro de acesso", conforme se refira à informação mantida pelo provedor de acesso à internet ou pelo provedor de "aplicações de internet". Estas, por sua vez, são definidas como o "*conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet*". Ou seja, comumente os "sites" ou serviços utilizados por quem se conecta à internet, como os buscadores, redes sociais, serviços de e-mail, *internet banking,* etc. Enfim, qualquer serviço ou utilidade, público ou privado, disponibilizado na internet.

Todas as citações de artigos que não indiquem o diploma legal respectivo referem-se à Lei nº 12.965/2014.

[27] Pablo Barcellos Bergmann é Pós-graduado em Direito Judiciário. Delegado de Polícia Federal desde 2008. Professor da Academia Nacional de Polícia. Atua na área de Crimes Cibernéticos há 3 anos, exercendo desde 2015 a Chefia da Unidade de Repressão à Pornografia Infantil.

2. DA DISPONIBILIZAÇÃO DE DADOS CADASTRAIS E CONTEÚDO

Na Seção II do Capítulo III a Lei trata da "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas". Em linha com os princípios elencados em seus Arts. 2º e 3º, a primeira disposição da referida Seção é a seguinte:

> *"**Art. 10.** A guarda e a **disponibilização** dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
> *§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no Art. 7º.*
> *§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do Art. 7º.*
> *§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. (...)"*

Leituras apressadas - ou, mais comumente, enviesadas - do texto podem indicar que a liberdade de expressão ou a proteção dos dados pessoais estariam acima de outros princípios constitucionais, o que não ocorre no sistema legal brasileiro, onde não existem princípios absolutos, eis que diante de conflitos aparentes estes devem ser harmonizados.

Os grifos acima têm a função de ressaltar que a lei, ao garantir a privacidade e intimidade do usuário, não ignorou que ocasiões existem em que esses valores serão sopesados diante de outros de igual importância, como o respeito aos direitos humanos[28], a vedação ao anonimato (Art. 5º, IV, da CR/88), a "responsabilização dos agentes de acordo com suas atividades" (Art. 3º, VI) e a garantia do *jus puniendi* estatal. Não seria possível à lei conferir à internet a qualidade de "território sem lei", onde qualquer um pudesse praticar atos

[28] Expressão que foi banalizada e apropriada por determinados grupos que não hesitam em bradá-la diante de toda e qualquer situação que seja contrária a seus interesses. Recordamos que entre os direitos básicos de todo ser humano estão o direito à liberdade, segurança e à proteção contra qualquer discriminação. Criar ambientes livres para a prática de crimes, impedindo ou impossibilitando a responsabilização dos ofensores, constitui, sem dúvida, violação a esses direitos.

criminosos impunemente, se escudando em um anonimato falsamente baseado na "garantia da privacidade".

Extrai-se do dispositivo acima transcrito que foram estatuídas as seguintes obrigações aos provedores[29]: **a**) guardar os registros de conexão e acesso; **b**) disponibilizar esses registros na forma do § 1º; **c**) disponibilizar o conteúdo das comunicações privadas na forma do § 2º; **d**) informar dados cadastrais a autoridades administrativas, na forma do § 3º.

Quanto ao item "**a**", a lei estabeleceu o prazo de 1 ano para os provedores de conexão (Art. 13) e de 6 meses para os provedores de aplicações de internet (Art. 15). Em ambos os casos os prazos podem ser prorrogados a pedido da Autoridade Policial ou administrativa ou do Ministério Público, na forma dos §§ 3º e 4º do Art. 13. Evidentemente os prazos legais equivalem ao período mínimo que os provedores devem guardar os dados. A manutenção dessa informação é uma medida que garante a segurança da própria empresa, que poderá demonstrar através dos registros qual usuário foi responsável por determinada ação, o que pode ser de extrema valia, por exemplo, em situações de danos decorrentes de conteúdo gerado por terceiros[30] (Art. 18 e ss. da lei).

Com relação à letra "**b**", temos que os registros de conexão e acesso - "de forma autônoma ou associados a outras informações que possam contribuir para identificação do usuário" -, devem ser obtidos conforme o procedimento previsto no Art. 22.

Apesar de o § 1º do Art. 10 conter a expressão "somente será obrigado a disponibilizar", o que poderia sugerir que o provedor responsável pela guarda pudesse disponibilizar voluntariamente esses dados, especialmente diante de uma requisição policial ou ministerial, entendo tratar-se de uma atecnia legislativa. A opção pela obrigatoriedade de submissão ao Poder Judiciário fica evidente na leitura dos §§ 5º e 3º dos Arts. 13 e 15, respectivamente. Ainda que o provedor se dispusesse a fornecer esses dados, correr-se-ia o risco de ver essa prova anulada posteriormente.

Passamos a analisar o procedimento que rege a obtenção dos registros:

> *"**Art. 22**. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.*
>
> *Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:*
>
> *I - fundados indícios da ocorrência do ilícito;*

[29] É importante ressaltar que a lei utiliza a palavra "provedor" tanto para as entidades que fornecem o serviço de conexão à Internet quanto para as que fornecem ou disponibilizam as aplicações de Internet (vide Art. 11, §3º, Art 13, §4º, Art. 15, Art. 29, par. único).

[30] Note-se que o prazo prescricional de ações de reparação civil é de 3 anos (Art. 206, § 3º, V, do Código Civil).

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
III - período ao qual se referem os registros."

No caso de investigações criminais de crimes cometidos pela internet, entendemos ser de fácil demonstração os itens I e II. A instauração de inquérito policial por si só já pressupõe a existência de "fundados indícios da ocorrência do ilícito". Não se instaura inquérito diante de meras elucubrações. As notícias-crimes não confirmadas estão sujeitas à "verificação de procedência das informações" (Art. 5º, § 3º, do CPP).

Quanto à "justificativa motivada da utilidade dos registros solicitados", cremos que tarefa mais difícil seria a oposta, a de demonstrar a inutilidade desses registros em uma investigação criminal. Em um paralelo grosseiro, mas pertinente, a utilidade dos registros de conexão ou acesso seria a mesma de se obter a placa de um veículo utilizado na prática de um crime, com a diferença de que, no caso de crimes cometidos pela internet, a obtenção dos registros é, muitas vezes, a única e primordial diligência que pode levar a indícios de autoria. Logo, o indeferimento do requerimento equivaleria à morte precoce desse tipo de investigação, por ausência de linha investigativa.

Esse procedimento de obtenção judicial de registros de conexão e acesso poderia até ter algum sentido para o caso de partes em processos cíveis. Para investigações criminais a lei apenas criou uma infeliz burocracia, dificultando ainda mais o já árduo trabalho dos órgãos de persecução penal. É estarrecedor que se tenha igualado o interesse privado de uma parte em processo cível ao interesse público da sociedade em ver esclarecidos fatos supostamente criminosos.

A corrente que prevaleceu durante a elaboração da lei parte do pressuposto que as Autoridades Públicas encarregadas da persecução penal estão a serviço de um Estado totalitário e opressor dos direitos e liberdades individuais e por isso não deveriam ter acesso aos registros de acessos ou conexão. Essa premissa, no entanto, revela apenas um pensamento anacrônico ou distópico, aliado à falta de conhecimento do que são os registros de acesso.

Crê-se que o Estado é o *big brother* de George Orwell, quando na verdade as entidades privadas é que concentram enormes volumes de dados e informações que o usuário médio da internet sequer imagina estar disponibilizando[31] [32].

Não é difícil encontrar na *deep web*[33] pessoas vendendo pacotes completos de

[31] O leitor interessado pode fazer um teste, baixando os dados associados a seu perfil que o Facebook dispõe. Para citar apenas alguns: dispositivos que utiliza para acessar a rede, locais onde esteve, pesquisas realizadas dentro e fora da rede social (o que pode revelar mais sobre hábitos e interesses do usuário do que qualquer outra coisa), contatos mais frequentes, etc. Veja como em https://www.facebook.com/help/131112897028467/

[32] Ainda sobre a questão, remeto o leitor ao documentário "Terms and Conditions May Apply", de 2013, que trata da coleta e utilização de dados de usuários por grandes prestadoras de serviço na Internet. O filme pode ser visto gratuitamente em https://freedocumentaries.org/documentary/terms-and-conditions-may-apply

[33] Parte da Internet não indexada por motores de busca, geralmente acessível com a utilização de softwares de anonimização, como por exemplo o TOR.

dados sigilosos de milhares de pessoas, ou ainda *malwares* com a função de capturar tais dados e que podem ser utilizados por pessoas sem qualquer conhecimento avançado de informática. Não estaria aí a verdadeira ameaça à privacidade e à segurança do usuário de internet?

Ademais, os registros de acesso não revelam qualquer informação privada ou dado pessoal. Configuram tão somente a possibilidade de identificação de uma conexão utilizada para realizar determinado acesso. Carros transitam com uma identificação visível a qualquer um. Têm essa mesma identificação registrada em inúmeros locais pelos quais transitam (pedágios, câmeras de segurança, estacionamentos, etc.) e ninguém considera isso uma "violação à intimidade/privacidade".

Para além da crítica que se possa fazer em relação à exigência de ordem judicial para obtenção dos registros de acesso e conexão, nota-se ainda a falta de técnica do legislador nesse ponto. A lei diz que "a parte interessada poderá" requerer o fornecimento dos registros. Ora, o delegado de polícia não é parte interessada, mas, sim, titular da investigação realizada por inquérito policial. A representação do Delegado pela obtenção dos registros não possui caráter meramente facultativo tal qual o requerimento de um particular, constituindo, sim, um poder-dever de agir derivado de sua atribuição investigativa conferida pelo Estado.

O inciso III é autoexplicativo. Ressalto apenas o anotado acima, no sentido de que nada impede que o período requerido seja superior aos mínimos legais (1 ano para registros de conexão, 6 meses para de aplicações), visto que é possível a guarda dessas informações por prazo superior.

Retomando, na letra "**c**" temos a questão da disponibilização de conteúdo das comunicações privadas. É justamente aqui que a falta de um conhecimento adequado tanto da lei quanto de questões técnicas afetas à área de informática e telecomunicações pode ocasionar resistências indevidas, prejudicando a obtenção de informações relevantes à instrução de uma investigação criminal.

O § 2º do Art. 10 diz que "o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do Art. 7º". Vejamos:

> *"**Art. 7º** O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:*
> *(...)*
> *II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;*
> *III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;"*

De início, nota-se que a pequena diferença na redação dos incisos recai sobre os termos "fluxo" e "na forma da lei", que não estão presentes no inciso III. O fluxo de comunicação/dados não se confunde com a comunicação ou os dados

em si[34]. O fluxo só existe quando a conversa ou dados estão sendo transmitidos/recebidos. Após o envio/recepção o conteúdo pode ou não ser armazenado em algum computador ou dispositivo.

A expressão "na forma da lei" submete a aplicabilidade do dispositivo a um regulamento próprio, que no caso é a Lei 9.296/96[35]. Já o inciso III trata da informação armazenada e, portanto, estática. Não há fluxo a ser violado/interceptado. E também não há necessidade de lei própria estabelecendo o modo como essa informação pode ser obtida. Basta uma ordem judicial lastreada no próprio marco civil, que é exatamente do que trata o § 2º, do Art. 10, ora sob análise[36].

Essa distinção tem efeitos práticos relevantes, visto que a Lei nº 9.296/96 possui requisitos bem mais estritos (demonstração de que a prova não pode ser feita por outro meio disponível e o crime deve ser apenado com reclusão, conforme incisos II e III do Art. 2º desse diploma) do que os exigidos para a obtenção de dados armazenados, que pode ser equiparada a uma busca e apreensão em meio virtual, regida pelo CPP (Art. 6º, § 1º e Art. 240 e ss).

Cabe ressaltar também que a obtenção de fluxo ou conteúdo de dados ou comunicações só pode ocorrer "para fins de investigação criminal ou instrução processual penal", nos termos do inciso XIII do Art. 5º da CR/88, ao contrário da obtenção de simples dados cadastrais ou mesmo de registros de acesso ou conexão, que podem ser utilizados em processos de outra natureza (Art. 22 do Marco Civil).

Importante frisar que a maioria dos serviços eletrônicos estão usando criptografia em seu fluxo de comunicações, logo, a interceptação direta no provedor de conexão pode se tornar inútil, caso não se tenha a capacidade de descriptografá-lo.

No curso da investigação deve-se ponderar sobre a real necessidade de se implementar uma interceptação de fluxo, visto que o acesso ao conteúdo armazenado pode muitas vezes ser suficiente. Em geral, o acesso ao conteúdo de uma caixa postal (e-mail) é mais facilmente obtido junto às empresas (mediante ordem judicial). A análise do material também pode ser mais simples do que a proveniente de interceptação bruta de pacotes de fluxo.

O que comumente se chama de "interceptação de e-mail" tecnicamente não é

---

[34]Essa distinção é pacífica no STF. "A proteção constitucional é da comunicação de dados, e não dos dados" (STF HC 91.867, julgamento em 24-4-2012).

[35]Cabível aqui menção à clássica lição de José Afonso da Silva sobre a aplicabilidade das normas constitucionais (categorizando-as em de eficácia plena, eficácia contida e eficácia limitada. Esta última dependeria de outro normativo para que produzisse plenos efeitos). A lei 12.965/2014 estabeleceu princípios e normais gerais sobre o uso da Internet no Brasil (conforme se extrai de sua ementa). Como tal, contém algumas normas com conteúdo mais aberto, sujeitas a regulamentações complementares, como é o caso desse inciso II, do Art. 7º.

[36]Sempre foi comum a Autoridade Policial ou o Ministério Público representarem em juízo visando obter o conteúdo existente em caixas de e-mail ou outros dados digitalmente armazenados com base na Lei 9.296/96. Uma impropriedade que esperamos ver superada à medida que o conhecimento sobre a Lei 12.965/2014 se dissemine.

uma interceptação de fluxo. Essa suposta "interceptação" é feita com a criação de uma conta-espelho pela empresa destinatária da ordem, para a qual são encaminhados os e-mails recebidos/enviados pelo alvo. Evidentemente existe um *delay* entre o envio/recebimento de mensagens pelo alvo e a remessa desses dados pela empresa para a conta-espelho. Ou seja, quando nós recebemos as mensagens, através da conta-espelho, o fluxo de comunicação do alvo já ocorreu. No entanto, esses conceitos não estão difundidos entre a comunidade jurídica, podendo haver resistência à interpretação de que não é necessário se basear na Lei 9.296/96 para obter dados via criação de "conta-espelho".

Em suma, caso não seja estritamente necessário o acompanhamento online das atividades do alvo, é suficiente obter uma decisão que determine o envio de todo o conteúdo existente na caixa postal/conta/perfil por ocasião do recebimento da ordem judicial. Em seguida, pode-se renovar essa ordem quantas vezes se fizer necessário.

Em todos os casos, e especialmente no caso de adoção da medida sugerida no parágrafo anterior, é importante requisitar a preservação do conteúdo a ser obtido. Isso impede que dados apagados pelo usuário tornem-se indisponíveis.

Retomando as obrigações instituídas aos provedores, finalizamos com o item "**d**", que trata do acesso a dados cadastrais "*que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição*". Não pretendemos esgotar quais "autoridades administrativas" poderiam exercer essa prerrogativa. Aqui nos interessa a atuação voltada à persecução penal, no mais das vezes exercida pela Autoridade Policial e pelo membro do Ministério Público, ambos com poder de requisição expressamente previsto em lei[37].

Apesar de o texto fazer referência apenas à qualificação pessoal, filiação e endereço, isso não significa dizer que outros dados cadastrais em poder do provedor não possam ser requisitados. A expressão "na forma da lei" harmoniza-se com o parágrafo único do Art. 3º do diploma em tela[38], ou seja, o poder requisitório possui um caráter genérico, delimitado tão somente pelas cláusulas constitucionais de reserva de jurisdição e outras normas legais que expressamente confiram especial sigilo ao dado/informação[39]. Por óbvio, o dado ou informação requisitada deve guardar relação teleológica com a investigação, bem como estar em consonância com o princípio da proporcionalidade[40].

---

[37] A Autoridade Policial tem competência legal de requisição estabelecida no Art. 6º, III do CPP, Art. 2º, §2º, da Lei 12.830/2013, Art. 17-B da Lei 9.613/98 e Art. 15 da Lei 12.850/2013. Já os membros do Ministério Público, em matéria penal, no Art. 8º, II e IV, da LC 75/93, e Art. 26, II, da Lei 8.625/93.

[38] "Art. 3º (...) Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

[39] Como, por exemplo, as informações classificadas como sigilosas nos termos da Lei nº 12.527/2011.

[40] Em razão da extrema pertinência com o tema aqui tratado, cito trecho do voto do Min. Marco Aurélio Belizze no AgRg no HC Nº 181546/SP, no qual se discutiu, dentre outras questões, a obtenção de dados cadastrais

Assim, por exemplo, não há qualquer ilegalidade na requisição e obtenção de dados que constem do cadastro do provedor de conexão ou de aplicações de internet tais como números de telefone, e-mails, meios de pagamento (contas correntes, cartões de crédito, paypal), outras contas ou serviços associados ao usuário, data de criação da conta ou cadastro, etc.

A requisição de Autoridade Policial é uma ordem, e como tal deve ser cumprida sob pena de desobediência (Art. 330 do CP) ou, mais apropriadamente e quando cabível, de capitulação no Art. 21 da Lei 12.850/2013, inclusive com a lavratura de Termo Circunstanciado, visto que a conduta de "recusar ou omitir" é permanente.

Caso entenda pela ilegalidade da ordem deve o destinatário buscar provimento judicial que o abstenha do cumprimento. A prática de algumas empresas de se arvorar em instância do Poder Judiciário, negando-se a cumprir ordens sob alegação de suposta inconstitucionalidade ou ilegalidade deve ser duramente combatida.

Veja-se que, via de regra, o direito que potencialmente poderia ser violado por uma requisição ilegal não pertence à empresa destinatária da ordem, mas sim ao investigado. Cabe a este arguir em juízo eventual nulidade. A empresa que detém os dados requisitados não tem procuração para representar o investigado. Tampouco pode ser punida por atender uma ordem formalmente legal.

3. DO CUMPRIMENTO DE ORDENS POR EMPRESAS ESTRANGEIRAS

O **Art. 11** estabelece:

"Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de

---

diretamente pela Autoridade Policial:"(...) *entendo importante consignar que, na ordem constitucional pátria, não existem direitos absolutos, que possam ser exercidos a qualquer tempo e sob quaisquer circunstâncias. E isso ocorre porque a tutela normativa de qualquer bem ou valor é sempre abstrata. No plano da realidade concreta, surgirão, inevitavelmente, situações de confronto entre dois ou mais titulares do mesmo direito, razão pela qual a lei estará autorizada a regulamentar soluções específicas para cada conflito, observado o princípio da proporcionalidade...*

O mencionado princípio, que não encontra previsão expressa na Constituição Federal, deriva, segundo entendimento do Supremo Tribunal Federal, do devido processo legal substantivo, sendo constituído de três subprincípios, quais sejam: adequação, necessidade e proporcionalidade em sentido estrito.

A adequação refere-se à idoneidade ou pertinência da medida que se impõe, que deve ser apta a atingir o objetivo pretendido. A necessidade significa que a adoção da medida restritiva só será válida se demonstrada a sua indispensabilidade. Já a proporcionalidade em sentido estrito deve ser verificada no âmbito do resultado produzido, de forma que se proporcione uma relação ponderada entre o grau de restrição das liberdades públicas e o grau de realização do princípio contraposto.

Assim, inviável proteger ilimitadamente a liberdade individual em detrimento dos interesses da sociedade. Com efeito, a liberdade individual não é o único bem protegido pelos direitos fundamentais. Medidas adotadas em favor da ordem pública, ainda que restritivas de liberdade, podem reforçar a defesa dos direitos fundamentais, desde que necessárias à democracia. Entendo que o princípio da proporcionalidade fornece o substrato necessário ao equilíbrio entre os direitos individuais atingidos pelo Direito Processual Penal e os direitos da comunidade."

*conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, **deverão ser obrigatoriamente respeitados a legislação brasileira** e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.*

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

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

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

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Em seguida, o Art. 12 prevê 4 tipos de sanções administrativas (advertência, multa de até 10% do faturamento, suspensão temporária e proibição de exercício das atividades) para empresas nacionais ou estrangeiras que descumprirem o disposto nos Arts. 10 e 11, consignando em seu parágrafo único: "*tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País*".

Note-se que os §§ 1º e 2º referem-se tão somente ao caput do Art. 11. No entanto, o Art. 12 prevê punição para o descumprimento tanto do Art. 11 quanto do Art. 10 (que expressamente prevê a "disponibilização dos registros de conexão, bem como conteúdo de comunicações"). Qualquer sanção é decorrente do descumprimento de um dever legal, logo, careceria de lógica o argumento de que as empresas estrangeiras estariam sujeitas somente ao cumprimento do Art. 11, e não do Art. 10.

A expressão grifada "deverão ser obrigatoriamente respeitados a legislação brasileira (...)" evidentemente inclui a própria Lei 12.965/2014. Ou seja, tudo o que foi dito no capítulo anterior se aplica às empresas estrangeiras que se enquadrarem nos parágrafos 1º e 2º acima transcritos. Apesar de o ponto de vista aqui exposto defluir diretamente do texto, sem necessidade de qualquer malabarismo interpretativo, há os que sustentam que as ordens judiciais brasileiras não são aplicáveis a empresas estrangeiras "quando os dados se encontrarem fora do Brasil", visto que o cumprimento de ordem brasileira no exterior estaria sujeita aos procedimentos previstos na legislação e tratados internacionais aplicáveis, como por exemplo, o Acordo de Assistência Judiciária

em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América (MLAT). A seguir demonstraremos a falácia desse argumento.

Nos casos de empresas que possuam estabelecimento (filial, sucursal, escritório, etc.) no Brasil (ex.: Google, Microsoft, Facebook, Twitter, Yahoo) a ordem deve ser dirigida diretamente ao Diretor desta. A eventual alegação de impossibilidade técnica de cumprimento da ordem, pois "os dados não estão no Brasil" é simplesmente mentirosa. A uma porque o local de armazenamento das informações não possui qualquer relação com a sua acessibilidade, sendo da própria essência da internet que os dados podem trafegar de um dispositivo para outro independentemente de sua localização, bastando que os mesmos estejam conectados nessa rede mundial. A duas porque, ainda que o estabelecimento não tenha autorização para acessar diretamente os dados requeridos, nada impede que esta os solicite à matriz, que os repassará a filial visando o cumprimento da ordem. Esse é o procedimento comumente empregado por empresas multinacionais que têm cumprido ordens judiciais e requisições policiais brasileiras muito antes da vigência do marco civil.

Há ainda outro fato que desmente a falácia do argumento "os dados estão na sede da empresa, que fica no país XX (em geral EUA)". As maiores e mais conhecidas empresas que fornecem serviços na internet possuem *data centers* (centros de processamento de dados onde estes são armazenados em computadores ou dispositivos de grande capacidade) espalhados em diversas regiões do mundo. É uma medida de segurança (em casos de catástrofes naturais, por exemplo) e de economia (mão de obra e/ou energia mais barata, incentivos fiscais, etc.) adotada pelas empresas. Tomemos o caso da Google. Em seu próprio site a empresa lista a localização de seus 13 *data centers*, espalhados por 3 continentes (em locais como Chile, Islândia, Hong Kong, etc.)[41]. Seria possível dizer em qual desses países os dados de determinado usuário de fato estão armazenados[42]? Deve-se então conhecer e aplicar a lei de cada um desses países conforme os dados se encontrarem em um ou outro? A resposta para essa inusitada situação não possui qualquer relevância, considerando o exposto nos parágrafos acima.

Outro argumento fartamente utilizado é o de que "a empresa seria punida nos EUA caso fizesse a entrega dos dados", que também não passa de embuste. Verdade fosse, essas empresas já teriam quebrado de tantas multas que teriam recebido. Aliás, a própria Google fornece desde julho de 2008 dados de conteúdo

[41]Vide http://www.google.com/about/datacenters/inside/locations/index.html. Consulta feita em 20 de outubro de 2014.

[42] Na verdade os dados são armazenados em vários deles, uma redundância que confere segurança no caso de problemas com um dos *data centers*. Além disso, para suportar os milhões de acessos feitos ao mesmo tempo, é utilizada uma tecnologia de computação distribuída, que permite que a requisição de um dado seja processada por diversos computadores simultaneamente.

do Orkut, por força de Termo de Ajuste de Conduta (TAC) firmado com o MPF/SP[43].

Essa foi a posição adota pelo STJ em julgamento de questão de ordem no INQ 784/DF[44], no qual foi fixada multa diária de R$ 50.000,00 à Google Brasil por descumprimento de decisão que determinou a entrega de conteúdo de e-mails. Em decisão de 17/04/2013, a Corte Especial assentou:

> *"Insistem, mais uma vez, na alegada impossibilidade física de cumprimento da ordem, além da impossibilidade jurídica, porque "a transmissão das informações solicitadas entre a Google Inc. e a embargante configuraria um crime para os dirigentes da empresa americana. (...) A ordem judicial já foi prolatada, quebrando sigilo telemático, mas a medida ainda não foi cumprida pela GOOGLE BRASIL, sob o pálido argumento de que é a empresa controladora GOOGLE Inc., sediada em território americano, que armazena os dados de e-mail, os quais estariam inacessíveis, física e juridicamente, para a subsidiária brasileira, ressaltando que essas informações estariam sob proteção da legislação americana. (...) O obstáculo oposto, ademais, não procede. A sede-matriz (empresa controladora) em território americano se faz representar aqui pela GOOGLE BRASIL.*
>
> *Ora, o que se pretende é a entrega de mensagens remetidas e recebidas por brasileiros em território brasileiro, envolvendo supostos crimes submetidos induvidosamente à jurisdição brasileira. Nesse cenário, é irrecusável que o fato desses dados estarem armazenados em qualquer outra parte do mundo não os transforma em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados.*
>
> *Trata-se, evidentemente, de elemento de prova produzido, transmitido e recebido em território brasileiro, repito. Nada tem a ver com terras alienígenas, a não ser pelo fato de, por questões estratégico-empresariais, estarem armazenados nos Estados Unidos.*
>
> *Cumpre observar que a mera transferência reservada - poder-se ia*

[43] Vide cláusula terceira, letra "c" do Termo, disponível em: http://www.safernet.org.br/site/sites/default/files/TACgoogleMPF_0.pdf

[44] Segue a respectiva ementa:

"QUESTÃO DE ORDEM. DECISÃO DA MINISTRA RELATORA QUE DETERMINOU A QUEBRA DE SIGILO TELEMÁTICO (GMAIL) DE INVESTIGADOS EM INQUÉRITO EM TRÂMITE NESTE STJ. GOOGLE BRASIL INTERNET LTDA. DESCUMPRIMENTO. ALEGADA IMPOSSIBILIDADE. INVERDADE. GOOGLE INTERNATIONAL LLC E GOOGLE INC. CONTROLADORA AMERICANA. IRRELEVÂNCIA. EMPRESA INSTITUÍDA E EM ATUAÇÃO NO PAÍS. OBRIGATORIEDADE DE SUBMISSÃO ÀS LEIS BRASILEIRAS, ONDE OPERA EM RELEVANTE E ESTRATÉGICO SEGUIMENTO DE TELECOMUNICAÇÃO. TROCA DE MENSAGENS, VIA E-MAIL, ENTRE BRASILEIROS, EM TERRITÓRIO NACIONAL, COM SUSPEITA DE ENVOLVIMENTO EM CRIMES COMETIDOS NO BRASIL. INEQUÍVOCA JURISDIÇÃO BRASILEIRA. DADOS QUE CONSTITUEM ELEMENTOS DE PROVA QUE NÃO PODEM SE SUJEITAR À POLÍTICA DE ESTADO OU EMPRESA ESTRANGEIROS. AFRONTA À SOBERANIA NACIONAL.IMPOSIÇÃO DE MULTA DIÁRIA PELO DESCUMPRIMENTO."

dizer interna corporis - desses dados entre a empresa controladora e controlada não consistiu, em si, quebra do sigilo, que só será feito quando efetivamente for entregue à autoridade judicial brasileira, aqui. (...)

A empresa aqui instalada não pode se apresentar apenas para colher os lucros, mas se eximir das obrigações que a legislação brasileira se lhe impõe. *" (grifei)*

Observe-se que essa decisão foi prolatada ainda antes da promulgação da Lei 12.965/2014, que expressamente regulou a situação nesse mesmo sentido.

Os argumentos aqui expostos também foram minuciosamente debatidos no julgamento do MS nº 2009.04.00.011335-1/PR do TRF-4[45]. No voto vencedor o Des. Federal Márcio Antonio Rocha afirmou:

"*Mister salientar, no ponto, a inexistência de qualquer inconstitucionalidade na não utilização do 'MLAT' em determinadas hipóteses, uma vez que o artigo 17 do referido acordo possibilita o uso de outros instrumentos para produção de provas (...)*

Resta plenamente facultado, portanto, a produção da prova por outros meios, como ocorre, v.g, nas hipóteses de cooperação direta policial, depoimento voluntário de testemunhas, troca de informações que não estejam cobertas por sigilo, etc.

Repita-se: embora, em regra, o acordo de cooperação seja útil na investigação criminal (como, v.g. para o bloqueio de contas no exterior, o envio de documentos, a tomada de depoimentos, etc.) é consabido que tal instrumento possui pouca efetividade - ou até mesmo nenhuma - nos casos em que se exija rapidez de ação (mormente quanto a possíveis atos delituosos e/ou terroristas que podem ocorrer em grandes eventos - copa do mundo, olimpíadas, etc. - sendo o e-mail, como é sabido, um dos principais meios de comunicação entre os agentes de organizações criminosas), cujo resultado deve ser imediato (inclusive na hipótese dos autos em que se pretendia verificar as mensagens remetidas e/ou recebidas durante os quinze dias seguintes à determinação judicial), sob pena de restar, ao final, prejudicado o devido esclarecimento dos fatos investigados.

Ademais, revela-se extremamente temerário vincular as autoridades judiciais brasileiras à legislação do local em que os dados, em tese, encontram-se armazenados, uma vez que a empresa pode, por qualquer motivo, simplesmente fazer a opção de transferir o servidor para qualquer país do mundo, sem que haja acordo de cooperação com o Brasil, o que, certamente, dificultará ainda mais a investigação criminal."

Pelo exposto, cremos que não há qualquer motivo técnico ou jurídico que as

[45] Disponível em http://www.migalhas.com.br/arquivo_artigo/art20130620-12.pdf

representantes de empresas estrangeiras aqui instaladas possam opor visando o não cumprimento de ordens judiciais brasileiras.

Quanto às empresas que não possuírem representação no Brasil, estas também estão sujeitas à legislação brasileira "desde que ofertem serviço ao público brasileiro". Este seria o caso, por exemplo, de sites como dropbox.com ou de qualquer aplicativo disponível para compra ou download nas lojas virtuais da Google, Apple ou Microsoft. Na ausência de representação local, pode-se encaminhar a ordem diretamente para a sede da empresa[46].

Nos casos em que o descumprimento reiterado de ordens esteja prejudicando as investigações, um caminho possível seria buscar a retirada do respectivo aplicativo das lojas virtuais, sendo esta, inclusive, uma das sanções previstas em lei (Art. 12, incisos III e IV)[47].

Um caso de grande repercussão ocorreu em dezembro de 2015, quando uma ordem judicial da 1ª Vara Criminal de São Bernardo do Campo/SP determinou o bloqueio do aplicativo WhatsApp por 48h. Noticiou-se que a sanção teria decorrido do descumprimento reiterado de ordens judiciais anteriores. A medida chegou a ser cumprida, mas foi suspensa 13 horas após sua implementação por decisão de 2º grau.

Afora a discussão sobre a adequação da medida - muitos afirmaram ser desproporcional, visto ter atingido todos os usuários -, o caso ilustra bem as resistências e dificuldades na aplicação da lei a empresas estrangeiras.

Em nossa experiência profissional vimos que muitas vezes são necessárias medidas de força como essa para mostrar que o Judiciário brasileiro é uma instituição séria e consolidada, e que não há outro caminho a não ser respeitar suas decisões (ou deixar de operar no País). Não podemos aceitar que a soberba e os interesses comerciais estejam acima de nossas leis.

4. CONCLUSÃO

A regulamentação foi benvinda. Houve importantes avanços, como o estabelecimento de prazos mínimos para guarda de registros de acesso e conexão e a obrigatoriedade de observância da lei brasileira para atos realizados no território nacional.

Apesar de o texto aparentar proteger os usuários da internet de ameaças às suas liberdades e vida privada quando praticadas pelo Estado, como se este fosse

[46] As maiores empresas, em geral, possuem um canal de interface próprio para "*law enforcement*", que pode ser encontrado bastando fazer uma busca com esse termo + nome da empresa.

[47] Esse foi o caso do aplicativo "Secret", que permite a publicação anônima de "segredos" a respeito de terceiros. Após diversos casos de calúnia e difamação, o Ministério Público do Espírito Santo ingressou em 18/08/2014 com ação civil pública requerendo a retirada desse aplicativo das lojas virtuais da Google e Apple. Proc. 0028553-98.2014.8.08.0024.

o maior interessado em violá-las, o fato é que até mesmo os que defenderam a total ausência de controle e guarda de registros na utilização da internet agora clamam por punição aos que se utilizam da rede para praticar toda a sorte de delitos, como racismo, injúria, fraudes eletrônicas, pornografia infantil, etc.

Por seu turno, os que atuam na persecução penal não possuem instrumentos suficientes para enfrentar o crescente uso do meio virtual para a prática de crimes.

A necessidade de ordem judicial para obtenção de registros de acesso, passo básico inicial de qualquer investigação nessa área, tornou-se uma burocracia que costuma retardar a apuração em meses. Em geral essa informação é necessária até mesmo para saber onde a investigação deve ser iniciada. E sem essa definição temos ou a multiplicidade de investigações idênticas ou a não instauração de investigação, visto que nenhuma autoridade se presume competente para iniciá-la.

A falta de legislação própria para crimes cibernéticos também tem servido como estímulo ao uso do ambiente virtual pelos delinquentes. A lei nº 12.737/2012, apelidada "Carolina Dieckmann", insuficiente e com penas pífias, é um atestado da incompreensão que impera sobre o potencial lesivo do uso de computadores para a prática de crimes.

De todo modo a lei está posta, e cabe aos operadores jurídicos sua interpretação e aplicação, sendo o Delegado de Polícia relevante ator nesse processo.

Nesse passo, esperamos que as linhas aqui traçadas possam lançar alguma luz sobre o tema, que apesar de algumas vezes ser visto como "novidade" faz parte de praticamente qualquer investigação de relevo atualmente, independentemente da área em que se atue.

6. REFERÊNCIAS

ARAS, Vladimir. *A questão penal no Marco Civil*. Em https://blogdovladimir.files.wordpress.com/2010/01/artigo-marco-civil-da-internet.pdf. Acesso em 06 de janeiro de 2016.

BINICHESKI, Paulo Roberto. *O Marco Civil Da Internet: Primeiras Linhas*. Em http://www.mpcon.org.br/Revista_mpcon/n01/artigos/ARTIGO_2014-O_MARCO_CIVIL_DA_INTERNET_PRIMEIRAS_LINHAS-PAULO_ROBERTO_BINICHESKI.pdf. Acesso em 28 de dezembro de 2015.

Capítulo IV

Contribuição crítica ao processo de investigação criminal da fraude bancária eletrônica: Ubi societas, ibi criminis?

Stenio Santos Sousa(*)

1. INTRODUÇÃO

Os direitos e garantias fundamentais balizados na Constituição Federal de 1988 traduzem aspirações decorrentes de vários anos em que o país se viu obrigado por sérias restrições na ordem jurídico-constitucional que se contextualizaram no regime militar.

A redemocratização, conquistada após longo processo político e lutas sociais, trouxe consigo uma busca desenfreada pela criação de freios e contrapesos que tornassem muito dificultoso algum revés de semelhante natureza.

As implicações dessas escolhas políticas refletem nos dias atuais, muitas vezes, em excessos de exigências de direitos, que inviabilizam a atuação do Poder Judiciário e dos órgãos de investigação criminal, em contraposição com as barreiras impostas ao seu contraponto, os deveres constitucionais e infraconstitucionais.

Têm sido objeto de inúmeros debates os direitos e garantias fundamentais, mas pouco tem sido discutidos ou mesmo pesquisada a efetividade dos deveres constitucionais, dentre eles o dever de cooperação com a Segurança Pública,

* Mestre em Ciências Policiais, Criminologia e Investigação Criminal (2015). Especialista em Ciências Criminais (2007). Graduado em Direito (2002). Professor e Tutor EaD da Academia Nacional de Polícia. Delegado de Polícia Federal (2003). Chefe do Grupo de Repressão a Crimes Cibernéticos da Polícia Federal no Distrito Federal. Autor do livro "Investigação Criminal Cibernética: por uma política criminal de proteção à criança e ao adolescente na Internet".

previsto no caput do Art. 144, da Constituição Federal de 1988: "direito e responsabilidade de todos".

Consequência dessa atitude, que poderíamos chamar de juventude constitucional de nossa pátria, é a percepção de que o Estado é pesado e ineficiente, ao passo que a criminalidade, e cada vez mais eficaz, em proporção direta à ineficácia da atuação dos poderes constituídos em deter suas investidas.

Por outro lado, com a percepção dessa crise, em uma busca por um equilíbrio e por fornecer respostas, diretrizes de natureza tanto executiva, quanto judiciária e legislativa, tendentes a um certo exagero, têm sido, paulatinamente, incorporadas no cotidiano social e refletem em políticas criminais como "Tolerância Zero" e "Lei e Ordem", dentre tantas outras de semelhante jaez.

No âmbito da Polícia Federal, as chamadas "operações policiais", inquéritos policiais com estratégias focadas diretamente na produção de resultados imediatos, com maiores restrições a direitos fundamentais, em conjunto com sua consequente publicidade midiática, aparentam terem sido uma das fórmulas escolhidas para buscar frear e reduzir o contraponto da criminalidade organizada.

Nesse contexto, é objetivo geral deste trabalho o estudo das fraudes bancárias em sua relação com os serviços de internet banking, em especial quando praticadas por meio de organizações criminosas.

Tratamos especificamente de apresentar o furto e o estelionato como crime cibernético, as classificações usualmente utilizadas para distinguir as diferentes espécies, bem como um breve estudo dos métodos de ataques por *phishing scam*, sem descuidar de definir qual o tipo penal mais adequado à conduta ilícito-típica investigada.

No que concerne à investigação criminal, demonstramos como ocorre, a importância da definição da competência ainda na fase do inquérito policial e fazemos resenha do Projeto Tentáculos no contexto do processo penal, inclusive tecendo breve crítica reflexiva, tendo por parâmetro a ideia de "direito penal moderno" de Hassemer e o conceito de "tardo-modernidade" de Faria Costa.

2. FRAUDE BANCÁRIA E SERVIÇO DE INTERNET BANKING

Na década de 80 as instituições financeiras iniciaram o primeiro movimento no sentido de disponibilizar serviços remotos a seus clientes, primeiro com o uso da telefonia e, então, a rede mundial de computadores. Aproveitava-se a tecnologia incipiente para otimização do tempo e dos custos. Em outubro de 1994 (BANCÁRIO.PT, 2015), o Stanford Federal Credit Union (2015), banco da Califórnia, tornou-se pioneiro ao disponibilizar o primeiro serviço de internet banking no mundo.

Também conhecido como banco eletrônico, banco virtual, banco móvel, dentre outras denominações, e considerado por Eduardo Diniz (2006) "*a principal inovação tecnológica incorporada aos serviços bancários na última década*", vem sendo intensamente utilizado pelas instituições financeiras no

Brasil desde 1995 (*Idem*) e atualmente utiliza o protocolo HTTPS (Hyper Text Transfer Protocol Secure - protocolo seguro de transferência de hipertexto), várias camadas de proteção[48] e tráfego encriptado da informação, garantindo um nível de acesso dificilmente quebrado, quando muito pelos hackers mais capacitados.

Uma grande vantagem do banco móvel é seu custo para a instituição financeira, bastante inferior ao serviço da agência ou por telefonia, uma vez que estabelece automatização de processos, bem como torna desnecessária, em grande parte, a intervenção humana, sempre sujeita a erros. É, portanto, estratégico para as instituições financeiras "*que os clientes da era digital não precisem ir na agência*" (PINHEIRO, 2010, p. 238).

Visando a incrementar a aplicação, no ano de 2008 foi implementado um método pouco conhecido de acesso ao internet banking no Brasil que consiste em digitar a URL do banco no seguinte formato: nomedobanco.b.br, a qual encaminha o usuário de forma segura para a respectiva página na internet (G1, 2008).

Considerando as vantagens e desvantagens do *home banking*, dentre as quais o interesse subjacente de hackers e crackers na exploração de falhas, em muitos casos visando ao lucro pessoal, remanesce o interesse dos bancos em sua proliferação. Todo investimento, assim, é considerado útil e a questão de ordem é buscar dar cada vez mais credibilidade ao serviço, o que inclui omitir resultados negativos, inclusive fraudes online.

Para o cliente bancário, ao seu turno, em face do recrudescimento da violência nos grandes centros urbanos, tornou-se cômodo ter acesso 24 horas por dia e sem custo adicional aparente ao serviço online em vez de arriscar a sorte nos terminais eletrônicos.

O horário de funcionamento das agências, de 10 às 16 horas, e dos caixas eletrônicos, muitas vezes não excedendo as 22 horas, consequência da insegurança exteriorizada nas estatísticas criminais[49], aliados à vida agitada dos novos tempos, são elementos de dificuldade do cotidiano que contribuem para o progressivo interesse[50], inclusive no uso de aplicativos para smartphones e tablets que permitem conectividade instantânea.

A fragilidade do sistema reside no fato de que muitos dos usuários desconhecem regras básicas de segurança informática que permitam garantir que

[48] Políticas de segurança como o uso de mais de uma senha para acessar a conta, uso de SMS para confirmação de transações, requisição de um terceiro número de identificação dos clientes, uso de token, uso de biometria, identificação da máquina que pode acessar a conta, dentre outros.

[49] Além dos já citados furto e o estelionato dentro das agências, há ainda o chamado "sequestro-relâmpago", dentre outros que oferecem um maior risco à integridade física e moral das vítimas.

[50] Segundo o sítio IDGNOW! (2005), pesquisa da Global Marketing Insite (GMI), divulgada no dia 27 de outubro de 2005, já apontava o Brasil como o sétimo no mundo com maior utilização do Internet banking, contando com 41% do total de correntistas. Por outro lado, dados da Pesquisa Febraban de Tecnologia Bancária de 2014 (CONVERGÊNCIA DIGITAL, 2015) apontou que o Internet banking foi o canal com maior volume de transações bancárias no Brasil, com 19 bilhões, correspondendo a 41% do total contra 21% daquelas realizadas por meio dos terminais eletrônicos e apenas 8% nas agências, sendo que 47% das contas ativas tinham Internet banking, crescimento esse ligado ao aumento dos smartphones e do acesso à Internet.

o tráfego de informações não esteja sendo redirecionado para terceiros mal intencionados. É precisamente nesse limiar que surge a maioria das fraudes bancárias pelo canal internet banking.

A falsa impressão de que o prejuízo é suportado pela instituição bancária e não pelo cliente, uma vez que usualmente o prejuízo é ressarcido a este, é uma das justificativas mais comuns apresentadas pelo fraudador. Ocorre que se trata de verdadeira falácia, como bem observa Misha Glenny (2011, pp. 59 e 87), uma vez que o custo das fraudes é sempre repassado aos correntistas, por meio da cobrança de tarifas extras.

3. FURTO E ESTELIONATO COMO CRIME CIBERNÉTICO

3.1. Crimes cibernético próprios e impróprios

O crime cibernético pode ser entendido em diferentes matizes. Um dos aspectos relevantes e que merece o destaque aqui trazido é o que diferencia em puro ou próprio e em impuro ou impróprio.

Na primeira hipótese, diz-se do crime que tem como objetivo o ataque ao próprio sistema computacional. É exemplo dessa conduta, a invasão de computadores, a disseminação de vírus e o ataque de negação de serviços, dentre outros.

Da segunda espécie, encontram-se todos os que são praticados por meio ou com auxílio da tecnologia. Ainda que não houvesse o sistema computacional o delito continuaria evidenciado, posto que existente em formato tradicional. A tecnologia apenas facilita a conduta ilícito-típica, mas não é sua *conditio sine qua non*.

Vale lembrar, ainda, uma terceira classificação em crimes cibernéticos mistos.

3.2. Crimes cibernéticos mistos

Crimes cibernéticos mistos são aqueles em que não apenas se utiliza a tecnologia para a comissão delitiva, mas onde esta se torna imprescindível ou ao menos torna o delito particularmente ofensivo ou lesivo. Crimes como os de pornografia infantil pela internet e as fraudes bancárias eletrônicas exemplificam essa classificação.

O furto e o estelionato praticado contra instituições bancárias, via de regra, utilizando-se de falhas no elo mais fraco do sistema, o cliente do banco, existem desde que se pensou no modelo de preservação da riqueza por meio da confiança em um terceiro.

Ocorre que, com o advento da rede mundial de computadores, o processo de obtenção de tais riquezas de modo ilícito tornou-se não apenas mais simples e seguro, mas especialmente eficaz.

Sem haver necessidade de sair de trás da tela de um computador, o criminoso digital consegue obter o acesso à conta e a partir dali transfere recursos para terceiros (laranjas), efetua pagamento de boletos ou mesmo recarga de aparelhos celulares, dentre outras ações.

A instituição bancária aproveitou a disseminação da tecnologia em rede para tornar disponível, praticamente 24 horas por dia, seus serviços, o que a tornou mais competitiva, diminuiu seus custos e, de certo modo, tornou-a mais independente em relação aos seus empregados, cujo poder de barganha terminou reduzido.

A facilidade do acesso, ao seu turno, trouxe ao cliente a possibilidade de resolver problemas à distância. Aqueles que investiram no processo de confiança com o sistema bancário pela internet, acostumaram-se a ter acesso às aplicações e movimentações em tempo real, sem grandes complicações ou perda de tempo, tudo ao alcance de um simples smartphone, cada vez mais popularizado.

Essas benesses para um lado e a vantagem competitiva para a instituição bancária fizeram-se acompanhar de semelhante benefício àquele que intenciona a violação da regra, o que implica a necessidade de permanente pesquisa e desenvolvimento de soluções para a segurança da relação cliente-banco.

Uma das consequências da necessidade de proteção e de aumento do nível de segurança é a exigência de diferentes níveis de acesso para alcance dos serviços a serem prestados, bem como a limitação destes em determinados períodos do dia, em geral no turno noturno.

Por melhor e mais caro que seja o sistema desenvolvido, e sabe-se que são realizados investimentos milionários nessa área, existe um limite que é elo mais frágil do processo, ou seja, o usuário final.

O criminoso típico não tenta invadir o sistema de segurança da instituição bancária, mas, sim, obter o mesmo acesso disponibilizado ao cliente. Para isso costuma utilizar-se de técnicas como a criação de malwares, distribuição destes por meio de SPAM e a engenharia social, como veremos a seguir.

3.3. Métodos de Ataques de Phishing Scam

A fraude bancária pela internet prolifera-se principalmente por meio de ataques conhecidos como *phishing scam*. Os primeiros casos no Brasil remontam ao ano 2000 (SOBRAL; BEZERRA, 2015), cronologicamente posterior aos primórdios da clonagem de cartão bancário, datados de 1998 (*Idem*).

Tal panorama demonstra claramente o brocardo *ubi societas, ibi criminis*, decorrência que é da gradativa transição da tecnologia do terminal eletrônico para o *home banking* por parte tanto das instituições bancárias, quanto de seus clientes.

O *phishing* é um neologismo criado a partir da homofonia com a palavra *fishing* (pescaria em inglês) e também devido à semelhança metodológica decorrente de ser usual alcançar o objetivo de pescar com uso de isca falsa (RAMZAN, 2010).

O ataque por meio de *phishing* caracteriza-se pelo sujeito ativo da fraude criar uma página falsa da instituição bancária alvo, em geral copiando o código de programação original. Promove, no entanto, a alteração do formulário de envio das informações para que sejam encaminhadas para o servidor de arquivos cujo acesso detém.

Para divulgar a página, o atacante pode adquirir uma base de dados com correios eletrônicos, muitas com milhares, por vezes milhões, de contas, para onde encaminham a mensagem falsa, esperando que um percentual, ainda que mínimo, de incautos usuários "mordam a isca".

Segundo dados da Kaspersky Lab (2013), mais de 20% de todos os ataques de *phishing* ao redor do globo teve como alvo a criação de páginas falsas de bancos e outras organizações financeiras de um total de mais de 37 milhões de vítimas, apenas no ano de 2013.

O *phishing* também pode ter efeito idêntico quando, em vez de disponibilizar um formulário falso, emulando a página da instituição bancária, o atacante decide enviar um arquivo contendo um *malware*[51], que irá infectar a máquina do cliente bancário e, a partir daí, pode obter total controle desta, ou simplesmente configurá-la para envio sistemático das informações digitadas, em especial aquelas relacionadas às instituições bancárias (número da conta, agência, senha, número do cartão de crédito).

Uma variação desse método é chamada de *pharming*[52]. Ocorre quando, em vez de fazer com que a vítima acesse a URL falsa, o atacante envenena o servidor de DNS[53] (*DNS cache poisoning*) do provedor de serviços de internet, redirecionando o tráfego para a página falsa mesmo quando é digitado o endereço correto no navegador.

Na hipótese aventada, se o cliente digita https://www.nomedobanco.com.br, o navegador encaminha automaticamente para, por exemplo, http://www.nomedobanco.com, onde se vai encontrar o formulário falso para transmissão das informações para o domínio do criminoso[54].

Além das fraudes iniciadas eletronicamente, técnicas de engenharia social permitem que o atacante tenha acesso à conta-vítima. O sujeito ativo comparece à instituição bancária munido de documentos falsos de um correntista verdadeiro com o objetivo de autorizar o acesso aos serviços de internet banking. Para que este golpe funcione, pressupõe-se o conhecimento de que o correntista existe, possui uma relativa quantia de dinheiro e de que a movimenta pouco.

Tais informações, em geral, são repassadas por "*insiders*", ou seja,

---

[51] Termo genérico para qualquer programa criado para atuar em um sistema computacional com finalidade maliciosa.

[52] Para uma maior compreensão de como ocorre o *pharming* remetemos o leitor ao sítio da empresa Symantec, disponível em: <http://us.norton.com/cybercrime-pharming>.

[53] Sigla para *Domain Name Service*, que em uma tradução livre seria "Serviço de Nome de Domínio".

[54] Durante investigação de fraude bancária pelo Grupo de Repressão a Crimes Cibernéticos da PF no Distrito Federal vimos que para realizar *pharming*, o investigado entrou em conluio com empregado do provedor de conexão à Internet, sem o qual não teria ocorrido o envenenamento do servidor DNS.

funcionários, ex-funcionários, terceirizados ou estagiários, em síntese, "internos", os quais têm maior acesso ao que ocorre dentro da agência bancária ou da empresa, aproveitando-se de informações privilegiadas.

Em posse dos dados e após a confecção dos documentos falsos, o atacante aproveita-se da grande quantidade de serviços e pessoas no local para solicitar um pedido de assinatura eletrônica, necessária à realização de transações pelo internet banking. Em tais casos, a conivência do gerente é possível, mas incomum.

Tão logo obtém a autorização de acesso à internet, a conta passa a ser movimentada pelo *"cracker"*[55], que pode realizar todas as ações como se fosse o titular, por meio de quebra de sigilo bancário, tipificando conduta prevista no Art. 10, da Lei Complementar nº 05, de 10 de janeiro de 2001.

3.4. Definindo o Tipo Penal Envolvido: Furto ou estelionato?

Mencionamos sobre conduta de furto e de estelionato para a comissão do delito, aqui genericamente denominado fraude bancária por meio de internet banking. Importa discutir a distinção e a opção jurídica a partir da visão policial.

O furto está previsto como tipo penal no Art. 155 do Código Penal, caracterizando-se pela subtração de coisa alheia móvel, para si ou para terceiros, com preceito secundário de um a quatro anos de reclusão e multa. Em sua forma qualificada, prevista no inciso II, do parágrafo 4º do artigo citado, a pena é de reclusão de dois a oito anos e multa, se o crime é cometido mediante fraude.

O estelionato, em sua forma simples, prevê como penalmente típica e antijurídica a conduta de obter, para si ou para terceiros, em prejuízo alheio, qualquer vantagem indevida, por meio do induzimento ou da manutenção da vítima em erro, por meio de artifício, ardil ou qualquer outro meio fraudulento. A pena é de um a cinco anos e multa. Na forma qualificada do parágrafo terceiro, a pena é aumentada de um terço (um ano e quatro meses a seis anos e oito meses e multa), se a vítima é entidade de direito público, como é o caso da Caixa Econômica Federal.

Percebe-se que a forma qualificada do furto é mais grave que a do estelionato, mas isso não explica a opção jurídica por uma conduta ou outra no contexto das fraudes bancárias por meio de internet banking. Qual a conduta afinal?

É importante notar que o autor da fraude pratica diversas ações antes de conseguir se apoderar da coisa alheia móvel e obter a vantagem ilícita. O primeiro passo é a produção do vírus ou da página falsa com o objetivo de obtenção do acesso à conta bancária do cliente, a qual é invadida.

Ao optar pela disseminação do *malware*, o atacante colhe diretamente do computador da vítima os dados bancários, tal como uma escavadeira obtém areia. O robô executa a operação por meio de uma farsa, a partir da qual o cliente da

[55] Terminologia aqui utilizada para designar o sujeito que detém algum conhecimento da tecnologia e o utiliza para realizar ações ilícitas ou antiéticas.

instituição bancária executa o aplicativo criado especificamente com aquela finalidade e passa a disponibilizar o acesso a sua conta.

Na hipótese da criação da página falsa, o método de *phishing* permite ao atacante receber diretamente do cliente da instituição bancária todos os dados necessários, inclusive a senha, para acessar a conta.

Em ambos os casos, portanto, o atacante tem acesso aos dados bancários e senha da vítima. Na primeira hipótese, obtém tais informações diretamente, por meio de um robô executado pela vítima; na segunda, obtém as informações diretamente da vítima, que as digita em um formulário criado com as características da página da instituição financeira.

Em um segundo momento, de posse das informações bancárias, o criminoso invade a conta, fazendo-se passar pelo titular. Afirma, portanto, para a instituição que é o cliente, em face da falsa identidade apresentada, assenhorando-se de todos os direitos àquele atinentes.

A terceira fase da complexa conduta é a obtenção da vantagem financeira. Ocorre que, uma vez que o cliente foi mantido em erro para dar acesso completo a sua conta bancária, o atacante já não precisa da vítima para realizar transferências, empréstimos, compras, recargas de celulares, pagamentos de boletos e o que mais tiver interesse. Tais condutas são realizadas diretamente pelo criminoso.

A principal distinção entre o furto qualificado pela fraude e o estelionato, seja na sua forma simples ou qualificada, é que na primeira hipótese fática o criminoso subtrai a coisa alheia móvel, ao passo que no estelionato, a vítima entrega a vantagem ilícita em razão da fraude.

Parece-nos, assim, que há um estelionato quando da segunda etapa da conduta complexa, aquela que visa obter o controle da conta bancária. Entretanto, quando da obtenção da vantagem ilícita, ou melhor dizendo, quando da subtração da coisa alheia móvel, é o próprio criminoso que realiza a conduta, sem intermediação, praticando, portanto, furto qualificado pela fraude.

Comungamos, pois, do entendimento consolidado no Superior Tribunal de Justiça de que a subtração de recursos de contas bancárias pelo canal Internet banking consubstancia-se em furto qualificado pela fraude, *ipsis litteris*: "*o juízo competente para processar e julgar a ação penal é do local da consumação do delito de furto, ou seja, de onde foi subtraído o bem da vítima, saindo de sua esfera de disponibilidade*" (CC 87.057-RS, Rel. Min. Maria Thereza de Assis Moura, julgado em 13/2/2008). São precedentes citados o Conflito de Competência nº 86.241-PR, DJ 20/8/2007, e o Conflito de Competência nº 67.343-GO, DJ 11/12/2007.

4. A INVESTIGAÇÃO DA FRAUDE BANCÁRIA ELETRÔNICA

A investigação criminal da fraude bancária no canal internet banking tem por substrato, ou instrumental tecnológico, o Inquérito Policial, conforme estabelecido no Título II, do Livro I, do Código de Processo Penal.

Trata-se de uma garantia para o investigador, de que não ultrapassará limites jurídico-constitucionais, para o investigado, de que poderá se socorrer de garantias fundamentais, em caso de abuso ou excesso de investigação, e para a própria investigação, pois será exercida de acordo com as regras democraticamente previstas, permitindo menores margens para contestações infundadas.

A despeito de sua secularidade, o Inquérito Policial, enquanto instrumento para o alcance de uma finalidade específica (esclarecimento de um fato ilícito-típico com todas as suas circunstâncias) permanece atual, na medida em que se adeque às peculiaridades de cada tempo e modelo investigativo.

O início da investigação ainda pode ter por fundamento a chamada *notitia criminis* da vítima. Mais comum, por outro lado, vem se tornando as investigações especiais (SANTOS, 2013), a exemplo da *investigação proativa*, ou seja, aquela que se inicia antes mesmo que a vítima manifeste ato volitivo direto e formal à polícia.

A investigação proativa torna-se uma realidade na medida em que se vão criando bases de dados com informações pertinentes à realidade criminógena e permite análises de cenários em vez de se restringir à visão unívoca do delito. Responde à evolução da metodologia criminosa, com o uso massivo das tecnologias de informação e comunicação.

Tal combate não prescinde de aparato tecnológico assemelhado à investigação criminal. Trata-se de uma evolução natural decorrente não apenas das melhorias tecnológicas, mas também do aumento populacional desproporcional em relação aos recursos policiais.

A polícia trabalha com um mosaico com diferentes delitos praticados mediante determinado método, tempo, lugar e circunstâncias tais que permitem ser associados uns aos outros e revelar uma ação que numa visão primeva e parcial aparentava ser isolada e geolocalizada.

Antes, porém, de tratar dessa visão sistêmica decorrente da complexidade do fenômeno criminal de forma mais verticalizada, importa discutir a competência no processo de investigação da fraude bancária eletrônica.

4.1. Competência Penal na Fraude Bancária Eletrônica

Pressupondo que o processo penal já se iniciou quando da instauração do Inquérito Policial (SOUSA, 2015), indubitavelmente exsurge a necessidade de

definição do juízo competente para decidir a respeito das próprias medidas cautelares, imprescindíveis ao alcance teleológico da investigação criminal.

Sabemos que uma das garantias fundamentais do jurisdicionado é o devido processo legal (Art. 5º, LIV , da CF/88), onde se insere o princípio do juiz natural (JARDIM, 1999, p. 330).

Certo que não se há de exigir na fase do inquérito policial juízos definitivos a respeito da competência, mas também não se afigura razoável, na mesma medida, que juízo absolutamente incompetente possa decidir a respeito de medidas que tenham por objetivo a definição de situações fulcrais, seja no *status quo* do fato, seja a própria situação pessoal do investigado, ainda que precariamente e desde que consciente das questões envolvidas.

É necessário estabelecer limites entre o interesse social no esclarecimento da situação apresentada ao delegado de polícia e a própria atuação deste que é (deve ser), enquanto representante da polícia[56], face visível do Estado, o primeiro garantidor dos direitos humanos no processo penal democrático (VALENTE, 2014, p. 20).

Oportunidades há em que a competência jurisdicional (CF/88, Art. 109) pode afetar a eficiência da investigação criminal (Art. 37, caput, da CF/88). É preciso coragem para saber quando mitigar a competência em prol não apenas da eficiência constitucional, mas, por vezes, da própria eficácia investigativa. É o caso em que se investiga furto praticado por associação ou mesmo organização criminosa especializada.

A competência criminal do estelionato se materializa no local em que foi obtida a vantagem ilícita. Essa é a melhor hipótese (competência *ratione loci*) para a investigação criminal das fraudes bancárias eletrônicas, pois é onde estará estabelecido o núcleo duro da organização criminosa.

Essa espécie delitiva tende a se espalhar em todo o território pátrio, tornando muito difícil a investigação com base no critério admitido para os crimes de furto qualificado pela fraude, o local em que foi subtraída a coisa alheia móvel, onde se encontra a conta-vítima.

Não descuidamos da validade do entendimento de que o furto, em geral, deve ser investigado no local em que foi expropriado o bem. É preciso compreender, entretanto, que essa era a realidade até a década de noventa.

Com o advento das novas tecnologias de informação e comunicação (TICs), em especial a partir do final do século XX e início do século XXI, principalmente com a massificação do uso comercial da rede mundial de computadores (Internet), cada vez mais se trata de repensar ideias como trabalho, relações pessoais/laborais e serviços à distância.

Com mais cidadãos usuários de serviços remotos, urge a adaptação do

[56] Entendemos o ser polícia como leciona Manuel Valente (2014, p. 18) *"[...] o resultado da actividade de polícia em todas as suas dimensões socioculturais, sócio-político-jurídicas e filosófico-políticas. [...] É a actividade de polícia que dá forma e matéria ao ser polícia e não ao contrário [...]*".

pensamento jurídico tendo em consideração as consequências desse novo espaço nas relações sociais. Os crimes à distância, previstos no Art. 7º, do Código Penal, solucionam apenas em parte a grande variedade de situações novas que surgem. É preciso repensar a nova realidade que se apresenta.

Uma solução que vem sendo proposta no âmbito da Polícia Federal é que, tendo por consideração que as fraudes bancárias eletrônicas são praticadas tipicamente por meio de associação ou organização criminosa, deve ser interpretada a competência com base na conduta ilícito-típica que melhor atenda aos interesses da investigação criminal.

In casu, o local em que o núcleo duro da associação ou organização criminosa se encontra é (deve ser) o local competente para a instrução do inquérito policial, bem como para decidir a respeito das medidas cautelares imprescindíveis ao esclarecimento dos fatos, com todas as suas circunstâncias.

Não é razoável entender que o delito investigado se revela em furto qualificado e, em razão deste, vilipendiar toda uma gama de recursos humanos especializados destacados, recursos financeiros utilizados ou disponibilizados, conhecimento produzido na identificação de suspeitos, relações entre estes, métodos de atuação na região, análise de material e todo um arcabouço jurídico e tecnológico envolvido na atuação policial.

Se por um lado se prestigia - e assim deve ser - a competência jurisdicional desde a fase do inquérito policial, por outro, é imprescindível que se respeite o tempo e o local da investigação criminal, de modo a torná-la não apenas eficiente, mas eficaz.

Atento às novas exigências da Sociedade da Informação, o Superior Tribunal de Justiça, teve a oportunidade de se manifestar sobre o tema e levou em consideração a organização criminosa existente na hipótese fática, bem como o risco para a eficiência da investigação criminal, como segue adiante:

> *[...]1. O simples fato de que duas organizações criminosas se dedicam à prática do mesmo tipo de delito (furto mediante fraude via internet, clonagem de cartões e roubo de senhas), valendo-se de modus operandi similar, por si só, não se presta a demonstrar a existência de conexão entre os processos que investigam suas condutas, máxime se ditas quadrilhas são integradas por pessoas diferentes e atuam majoritariamente em Estados da Federação diferentes. 2. Ainda que assim não fosse, o fato de que uma das investigações ainda se encontra na fase inicial do inquérito policial (com pedido de quebra de sigilo bancário e de dados) e a outra, em marcha mais adiantada, já teve denúncia oferecida e tramita como ação penal desaconselha a união dos feitos pela conexão. Isso porque tal deslocamento de competência não traria nenhum benefício em termos de celeridade e de economia processual, segurança jurídica e conveniência da instrução criminal, critérios que orientam o instituto da conexão. 3. De mais a mais, se o local onde atua a quadrilha é o Estado*

de São Paulo, onde se encontram as contas correntes de origem e de destino, nos golpes efetuados junto à Caixa Econômica Federal, é mais vantajoso que as investigações sejam ali conduzidas, solicitando-se, eventualmente, provas emprestadas relacionadas à investigação similar levada a efeito na Justiça Federal do Distrito Federal. [...] (CC 126.237/DF, Rel. Ministro REYNALDO SOARES DA FONSECA, TERCEIRA SEÇÃO, julgado em 23/09/2015, DJe 29/09/2015)

Com a razão o Tribunal da Cidadania. Muitas vezes, um ano ou mais de trabalho investigativo especializado é (ou pode ser) completamente destruído pela intromissão indevida no juízo de discricionariedade do delegado de polícia na fase do inquérito policial, com prejuízo para a sociedade.

Assim, sendo possível, importante respeitar e priorizar o melhor lugar para a investigação criminal, em detrimento da melhor técnica aplicável, em tese, na fase judicial do processo penal. E no caso das fraudes bancárias eletrônicas sempre será onde estão localizados os membros da organização criminosa e não o local das contas bancárias cujos recursos foram ilicitamente subtraídos.

Privilegia-se o conteúdo material da Constituição Federal, que afirma o direito e responsabilidade de todos com a Segurança Pública (Princípio da Cooperação, previsto no Art. 144, caput, da CF/88), em detrimento de conteúdo infraconstitucional da legislação processual penal em sentido contrário.

Pensamos, no entanto, seja importante aprofundar um pouco mais a respeito da sistematização que vem sendo feita da investigação aos novos tempos.

4.2. Projeto Tentáculos

A base de uma nova visão sistemática da investigação do delito, a partir de um prisma nacional, nasce formalmente por volta do ano de 2009, com o acordo de cooperação técnica entre a Polícia Federal e a Caixa Econômica Federal (CEF), denominado Projeto Tentáculos.

Diferentemente do que faz a maioria das instituições bancárias e até mesmo por ser uma empresa pública e, portanto, com maiores controles sobre o patrimônio, a CEF teve a "ousadia", no bom sentido, de apresentar os números reais da fraude de que era vítima à Polícia Federal, visando a tornar eficaz a atividade de investigação criminal e, por via indireta, mais complicada a vida dos criminosos.

Age em contrariedade ao senso comum, conforme menciona Misha Glenny (*Op. cit.*, p. 59), referindo-se às instituições bancárias: "*eles não querem que o público descubra a frequência com a qual seus sistemas são invadidos por criminosos eletrônicos*". O problema é que, agindo assim, "*por medo de perder uma eventual vantagem em relação à concorrência, os bancos estão indiretamente facilitando o trabalho dos cibercriminosos*" (*Idem*). Felizmente para essa experiência, a CEF tornou-se pioneira nesse novel processo de combate às fraudes bancárias.

Em relação ao Projeto Tentáculos, inicialmente, cerca de 50 mil inquéritos policiais que tramitavam de forma isolada em todas as unidades da Polícia Federal ao redor do país, a grande maioria sem grandes perspectivas de localização de autoria, foram transferidos para a então Unidade de Repressão a Crimes Cibernéticos (URCC), atual Serviço de Repressão a Crimes Cibernéticos (SRCC) da PF no Distrito Federal para ajudar a formar a Base Nacional de Fraudes Bancárias Eletrônicas (BNFBe).

A partir da cooperação citada, as agências bancárias da CEF deixaram de encaminhar *notitias criminis* individualmente às delegacias e superintendências regionais da Polícia Federal para, em vez disso, passarem a alimentar a BNFBe. Uma equipe especializada do Grupo Permanente de Análises (GPA) inclui, semanalmente, as informações recebidas contidas nos processos de contestações de fraudes considerados pertinentes pela CEF na citada base.

Dentre as informações recebidas e disponibilizadas na BNFBe, encontram-se dados cadastrais, número de contas e agências bancárias, números de cartões de crédito, número de telefones, placas de carros, endereço de lotéricas, endereços IP, etc., os quais podem ser objeto de análise cruzada e prospectiva, visando a formação do entendimento quanto à origem, quantidade e autoria das fraudes.

As análises visam, pois, à identificação das organizações criminosas especializadas, sua metodologia e seus integrantes, qual modalidade criminosa está tendo mais efetividade, em determinado período e local, qual o tamanho do prejuízo e de que maneira poderá ser saneado, viabilizando, inclusive, identificar gargalos no sistema da própria Polícia, no que concerne aos recursos humanos, materiais e tecnológicos necessários ao cumprimento do múnus constitucional.

Os resultados desse processo são apresentados nas Superintendências Regionais ou Delegacias descentralizadas da Polícia Federal, onde são registradas nas Corregedorias Regionais e recebidas como *notitias criminis* qualificadas, permitindo a instauração de Inquéritos Policiais com maior vigor, em decorrência da maior quantidade de informações disponíveis, englobando não apenas uma fraude, mas um conjunto delas, por vezes centenas, inclusive com suspeitos pré-identificados.

O foco passa a ser a organização criminosa e não a fraude considerada em sua individualidade e isso tem feito toda a diferença, como se pode ver dos dados estatísticos que demonstram quedas significativas nas ações das organizações criminosas, em especial após a realização de ações especiais no curso dos inquéritos policiais, que se convencionou denominar operações policiais, dentre as quais, em nível nacional e de 2014 a 2015, destacamos a Corrieu (SP), Tentáculos III (SP), IB2K (DF) e Sheik (GO), sendo as duas últimas referentes ao canal internet banking.

Pela metodologia antiga, cada notícia de crime gerava a instauração de um inquérito policial, com comunicações dispersas pelo país, muitas vezes até em duplicidade, com informações limitadas, sem possibilidade de cruzamento de dados, focando no local onde estava a agência bancária do cliente-vítima, e com diversas diligências sendo realizadas por meio de cartas precatórias.

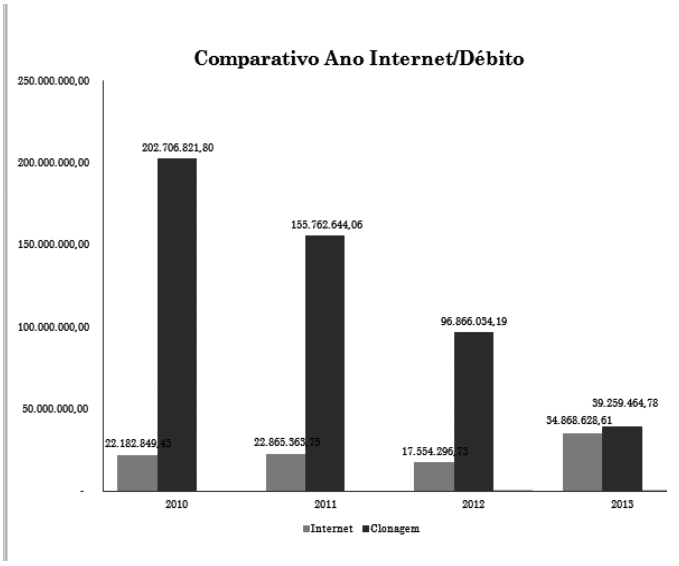
A partir da mudança paradigmática, passa-se a ter uma comunicação centralizada, com inserção de todas as informações sobre o tema em uma única base de dados (BNFBe), onde são realizados cruzamentos prévios das informações, buscando fornecer o máximo de dados de identificação da organização criminosa, sua metodologia e seus integrantes, que passa a ser o foco, inclusive para a definição da competência jurisdicional, uma vez que é onde aquela se encontra que poderão ser realizados os atos de polícia judiciária com maior eficiência e, muitas vezes, até mesmo com eficácia mínima à realização da Segurança Pública.

Em suma, a partir do projeto tentáculos cria-se uma nova forma de ver e de realizar a investigação policial, mitigando o princípio da obrigatoriedade para focar no princípio constitucional da eficiência, o qual avalia custos e resultados.

4.3. Uma breve reflexão crítica sobre os perigos da tardo-modernidade

Um estudo comparativo com base na análise das informações gerais disponíveis na BNFBe permitiu concluir que entre 2010 e 2013, a Polícia Federal investiu muito mais no combate às fraudes bancárias realizadas por meio de clonagem de cartão de débito.

Essa política de atuação da Polícia Federal teve como consequência direta uma migração da criminalidade organizada da clonagem para o canal internet banking, considerado mais seguro, uma vez que não demandaria a instalação do *skimmer* ("chupa-cabras") no terminal eletrônico da agência bancária e, portanto, menos sujeito a ações flagranciais. O gráfico abaixo ilustra bem essa perspectiva:



Fonte: Base Nacional de Fraudes Bancárias Eletrônicas da PF

Do ponto de vista metodológico, em face da sociedade de riscos (BECK, 2006) e da realidade da nova era digital (SCHMIDT; COHEN, 2013), entendemos que a experiência do projeto tentáculos tende a ser reflexo do que Winfried Hassemer (2007, p. 194) chamou de "direito penal moderno"[57]

Exemplifica essa tendência, no âmbito legislativo, a recente incriminação da mera posse do cartão de crédito falsificado (popularmente denominado "cartão clonado"), ato preparatório da conduta de furto qualificado, sutilmente agregada ao Art. 298 do Código Penal pela Lei nº 12.737, de 30 de novembro de 2012, não sem motivo apelidada de "Carolina Dieckmann".

Nesse contexto, as operações policiais contra os cibercriminosos, cada vez mais internalizadas, exigidas, enfatizadas e repetidas na mídia em geral e na mídia digital, em especial, exterioriza a exigência de aplicação do direito penal "*como instrumento pedagógico do povo para sensibilizar as pessoas*" (*Idem*, p. 196), com o objetivo declarado de ampliar a capacidade do direito penal como instrumento de controle social, não mais de *ultima ratio*, mas perigosamente de seu contrário.

Tais considerações, longe de apontar um caminho a ser seguido, que, no momento hodierno, ou ainda não há ou são vários e tortuosos, primam mais por levar o pensamento a reflexões imprescindíveis sobre os perigos da tardo-modernidade[58] (FARIA COSTA, 2012, p. 47), mais especificamente sobre a funcionalidade do sistema que se deseja e do que vem se concretizando, em suas muitas nuanças, matizes e variáveis, numa sempiterna busca pela luz ao final do túnel.

5. CONCLUSÃO

No curso deste trabalho, inicialmente demonstramos um pequeno histórico do serviço de internet banking, visando a sua adequada contextualização com a fraude bancária eletrônica.

Em seguida, apresentamos o que entendemos como crime cibernético, apontando as classificações comumente utilizadas, próprios, impróprios e mistos, enquadrando a fraude bancária eletrônica nesta última.

Descrevemos alguns dos principais métodos criminosos utilizados para a consecução dessa espécie delitiva, a exemplo do *phishing scam*, *pharming*,

[57] : "ao lado do abandono do metafisicismo como movimento geral do pensamento jurídico penal, as três características conhecidas são as seguintes: proteção ao bem jurídico, prevenção e orientação pelas consequências".

[58] "[...] é no processo (penal) que qualquer tensão ou desequilíbrio normativo que ultrapasse o razoável tornará todo o sistema ineficiente e, pior, injusto. O equilíbrio entre os valores de segurança e garantia que devem envolver a figura do arguido e os interesses ou valores de celeridade processual e eficácia tem que ter um ponto de equilíbrio instável nem sempre fácil de determinar."

distribuição de *malwares* por meio de SPAM e técnicas de engenharia social.

Em razão da grande celeuma envolvida no início dos anos 2000, em especial no âmbito jurisprudencial e doutrinário, a discussão sobre a definição do tipo penal para definição adequada da fraude bancária eletrônica, pareceu-nos importante e teve seu lugar reservado, concluindo que, apesar da complexidade da conduta, trata-se de furto qualificado e não estelionato.

Do mesmo modo, foi objeto de análise acurada a sempre envolvente questão da competência penal, em especial em se tratando de crimes cibernéticos, onde apontamos a importância de que seja definida desde a fase do inquérito policial, porém tendo especial consideração por suas peculiaridades, eficiência e eficácia, sob pena de inviabilizar a fase judicial do processo. Além disso, sempre que envolver associação ou organização criminosa, o local onde esta se encontra deve ser o critério definidor da competência penal.

Ao final, cuidamos de apresentar um pouco do que é o processo de investigação criminal da fraude bancária cibernética, com especial atenção ao novel Projeto Tentáculos, que modificou e vem modificando de forma paradigmática o modo de fazer a investigação, com provável repercussão para outros tipos penais. Objetivou-se permitir sua compreensão fenomênica, inclusive para a fase judicial do processo penal.

Encerramos com uma brevíssima, mas necessária, reflexão crítica quanto ao modo de atuação da investigação criminal diante da criminalidade cibernética organizada, concluindo que a busca desenfreada pelo combate ao crime pode levar a caminhos perigosos.

6. REFERÊNCIAS

BANCÁRIO.PT. Disponível em: <http://bancario.pt/internet-banking-e-banking/>. Acesso em: 14.12.2015.

BECK, Ulrich. **La sociedad del riesgo: hacia una nueva modernidad**. Barcelona: Paidos Iberica, 2006.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência nº 87.057-RS**, Rel. Min. Maria Thereza de Assis Moura, julgado em 13/2/2008.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência nº 126.237/DF**, Rel. Min. Reynaldo Soares da Fonseca, Terceira Seção, julgado em 23/09/2015, DJe 29/09/2015.

CONVERGÊNCIA DIGITAL. Apenas 4% dos correntistas brasileiros fazem operações financeiras no banco móvel. 14.abr.2015. Disponível em:< http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/stArt.htm?infoid=39376&sid=5#.VS5X9LkU-9I>. Acesso em 15.12.2015.

DINIZ, Eduardo Henrique. **10 anos de internet banking: desvendando o processo de incorporação de tecnologia em um banco brasileiro através de uma abordagem sociotécnica**. São Paulo: FGV, 2006. Disponível em:<https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/13387/10%20Anos%20de%20Internet%20Banking.pdf>. Acesso em: 14.12.2015.

FARIA COSTA, José de. **Noções fundamentais de direito penal**. 3. ed. Coimbra: Coimbra Editora, 2012.

GLENNY, Misha. **Mercado sombrio: o cibercrime e você**. Trad.: Augusto Pacheco Calil, Jorge Schlesinger, Luiz A. de Araújo. São Paulo: Companhia das Letras, 2011.

G1. **Sites de bancos no Brasil ganham extensão 'b.br'**. 24.09.2008. São Paulo. Disponível em:

<http://g1.globo.com/Noticias/Tecnologia/0,,MUL771767-6174,00.html>. Acesso em: 14.12.2015.

HASSEMER, Winfried. **Direito penal libertário**. coord. superv. Luiz Moreira. Belo Horizonte: Del Rey, 2007.

IDG NOW! Brasil é o sétimo país em internet banking. 27.out.2005. Disponível em: <http://idgnow.com.br/internet/2005/10/27/idgnoticia.2006-03-12.81926265 95/>. Acesso em: 15.12.2015.

JARDIM, Afranio Silva. **Direito processual penal**. 7. ed. rev. atual. Rio de Janeiro: Forense, 1999.

KAPERSKY Labs. **Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year**. 20.jun.2013. Disponível em:< http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_

3_million_users_experienced_phishing_attacks_in_the_last_year>. Acesso em: 15.12.2015.

PINHEIRO, Patricia Peck. **Direito digital**. 4. ed. rev. atual. ampl. São Paulo: Saraiva, 2010.

RAMZAN, Zulfikar. Phishing attacks and countermeasures. In: STAMP, Mark; STAVROULAKIS, Peter. **Handbook of Information and Communication Security**. Springer, 2010.

SANTOS, Célio Jacinto dos**. Investigação criminal especial**. Porto Alegre: Núria Fábris, 2013.

SCHMIDT, Eric; COHEN, Jared. **A nova era digital: como será o futuro das pessoas, das nações e dos negócios**. trad. Ana Beatriz Rodrigues; Rogério Durst. Rio de Janeiro: Intrínseca, 2013.

SOBRAL, Carlos Eduardo Miguel; BEZERRA, Clayton da Silva. A investigação dos crimes cibernéticos e a segurança pública cibernética. *In*: **Inquérito policial: doutrina e prática**. Org. Clayton da Silva Bezerra e Giovani Celso Agnoletto. São Paulo: Letras Jurídicas, 2015.

SOUSA, Stenio Santos. **Investigação criminal cibernética: por uma política criminal de proteção à criança e ao adolescente na internet**. Porto Alegre: Núria Fabris, 2015.

STANFORD Federal Credit Union. **About us**. Disponível em: <https://www.sfcu.org/about/>. Acesso em: 14.12.2015.

SYMANTEC. **Online fraud: pharming**. Disponível em: <http://us.norton.com/cybercrime-pharming>. Acesso em: 13.12.2015.

VALENTE, Manuel Monteiro Guedes. **Ciências policiais: ensaios**. Lisboa: Universidade Católica, 2014.

WIKIPEDIA. Disponível em: <http://www.wikipedia.com>. Acesso em dez.2015.

CAPÍTULO V

Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal

Erick Ferreira Blatt[59]

1. INTRODUÇÃO

O acesso à internet está amplamente difundido no mundo e se tornou parte da cultura brasileira. Milhões de residências dispõem de conexão à rede e, além disso, quem não dispõe de acesso residencial ou no trabalho, tem acesso à internet através de *tablets* e *smartphones*.

Os serviços oferecidos estão se ampliando e se popularizando, o comércio eletrônico vem crescendo em volume de vendas, os sites de bancos oferecem tantas facilidades para o cliente que acabam se tornando raras as vezes em que é necessário ir até uma agência bancária para pagar uma conta, por exemplo.

Até mesmo órgãos governamentais também têm disponibilizado vários serviços em suas páginas, como emissão de certidões, entrega de declarações e esclarecimento de dúvidas. As pesquisas para estudo, que antes eram restritas às bibliotecas, agora são possíveis na rede, sendo corriqueiro encontrar farto material de qualidade para consulta.

[59] O autor é Delegado de Polícia Federal desde 2006. Agente da Polícia Civil do DF de 2002 a 2006. Advogado nas áreas cível e tributária de 1999 a 2002. Formado em Direito pela Universidade Federal do Rio de Janeiro. Especialista em Investigação Criminal pela Academia Nacional de Polícia - ANP. Especialista em Políticas de Segurança Pública e Direitos Humanos pela Universidade Federal do Mato Grosso. Pós-graduado em Direito Penal Econômico e Criminalidade Organizada pela Universidad de Castilla-La Mancha - Espanha. Pós-graduado em Direito Penal e Processo Penal pela Universidade Católica Dom Bosco. Mestre em Direito Penal - Universidad Castilla-la Mancha, Doutor em Direitos Humanos e Constitucionais pela mesma Universidade. Atualmente é Coordenador do Grupo de Repressão aos Crimes Cibernéticos da Superintendência de Polícia Federal no Rio de Janeiro, já tendo sido Chefe da Delegacia de Defesa Institucional, de Crimes Financeiros e da Delegacia de Imigração na Superintendência de Polícia Federal no Mato Grosso, além de Representante Regional da INTERPOL naquele Estado. Atuou ainda na Corregedoria da PF no Rio de Janeiro e no combate à pedofilia na DELINST/SR/PF/RJ. Tem experiência na área de Direito, com ênfase em Direito Penal, Processual Penal e Administrativo, já tendo exercido a função de professor por diversas vezes na Academia Nacional de Polícia, além da UFMT e UFRJ como professor convidado. Atua desde 2007 como tutor dos cursos EAD da Senasp nas áreas de segurança pública e direitos humanos.

Porém, o uso ilícito da rede também está acompanhando o seu crescimento, pois os criminosos a utilizam como uma ferramenta para atingirem seus objetivos. Os pedófilos usam sites, redes ponto a ponto como *Kazaa e eMule* ou correio eletrônico, para a troca de imagens pornográficas. Os sites de relacionamentos podem ser usados para a calúnia, difamação, apologia ao crime, exposição de pedofilia e negociação de produtos ilícitos, dentre outras modalidades.

Muitos dos crimes que estão sendo ou que podem ser cometidos com o uso da internet no Brasil são investigados pela Polícia Federal Brasileira, sendo que o fato do crime ser cometido na rede no Brasil não altera o juízo competente para julgá-los nem o órgão responsável por reprimi-los. Diversos trabalhos nessa área já foram realizados com êxito, grandes operações, muitas coordenadas com as polícias de outros países, foram desencadeadas e apresentaram excelentes resultados com muitas prisões e apreensões.

2. INVESTIGAÇÃO CRIMINAL NA INTERNET

Muitos crimes podem ser cometidos com auxílio da tecnologia da informação ou contra redes e sistema de informática e são várias as áreas de atuação no Brasil das polícias, investigadores particulares e peritos com o objetivo de produção de provas ou mesmo de elucidação de delitos.

A Constituição Federal Brasileira em seu artigo 144 define quais os órgãos são responsáveis pela segurança pública e atribuem a função de polícia judiciária e a apuração de infrações penais às polícias Civis e Federal, indicando os casos em que cada uma deve atuar[60]

A investigação dos crimes que utilizaram a rede mundial de computadores, portanto, é responsabilidade dos órgãos policiais citados acima e o fato de o crime ter sido cometido com o uso da internet, por si só, não altera a atribuição para uma ou outra instituição, se o crime em questão, no caso de ser cometido fora da rede, está entre os que devem ser investigados pela Polícia Civil, quando for cometido com o seu uso, também será investigado pela mesma.

> ***Art. 1º*** *Na forma do inciso I do § 1º do Art. 144 da Constituição, quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no Art. 144 da Constituição Federal, em especial das Polícias Militares e Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais [...]*[61].

[60] BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil.* Disponível em http://www.planalto.gov.br/ccivil03/constituicao/constituiçao.html
Acesso em: 28/11/2015

[61] BRASIL. Lei 10.446 de 08 de maio de 2002. Dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do § 1º do Art. 144 da Constituição. Publicado no D.O.U. de 9.5.2002. Disponível em

Assim sendo, apesar das atribuições originariamente cometidas às polícias civis e militares dos Estados, o texto legal da Constituição Federal Brasileira, amplia a competência da Polícia Federal para reprimir o crime cometido pela internet, desde que a infração penal tenha repercussão interestadual ou internacional, exija repressão uniforme e seja autorizada ou determinada pelo Ministro da Justiça.

Já existem no Brasil alguns grupos especializados na investigação de crimes cibernéticos, porém normalmente enfrentam muitas dificuldades para a execução de seu trabalho devido à carência de pessoal especializado, de materiais e dificuldades com a falta de legislação específica.

A Polícia Federal mantém na estrutura da Coordenação Geral de Polícia Fazendária - CGPFAZ/DIREX um Serviço de Repressão a Crimes Cibernéticos (SRCC), com ramificações em várias Superintendências Regionais da Polícia Federal com os Grupos de Repressão a Crimes Cibernéticos (GRCC), os quais vêm realizando diversas operações de grande porte visando a repressão aos crimes cometidos pela internet e os que utilizam de tecnologia computadorizada, tendo resultado em muitas prisões. Cabe dizer aqui que desde janeiro de 2014, este signatário é o Coordenador do GRCC/DRCOR/SR/DPF/RJ.

2.1. Principais problemas da criminalidade na internet

Para o combate à criminalidade na internet é preciso superar os variados empecilhos apresentados e que estão relacionados não só às lacunas legislativas, mas também quanto aos reflexos ocasionados pela liberdade de expressão aliado ao rápido desenvolvimento das tecnologias.

Como a internet está apoiada no anonimato dos usuários, fica difícil a identificação de quem pratica crimes através de sua rede de informações que são, na verdade, dados digitais, os quais podem ser destruídos, dificultando assim a realização do flagrante.

Dificuldade também quanto ao tempo da persecução, que caso não aconteça rapidamente pode inviabilizar o acesso ao criminoso, uma vez que o resultado da investigação só aparece tempos depois do ato praticado, e se aqueles que investigarem não agirem com métodos específicos e com celeridade, terão grandes problemas com a localização do sujeito ativo.

Aliado a esse fato existe também uma falta de conscientização em termos de prevenção quando se navega pela rede mundial. Milhões de usuários conectam-se diariamente à rede, sem nem ao menos terem em seus computadores um bom sistema antivírus, que possa dificultar invasões em seus computadores. Acessam páginas na internet sem verificar se aquela empresa que oferece *"ótimas vantagens online"* existe de fato, se é idônea, se atendeu outros clientes sem nenhum tipo de problema. A maioria não tem a devida cautela e ainda respondem aos mais variados tipos de pesquisas com dados financeiros e pessoais, mesmo sabendo o perigo que incorrem quando o fazem.

<http://www.planalto.gov.br/ccivil03/Leis/2002/L10446.htm>. Acesso em: 28/11/2015

As leis brasileiras ainda não estão adequadas à realidade mundial, assim como na maioria dos outros países. Aliado a esse fato, alguns grupos tentam de todas as formas possíveis dificultar o surgimento de tais leis, alegando que elas estariam inibindo a liberdade de expressão e a plena democracia, duas das mais importantes características da rede mundial. É inegável que se teve algum avanço com a edição do Marco Civil na internet, porém as penas são muito brandas e estão longe das ideais.

Além disso, existe outra grande barreira no avanço dessas leis, já que um crime pode ser cometido em um país contra alguém em outro, e nesse, não ser considerado um crime. Cumpre dizer que a territorialidade desaparece em termos de rede, ou fica mais difícil de ser verificada, tornando-se também barreira na aplicação das leis.

A falta de leis internacionais específicas dificulta ainda a investigação para saber onde o crime foi executado, onde gerou resultados, o material obtido, a autoria e a identificação da sua respectiva culpa, todos ainda são fatores que tornam problemática a punição dos internautas de má-fé.

Novas tecnologias surgem a cada dia, tanto do lado daqueles que estão tentando dificultar esse tipo de atitude, mas também por parte dos usuários que agem de má-fé, pois na realidade, eles estão sempre buscando formas de burlar os conteúdos e parâmetros impostos. É uma verdadeira briga de gato e rato, onde o vencedor leva como prêmio maior a fama, mesmo que restrita. Para combatê-los, seria necessário dispor de técnicos e estrutura altamente especializados, que estivessem à frente desses usuários.

As provas desses crimes são, até certo ponto, manipuláveis, já que são documentos eletrônicos que podem ser modificados devido à necessidade do autor. As máquinas, em si, podem ser identificadas, pois quando conectadas à grande rede utilizam-se de uma assinatura digital - o IP -, que irá dizer qual computador teve acesso àquela informação ou enviou certo arquivo, restando somente a difícil análise em saber qual foi o usuário daquele computador.

3. METODOLOGIA INVESTIGATIVA DE CRIMES CIBERNÉTICOS

Pois bem, nos atendo às especificidades deste artigo, cumpre adentrarmos ao nosso tema específico, ou seja, a análise de alguns métodos de investigação e ferramentas utilizadas pela Polícia Federal na repressão aos crimes cibernéticos. Certamente que aqui não há um rol exaustivo e não haverá grande profundidade na análise de cada item descrito, mas sim uma exposição, ainda que concisa, dos principais elementos analisados em uma investigação.

Quando um crime é cometido com o uso da internet é preciso buscar e analisar informações que possam ajudar na identificação do criminoso, tanto no mundo virtual quanto no mundo real. Muitas vezes somente a análise de uma única informação não será suficiente para o esclarecimento do delito, sendo necessárias diversas ligações de fatos e a quebra do sigilo de dados dos suspeitos.

Um ponto que deve ser observado quando se busca informações relativas à internet é que, por se tratar de uma rede mundial, informações relativas à data e hora podem estar apresentadas com fusos horários diferentes. A hora mundial tem por base, normalmente, o meridiano de Greenwich GMT (Greenwich *Mean Time),* ou relógios atômicos que registram o *IAT (International Atomic Time)*. Atualmente, para a maioria dos fins, utiliza-se o UTC *(Universal Time, Coordinated)* para indicar fusos horários, o UTC é o tempo registrado nos relógios atômicos e todos os demais 23 fusos horários do globo são relativos a ele[62].

No Brasil o horário oficial (Brasília) possui uma diferença de três horas a menos em relação ao UTC, logo é representado como UTC -3. Quando estamos em horário de verão essa diferença diminui e passa a ser representado como UTC -2. Vale lembrar, ainda, que o Brasil possui outros dois fusos horários que são UTC -2 para Fernando de Noronha e Ilha de Trindade e UTC -4 para os estados do Mato Grosso, Mato Grosso do Sul, Amazonas, Rondônia, Roraima e Acre.

Outras formas de se referir aos fusos horários podem ser encontradas em registro de servidores ou cabeçalhos de mensagens de correio eletrônico como o PDT *(Pacific Daylight Saying Time)* que seria o UTC -*7 (Daylight Saving Time* se refere a horários de verão), BRST *(Brazilian Summer Time)* equivalente a UTC -2, BRT *(Brazilian Time)* igual a UTC -3 e outra forma, ainda, é apenas uma seqüência de quatro zeros (0000) que se refere ao próprio UTC.

3.1. Os serviços de Whois

Os serviços de *Whois* oferecem acesso a alguns dados que podem identificar os responsáveis pelos domínios registrados na internet, esse acesso é público e pode ser feito a partir de qualquer computador ligado à internet. Os Registradores Regionais, os Registradores Locais e também os Registradores credenciados pela ICANN precisam manter os serviços de *Whois,* que visam permitir identificar os responsáveis por um domínio ou a quem foi alocado um determinado endereço IP.

O Serviço de *Whois* do Comite Gestor da Internet no Brasil é acessado por meio do endereço <http://registro.br> e informa diversos dados do responsável por um dominio.br ou por um endereço IP alocado para o Brasil, entre essas informações disponibilizadas estão o nome da empresa ou pessoa responsável pelo IP ou domínio, o endereço para contato e o número do telefone.

Analisar, portanto, o papel dos órgãos responsáveis pelo controle de nomes de domínio e endereços IPs na internet em nível mundial, regional e também no Brasil é necessário para toda e qualquer investigação na internet, e o contato com tais instituições pode ser muito importante na busca por informações úteis para a definição de materialidade e autoria de delitos.

[62] NOVO MILÊNIO. Jornal Eletrônico. *Fusos Horários e Códigos (time zones e Codes)*. Disponível em http://www.novomilenio.inf.br/porto/mapas/nmfusos.htm>. Acesso em 23/11/2015.

3.2. Análise do cabeçalho da mensagem de e-mail

Quando o crime é cometido com o uso do e-mail as mensagens podem ser ricas em informações, uma mensagem de correio eletrônico é constituída basicamente de duas partes, o corpo da mensagem e o seu cabeçalho. É justamente neste último que constam as mais importantes informações, algumas colocadas pelo software cliente de e-mail, por outros programas, como antivírus ou pelo próprio usuário e outras adicionadas pelos servidores SMTP envolvidos na transação, essas últimas, que não podem ser manipuladas pelo emissor, mas somente pelos servidores envolvidos, é que são as mais importantes para a identificação do remetente[63].

> *Quando a evidência investigada for um e-mail (por exemplo, uma mensagem que contenha arquivos com pornografia infantil anexado) é preciso não apenas preservar o conteúdo da mensagem, como também* ***identificar o cabeçalho do e-mail,*** *ou seja, a parte do e- mail que informa os dados do remetente e do destinatário da mensagem. O objetivo é aquele já mencionado: descobrir o número IP, a data e a hora da transmissão e a referência à hora GMT.*[64]

No cabeçalho de uma mensagem de correio eletrônico cada linha começa com uma palavra (campo) seguida pelo sinal de dois pontos (:), nem todos os campos são obrigatórios. O significado de alguns campos é indicado nas tabelas abaixo[65]:

Cabeçalho	Significado
To:	O(s) endereço(s) de correio eletrônico do(s) destinatário(s) principal(is)
Cc:	O(s) endereço(s) de correio eletrônico do(s) destinatário(s) secundário(s)
Bcc:	O(s) endereço(s) de correio eletrônico para cópias carbono ocultas
From:	A(s) pessoa(s) que criou(aram) a mensagem
Sender:	O endereço de correio eletrônico do remetente
Received:	A linha incluída por cada agente de transferência ao longo da rota
Return- Path:	Pode ser usado para identificar um caminho de volta ao remetente

Tabela 1- Os campos de cabeçalho relacionados ao transporte de mensagens.

[63] TEIXEIRA, R.C. *Combatendo o Spam*. São Paulo: Novatec Editora, 2014.
[64] COMITÊ GESTOR DA INTERNET NO BRASIL. *Manual Prático de Investigação de Crimes Cibernéticos*. São Paulo: Comitê Gestor da Internet no Brasil, 2014. Não paginado.
[65] TANEMBAUM, A. S. *Redes de Computadores*. 4. ed. São Paulo: Editora Campus, 2013, p. 618.

Cabeçalho	Significado
Date:	A data e a hora em que a mensagem foi enviada
Reply-to:	O endereço de correio eletrônico para onde as respostas devem ser enviadas
Message-id:	O número exclusivo que será usado para fazer referência a ssa mensagem posteriormente
In-Reply-To:	Message-Id da mensagem original correspondente a essa resposta
References:	Outras Message-Ids relevantes
Keywords:	Palavras-chave do usuário
Subject:	Pequeno resumo da mensagem apresentado em apenas uma linha

Tabela 2 - Alguns campos usados no cabeçalho de mensagem RFC 822.

O principal campo a ser analisado no cabeçalho de um e-mail é o *Received,* pois é muito difícil de ser adulterado e indica a trajetória da mensagem. O campo *Received* apresenta os subcampos *"From:,"* que indica o servidor que enviou a mensagem; "By", que indica o nome do servidor que recebeu a mensagem; *"Via",* que indica o caminho físico da mensagem; *"With",* que indica o protocolo de comunicação utilizado; *"Message-ID",* com uma identificação única da mensagem, e o campo *"For",* com o e-mail do destinatário.[66]

> *Uma linha contendo Received. é incluída por cada agente de transferência de mensagens ao longo do percurso. A linha contém a identidade do agente, a data e a hora em que a mensagem foi recebida e outras informações que podem ser usadas para localização de bugs no sistema de retomada.*[67]

A princípio o correio eletrônico seria capaz de enviar somente textos puros, porém a RFC 1341 (RFC = request for comments), atualizada pelas RFCs 2045 a 2049 (são documentos de referência), propôs uma solução que é amplamente adotada, chamada MIME *(Multipurpose Internet Mail Extensions)* que permite o envio de mensagens contendo arquivos de áudio, vídeo, binários ou qualquer outro formato. O MIME utiliza campos de cabeçalho próprios como: *MIME-Version,* que indica a versão utilizada e *Content-Type,* indicando tipo e subtipo do arquivo.

Segundo a RFC 822, os usuários podem criar cabeçalhos para seu próprio

[66] TEIXEIRA,R.C. *Combatendo o Spam*. São Paulo: Novatec Editora, 2014.
[67] TANEMBAUM, A. S. *Redes de Computadores*. 4. ed. São Paulo: Editora Campus, 2013, p. 634.

uso, porém todos eles devem iniciar com *a string "X-",* sempre que um campo do cabeçalho iniciar por "X-" significa que ele foi criado por um aplicativo (um antivírus, por exemplo) ou pelo usuário.

3.3. Análise de logs de servidores

Servidores SMTP, POP3, IMAP, WEB, *Proxy, Free Shell,* entre outros, registram em arquivos de *log* todas as conexões a eles realizadas, registrando dados relativos às transações efetivadas, formando um valioso banco de dados de informações relativas a datas e horários de acesso, endereços IP, usuários, etc.

Os *logs* podem conter informações como o nome de *login* utilizado, data e hora de início e término da conexão, tempo que ficou conectado, telefone que originou a conexão e endereços IP ou MAC. No Brasil esses *logs,* dependendo do provedor, podem ficar disponíveis por noventa dias ou em alguns casos por até cinco anos.[68]

Várias são as situações em que é preciso analisar nos registros de um servidor para buscar a autoria de um crime, como nos casos de delitos envolvendo perfis do Facebook, fóruns de discussão, fotologs e até mesmo no caso de furto realizado por intermédio dos serviços de *internet banking*.

O Facebook é atualmente o site de relacionamentos mais popular na internet brasileira e mundial. É sediado nos Estados Unidos da América e com representação no Brasil. Quem se cadastra passa a ter um perfil por meio do qual é possível escrever recados para outros usuários, visualizar outros perfis, expor fotografias, vídeos e criar ou participar de grupos ou comunidades temáticas. Para realizar o cadastro no Facebook só é preciso informar um endereço de e-mail ou número de telefone, que será utilizado como nome de *login e* escolher uma senha.

Quando um crime é cometido nesse ambiente e se faz necessário identificar quem criou um perfil, será preciso requisitar, mediante ordem judicial, à empresa *Facebook Inc.,* por meio de seus representantes no Brasil, todas as informações possíveis relativas às conexões realizadas pelo usuário do perfil em questão e as informações relativas à conexão realizada para a sua criação ou alteração. Quando essa requisição for respondida é preciso analisar com atenção os *logs* fornecidos pela empresa, a fim de identificar os endereços IPs envolvidos, não se esquecendo de verificar a data e hora das conexões que normalmente são informadas em UTC. Verificando-se com essa análise que existem endereços IPs alocados para o Brasil, por meio de consulta a serviços de *whois,* o próximo passo é requisitar que a empresa responsável informe a qual de seus usuários foi atribuído esse endereço na data e hora da conexão.

[68] MARIMOTO, C.E. *Faixas de Endereço IP, CIDR e Máscara de Tamanho Variável* – Tutorial. 17/04/2013. Disponível em <http://www.guiadohardware.net/tutoriais/enderelo-ip-cidr/>. Acesso em: 25/11/2015.

3.4. Interceptação de correspondência eletrônica

Quando um crime vem sendo cometido com o uso do correio eletrônico é possível que seja requisitada judicialmente, a quebra do sigilo de dados das contas de e-mails utilizadas, o pedido ao juiz deve ser para que ele determine ao provedor responsável pela conta, que desvie todas as mensagens, enviadas ou recebidas, para uma conta de monitoramento, permitindo que elas possam ser analisadas. No início da investigação é importante pedir que todos os *logs* de conexão que registraram acesso à conta alvo, inclusive para a sua criação, também sejam disponibilizados pelo provedor. Com o monitoramento das mensagens será possível saber com quem o alvo se corresponde e de onde normalmente realiza os acessos.

Um exemplo do uso desse método de investigação é em crimes em que alguém começa a oferecer produtos ilícitos (remédios abortivos, armas, diplomas falsos ou até drogas) em fóruns de discussão e só permite o contato por intermédio de e-mail. Num caso como esse, além do monitoramento do correio eletrônico também é importante requisitar registros de conexão aos responsáveis pelo fórum ou página *Web* onde os produtos foram anunciados.

3.5. Análise de pacotes de dados

Existem diversas quadrilhas especializadas em fraudes contra instituições financeiras, na maioria das vezes, elas são muito organizadas, possuem uma rígida distribuição de tarefas e seus membros estão espalhados por todo o país. Nessas quadrilhas existem programadores que desenvolvem *os malwares* responsáveis pela captura de senhas de acesso, *spammers* que realizam *o phishing scam* e os "laranjas" que disponibilizam contas correntes em seus nomes para as transferências fraudulentas. Alguns *softwares* maliciosos criados por essas quadrilhas ficam residentes na memória do computador contaminado, aguardando que seja realizado acesso a um sistema de *internet banking,* no momento em que o usuário fornece sua senha, sem que ele saiba, os dados são capturados e enviados para a quadrilha por intermédio de e-mail.

Há ferramentas que permitem interceptar o tráfego de dados em um adaptador de rede, visualizando os pacotes enviados e recebidos. O monitoramento da interface de rede do computador contaminado pode permitir a identificação do envio de e-mail pelo *malware,* com essa informação é possível iniciar o monitoramento das mensagens recebidas pela quadrilha.

Por ordem judicial também é possível a interceptação de todo o fluxo de dados em uma conexão ADSL, tornando possível a análise de todas as informações que trafegam por esse canal de acesso à rede na busca de dados que possam interessar para as investigações.

3.6. Identificação de sites

As páginas web podem ser utilizadas para a exposição de pornografia infantil, venda de produtos ilícitos, apologia ao crime e para o cometimento de

diversos crimes. A identificação dos responsáveis por uma página na internet nem sempre é tarefa fácil, normalmente quando a ilegalidade do conteúdo do site é visível, os criminosos procuram registrar o domínio e hospedá-lo em outros países, porém quando se busca passar uma falsa imagem de legalidade, o registro do site pode ser realizado sob o domínio de primeiro nível ponto".br".

Como foi visto, quando alguém registra um nome de domínio no Brasil, o servidor que armazenará o conteúdo do site não precisa especificamente ser brasileiro. É possível descobrir o endereço IP do servidor web que está armazenando um determinado site com a utilização do comando *ipconfig* do *Windows*. Para se utilizar deste comando os passos são os seguintes: pressiona-se o botão esquerdo do mouse sobre o botão iniciar, depois em "executar"; na caixa de diálogo que aparece é preciso digitar o comando "cmd" que ativa o interpretador de comandos, após o pressionamento da tecla *"enter"* surge uma tela preta com um sinal de *prompt* onde deve ser digitado o comando *ipconfig* seguido de um espaço e o endereço do site a ser pesquisado. Como resposta, o comando realiza uma consulta ao DNS e retorna o endereço IP do servidor, uma consulta a sites de *whois* sobre esse endereço permite saber se ele foi alocado para o Brasil.

Outro comando disponibilizado pelo *Windows* que pode ser útil na localização de um site ou até mesmo de um endereço IP é o *tracert,* que traça uma rota até o endereço ou domínio consultado, indicando todos os roteadores pelos quais é preciso passar para se chegar até o destino, para a utilização do comando é só digitar no *prompt* do interpretador de comandos, *"tracert",* um espaço e o endereço a ser consultado.

3.7. Algumas considerações sobre métodos de investigação

São muitas as especificidades de cada caso de investigação dos crimes cometidos com o uso da internet, como numa operação matemática um erro pequeno em relação a um número ou um horário pode levar os trabalhos para uma direção totalmente errada, a responsabilidade é muito grande para os policiais envolvidos nos trabalhos relativos aos crimes cibernéticos, sendo preciso sempre estar muito atento às minúcias.

O professor titular da Faculdade Econômica da Universidade de Barcelona, Diogo Torrente[69], declarou que:

Otro tipo de inconvenientes tiene que ver con la fiabilidad e integridad de los datos. La naturaleza de los datos digitales hace que su manipulación pueda ser fácil si no se toman las medidas adecuadas. Por ello, los expertos destacan la complejidad y necesidad de garantizar la autenticidad, integridad y fiabilidad de las informaciones y de certificar su origen auténtico. También está

[69] TORRENTE, Diogo. Conferencia *AEEC: en Busca de una definición para Prueba Electrónica*. CYBEX. e-newsletter. Pruebas electrónicas y Computer Forensics. Abril, 2014, nº 26.

la cuestión delicada de cómo conservar dichas pruebas adecuadamente para que no pierdan valor ante un juez. Un inconveniente adicional que destacan varios expertos es la complicada identificación de la autoría de un delito de carácter telemático.

Outro tipo de dificuldade tem a ver com a confiabilidade e integridade dos dados. A natureza dos dados digitais faz com que sua manipulação seja fácil se não forem tomadas medidas adequadas. Portanto, os especialistas destacam a complexidade e a necessidade de garantir a autenticidade, integridade e confiabilidade das informações e certificar a sua verdadeira origem. Há também a delicada questão de como preservar as provas adequadamente, assim ele não perde valor perante um juiz. Outro problema que os especialistas enfatizam é a complicada identificação da autoria de um crime de caráter telemático. (tradução do autor)

Muitas vezes, somente peritos criminais conseguirão fazer a extração de dados de um disco rígido, a busca por registros de conexões em um servidor, a quebra de criptografia, entre outras. Estas são tarefas que se recomenda serem realizadas por tais profissionais que, por meio de laudos, passarão para o delegado que preside o inquérito as informações para serem analisadas. Quando nos deparamos com um site que por si só é prova de crime, também é o perito que poderá efetuar um laudo constatando a existência do site criminoso.[70]

Algumas grandes operações de abrangência nacional realizadas pela Polícia Federal do Brasil procuram reprimir um determinado tipo de crime, porém não existe uma única organização por trás de todas as ocorrências, mas sim, diversos grupos independentes espalhados pelo país, nesse caso é melhor dividir a investigação para que cada descentralizada atue em sua área circunscricional, porém com a coordenação de um órgão central, nesse caso, os levantamentos e até os pedidos de busca e prisão, necessários para o desencadeamento final da operação, precisam ser descentralizados.

Todavia, quando se trata de uma única organização criminosa, o melhor parece ser o trabalho centralizado. Crimes realizados com o uso da internet anteriormente eram instaurados para apurar cada fato isoladamente e, muitas vezes, em uma mesma Unidade, vários Delegados instauravam inquéritos para apurar esses crimes sem saber que possuíam ligação. Dessa forma, se uma quadrilha cometesse diversos furtos pela internet em todo o país, seria instaurado um inquérito para cada furto e as chances de responsabilização do grupo eram mínimas.

Desde 2010 a Polícia Federal Brasileira possui o projeto Tentáculos, no qual é utilizado um software que é o responsável por fazer uma análise que associa as características comuns de diferentes transações ilícitas, espalhadas por todo o

[70] CAMPELLO, R. S. ET AL. *Informática Forense*. Brasília: Academia Nacional de Polícia, 2013, p. 22.

território brasileiro, permitindo uma investigação mais efetiva. A ideia inicial foi a de realmente juntar todos os dados num programa de computador (alimentado através da Base Nacional de Fraudes Bancárias Eletrônicas) de milhares de notícias-crime recebidas sobre crimes cibernéticos viabilizando uma investigação otimizada dos processos.

Muitos crimes cibernéticos acontecem com ações em vários países, inclusive os membros de uma quadrilha podem estar espalhados pelo mundo, sendo que em casos onde há a necessidade de ações ou busca de informações em outros países é possível contar com a colaboração dos policiais federais lotados na Coordenação Geral de Polícia Criminal Internacional. Atualmente participam da Organização Internacional de Polícia Criminal (OIPC/INTERPOL) 186 países membros.

> *Conforme disposto no Art. 2° do seu estatuto, a Interpol tem como finalidade principal desenvolver a mais ampla assistência recíproca por parte das autoridades de polícia criminal, bem como estabelecer e desenvolver parcerias com todas as Instituições que possam contribuir para a prevenção e repressão das infrações ao direito comum, dentro do marco das leis dos diferentes países e do respeito à Declaração Universal de Direitos Humanos*[71]

A Interpol também possui um sistema mundial de comunicação para troca de informações chamado I-24/7, que funciona vinte e quatro horas por dia, nos sete dias da semana. Qualquer policial federal pode solicitar uma senha de acesso a esse sistema para realizar consulta a seus bancos de dados. Em muitas investigações de crimes cibernéticos são necessárias algumas informações desse sistema ou da ajuda dos policiais lotados na CGPCI (Coordenação Geral de Polícia Criminal Internacional).

> *A Interpol dispõe de uma excepcional base de dados internacionais com milhares de imagens sobre delitos contra menores, as quais têm sido enviadas por organismos encarregados da aplicação da lei em todo o mundo. Essa base de dados foi concebida para facilitar a identificação das vítimas e dos agressores. Permite centralizar os dados enviados por países membros e facilita a coordenação das investigações, evitando a duplicação de tarefas. Sua análise ajuda a localizar os produtores e distribuidores de imagens sobre delitos contra menores.*[72]

Os policiais que trabalham com investigações dessa natureza precisam

[71] FILHO, A. L. K.; SOUZA, V. G. L. *Polícia Criminal Internacional.* Brasília: Academia Nacional de Polícia, 2014. p. 8.
[72] Idem. p. 26.

acessar o sistema I-24/7, inclusive para alimentá-lo com informações, a fim de colaborar com outros países.

As ferramentas de busca da internet, como o Google, também podem ser utilizadas para a investigação de crimes. As consultas podem ser realizadas de diversas formas, pesquisando por um único termo ou por frases completas, muitas vezes a página indicada no resultado da pesquisa e que possui a informação desejada já foi retirada do ar, porém o Google mantém uma cópia, em muitos casos, idêntica à que o sistema acessou quando da inclusão da referência a ela na ferramenta, essa cópia pode ser acessada por intermédio da opção "em *cache"*.

Para a análise dos registros de conexão a servidores fornecidos mediante ordem judicial é muito importante, como já foi dito antes, observar qual fuso horário os *logs* fazem referência, em caso de dúvidas é melhor consultar a empresa que os forneceu. Normalmente quando são empresas localizadas no Brasil, o fuso horário utilizado é o UTC -3, porém é bom lembrar que temos outros fusos horários no país e em determinadas épocas do ano utilizamos o horário de verão. No caso de informações prestadas por outros países pode acontecer de o fuso horário utilizado ser o UTC ou o fuso local, em todos os casos, na hora de formular pedidos de quebra de sigilo, deve-se deixar muito claro a qual fuso horário está se referindo.

A empresa americana *Microsoft Corporation* oferece diversos serviços na internet que são muito utilizados no Brasil como o sistema de webmail Hotmail, e o mensageiro instantâneo Messenger. Esta empresa é representada no Brasil pela Microsoft Informática Ltda. com sede em São Paulo/SP. Quando se faz necessário a requisição de informações sobre registros de conexão dos servidores da *Microsoft Corporation é* possível realizar o pedido mediante ofício da autoridade policial, sendo que o documento deverá ser direcionado para a Microsoft do Brasil. pedindo que esta solicite as informações para a empresa americana.

Algumas empresas que fornecem acesso à internet por meio da tecnologia ADSL alegam ter dificuldade de identificar o usuário de um determinado endereço IP quando ele não está conectado à rede no momento da pesquisa. A dificuldade estaria no fato de que estas empresas utilizam duas tecnologias distintas para o acesso a ATM e a *Ethernet.*

No caso em que o acesso se dá por meio de um switch ATM as informações sobre o usuário que se conectou ficariam gravadas nos *logs* e a identificação poderia ser feita sem maiores problemas. Porém, no caso em que o acesso se dá por intermédio de um *switch Ethernet* a identificação da conexão se dá por meio do MAC *address* do sistema do usuário, nesse caso, seria preciso realizar uma pesquisa na rede em busca deste identificador e para que a pesquisa tivesse sucesso uma conexão precisaria estar ocorrendo no momento.

Logo, neste caso, se o usuário trocar a máquina que está utilizando fica

mais complicado identificá-lo. Porém a empresa pode fornecer à polícia o endereço MAC utilizado na conexão e o nome que foi utilizado para *login,* este nome normalmente é o endereço de e-mail que o usuário cadastrou em seu provedor de acesso e um pedido de informações a esse provedor pode identificar o criminoso.

Por último, é importante lembrar que qualquer investigação de crimes cibernéticos não deve ficar restrita aos trabalhos técnicos, todas as técnicas de investigação utilizadas para os crimes comuns como acompanhamentos, interceptação de comunicação telefônica e vigilância devem ser utilizadas em conjunto para que haja sucesso.

3.8. Cooperação policial e judicial internacional

A responsabilidade da polícia e da Justiça é identificar os suspeitos e apresentar provas do delito que lhes foi atribuído. No entanto, a falta de recursos e pessoal especializado dificulta a investigação de responsabilidade na complexa cadeia de comunicação que se inicia na inserção de material e vai até o usuário final.

Não é de hoje que os representantes da Interpol dedicados a esses assuntos enfatizam a necessidade de policiais especializados no uso da internet. Mas isto nos leva a outro problema: nem sempre os peritos em crimes contra crianças são especialistas em informática. Em geral, não dispõem dos equipamentos necessários ao rastreamento dos infratores na internet.

No tocante ao uso da internet, existe um verdadeiro desequilíbrio entre o conhecimento dos criminosos e o da polícia. Mas felizmente, esta situação está mudando, como decorrência dos próprios acontecimentos e da pressão dos envolvidos no trabalho. Cada vez mais unidades nacionais estão sendo criadas especificamente para combater o uso criminoso da internet. Apesar da existência de unidades nacionais contra atos de criminosos, muitos infratores escapam à aplicação das mesmas devido ao cruzamento das fronteiras e à limitação territorial da competência dos membros da polícia.

À luz de tais fatos, a Interpol reconhece o papel fundamental da cooperação internacional e a importância de seu próprio empenho em definir estratégias para se agir em nível internacional. A missão básica da Interpol é facilitar e fortalecer a cooperação internacional da polícia, com o objetivo de ampliar a eficácia na luta contra o crime internacional e também contra o uso ilegal de novas tecnologias. É necessário também, priorizar o treinamento adequado dos policiais, que precisam, além disso, ser equipados com computadores de alto desempenho.

É fundamental que a indústria de computadores perceba sua responsabilidade e o papel que lhe cabe na conservação de provas dos crimes na internet. Deve, além disso, transmitir tais informações aos serviços responsáveis pela aplicação da lei. Desta forma, estarão dando uma contribuição efetiva à prevenção e

combatendo os crimes na internet. Infelizmente, os líderes da indústria de tecnologia ligada à internet ainda não se convenceram dessa responsabilidade, usando dos mais variados pretextos para não apoiar a polícia.

Para fundamentar estes argumentos com ilustrações concretas, verifica-se brevemente um caso de pornografia infantil que esteve nas manchetes dos jornais há alguns anos atrás no Brasil e que foi verificado a partir de uma notícia veiculada através do site do Jornal Folha de São Paulo e citado na obra de Flávia Gouveia[73]

> *A história começou em 2008, na cidade californiana de San José, (Estados Unidos), quando policiais americanos descobriram pedófilos filmando estupros de crianças e transmitindo-os ao vivo para os seus assinantes na internet. Os criminosos se denominavam pertencentes ao "Clube da Orquídea". Entre os assinantes, havia um homem britânico cujos detalhes foram fornecidos à polícia inglesa. Durante o interrogatório, descobriu-se que esse homem estava de posse de pornografia infantil do "Clube da Orquídea" e também por trás da criação de uma rede muito mais ampla, conhecida como "País das Maravilhas".*

O caso foi o exemplo concreto de cooperação internacional de policiais nacionais, com a assistência da Interpol. Já em junho de 2014, policiais de doze países trabalharam juntos para se atualizar mutuamente sobre todas as atividades dos membros da rede e para esmiuçar o material apreendido durante as prisões simultâneas realizadas em setembro de 2014, na qual 96 pessoas foram presas em doze países diferentes.

Somente em uma das casas vistoriadas foram confiscados 48 gigabytes de pornografia infantil. No Reino Unido, foram apreendidas aproximadamente 250.000 imagens. Nos Estados Unidos, foram encontradas 500.000 imagens e mais de 120 vídeos de pornografia infantil. A maior apreensão em lar americano rendeu 75.000 imagens. Se reunirmos todo o material apreendido nos diferentes países, chegaremos a números impressionantes, sem falar que as imagens foram copiadas muitas vezes. Isto nos mostra o sofrimento das crianças envolvidas na produção do material e o papel da internet na transmissão de pornografia infantil.

No Brasil, alguns métodos estão sendo amplamente adotados, com o acesso da Polícia Federal Brasileira ao Sistema de Monitoramento de Exploração de Crianças, ou o denominado *Child Exploitation Tracking System* - CETS, programa esse viabilizado pela Microsoft com o apoio da Polícia Federal do

[73] GOUVEIA, Flavia. *Tecnologia a serviço do crime*. Ciência e Cultura, jan/mar. 2014, vol. 59, nº 1, p.6-7. Disponível em: < http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252007000100003&lng=pt&nrm=iso>. Acesso em: 24/11/2015

Canadá para identificar e punir o maior número possível de pedófilos que atuam na rede mundial de computadores.

A Polícia Federal Brasileira já deflagrou várias operações na repressão aos crimes virtuais, denominadas como: Pagasus, Cash Net, Web Pagem Pontocom; Scam, Cavalo de Tróia, entre outras.

Entre as operações da Polícia Federal, algumas tiveram apoio e repercussão internacional, como a operação denominada Araras, que foi deflagrada juntamente com o FBI, no qual os policiais brasileiros encontraram hacker que pirateava softwares.

Outra operação de âmbito internacional ocorrido no Brasil foi à chamada Azahar (uma flor cujo chá "acalma os ânimos dos homens") que aconteceu simultaneamente em vários países no mundo, no combate à pedofilia pela rede mundial de computadores. Este foi um exemplo de trabalho de cooperação internacional entre as policias que se tornou essencial no combate aos crimes virtuais.

Finalmente, convém citar também as operações denominadas Carrossel 1 e Carrossel 2, que resultaram em mais de 500 prisões em todo o mundo.[74]

A Polícia Federal Brasileira é fundamental na investigação e combate aos crimes de fraude bancária, de divulgação de pornografia infantil e outros praticados na internet, isso sem contar que a legislação brasileira vem avançando no tocante à pornografia infantil na rede mundial de computadores, pois pune tanto a posse, como a aquisição, ou venda, da pornografia infantil e aos crimes de internet em geral.

4. CONCLUSÃO

O objetivo do presente artigo foi o de analisar o funcionamento da investigação criminal na internet para propor métodos de investigação de crimes cometidos com o uso da rede. Para isso, foram realizadas diversas pesquisas bibliográficas, a fim de analisar o uso e a importância da rede mundial no mundo e principalmente no Brasil. As pesquisas continuaram para focar no uso ilícito que criminosos estão fazendo desta rede e na responsabilidade das Polícias em reprimir a criminalidade cibernética.

Para tratar dos métodos de investigação foi necessário conhecer o funcionamento da internet relativo a aspectos técnicos e também do controle do

[74] SOBRAL, Carlos. Idealizador e Ex-Chefe do Serviço de Repressão a Crimes Cibernéticos da Polícia Federal. Disponível em < http://www.todoscontraapedofilia.com.br/site/index.php?option=com_content&view=article&id=1883:chefe-da-unidade-de-repressao-a-crimes-ciberneticos-da-policia-federal&catid=34:noticias&Itemid=28>. Acesso em: 26/11/2015.

registro de domínios e da alocação de endereços de rede. Com o resultado dessas pesquisas foi possível propor formas de buscar por via judicial informações técnicas e requisitar dados a empresas responsáveis, a fim de identificar os infratores.

O artigo trouxe de maneira sucinta alguns métodos a serem utilizados na busca de informações que possam ajudar na comprovação da autoria e materialidade de crimes cibernéticos. Os registros relativos a conexões aos servidores da internet contêm dados que podem identificar com exatidão a origem de qualquer transação. Outras fontes de informação importantes são os cabeçalhos de mensagens de e-mail, a consulta a ferramentas de *whois* e a servidores DNS.

Foi demonstrado que os policiais encarregados de investigar crimes que utilizam a internet necessitam de treinamento eficaz e contínuo, pois a evolução da rede é constante e, além do mais, a criatividade e o conhecimento de pessoas que se dedicam a pesquisar falhas de segurança, métodos para invadir sistemas, tornar-se anônimo e causar prejuízos aos usuários da rede são enormes.

Por intermédio de uma legislação adequada, do comprometimento de todos os países do globo e da eficiência dos órgãos encarregados de combate ao crime é que se pode coibir a ação de criminosos na grande rede mundial de computadores.

No entanto, para que isso ocorra, tais investigações devem acontecer de forma rápida e até mesmo simultaneamente aos crimes praticados, pois se trata de alta tecnologia que pode rapidamente afetar as pessoas em muitos países, e o mais preocupante é que as provas desses crimes podem ser rapidamente alteradas ou destruídas, o que dificultaria qualquer investigação.

Reconhecer que os crimes em questão podem ser localizados em qualquer parte do mundo, e tendo em conta os princípios relativos à soberania e à proteção dos direitos humanos, democráticos, liberdades e privacidade, as autoridades policiais devem, na realização de investigações criminais, em certas circunstâncias, serem capazes de prosseguir as investigações para além das fronteiras territoriais.

Em suma, o pequeno estudo abordado neste artigo visa fomentar a discussão e a repressão ao cibercrime até mesmo porque, é sabido que para combater algo é necessário conhecer, ainda que da maneira concisa, como a que aqui se fez presente.

Enfim, o objetivo deste artigo não tem nenhuma intenção de promover qualquer defesa irrestrita e sem métodos de investigação criminal no combate aos crimes cibernéticos, mas, sim, gerar uma discussão sobre o tema, para que sejam pesados os prós e contras de sua aplicação, com o escopo de proporcionar formas de se atingir o maior objetivo do Estado, no âmbito criminal, a Justiça.

REFERÊNCIAS

BECHARA, M. Os espaços públicos de acesso à Internet. in: COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa Sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil TIC DOMICÍLIOS E TIC EMPRESAS 2012. São Paulo: Comitê Gestor da Internet no Brasil, 2013. p. 47-50.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Disponível em

<http://www.planalto.gov.br/ccivil03/constituicao/constituiçao.html>.

Acesso em 28/11/2015.

BRASIL. Lei 7.716 de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça e de cor. Publicado no D.O.U de 6.1.1989. Disponível em <http://www.planalto.gov.br/ccivil 03/Leis/L7716.htm>. Acesso em 22/11/2015.

BRASIL. Estatuto da Criança e do Adolescente. Lei 8.069 de 13 de julho de 1990. Publicado no D.O.U. 16.7.1990. Disponível em <http://www.planalto.gov.br/ccivil 03/Leis/L8069.htm>. Acesso em 23/11/2015.

BRASIL. Decreto 99.710 de 21 de novembro de 1990b. Promulga a Convenção sobre os Direitos da Criança. Publicado no DOU de 22.11.1990. Disponível em <http://www.planalto.gov.br/ccivil 03/decreto/1990-1994/D99710.htm>. Acesso em 18/11/2015.

BRASIL. Lei 9.609 de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no país e dá outras providências. Publicado no D.O.U. de 20.2.1998 e retificado no D.O.U. de 25.2.1998. Disponível em <http://www.planalto.gov.br/ccivil 03/Leis/L9609.htm>. Acesso em 18/11/2015.

BRASIL. Lei 10.446 de 08 de maio de 2002. Dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para os fins do disposto no inciso I do § 1º do Art. 144 da Constituição. Publicado no D.O.U. de 9.5.2002. Disponível em <http://www.planalto.gov.br/ccivil 03/Leis/2002/L10446.htm> Acesso em 28/11/2015.

BRASIL. Decreto n° 4.829 de 3 de setembro de 2003. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil e dá outras providências. Publicado no D.O.U. de 04/09/2003, Seção I, pág. 24. Disponível em http://www.cgi.br/regulamentacao/decr4829.htm

Acesso em 23/11/2015.

BRASIL, Comitê Gestor da Internet no Brasil. Resolução 0001/2005a. Dispõe sobre a execução do registro de Nomes de Domínio, a alocação de Endereços

IP (Internet Protocol) e a administração relativa ao Domínio de Primeiro Nível, atribuídas ao Núcleo de Informação e Coordenação do Ponto BR - NIC br e dá outras providências. Publicada nos jornais O Estado de São Paulo, Folha de São Paulo e O Globo, no dia 05 de dezembro de 2005 e no D.O.U. de 14 fev. 2006, seção 1, página 17. Disponível em:

http://www.cgi.br/regulamentacao/resolucao2005-01.htm Acesso em 17/11/2015.

BRENNER, Susan W. & KOOPS Bert-Jaap, "*Approaches to Cybercrime Jurisdiction*", tradução *Abordagens para descobrir a Jurisdição dos Cybercrimes*. Cite as: 4 J. High Tech. L.1 (2014). Copyright © 2014 Journal of High Technology Law. All Rights Reserved. ISSN 1536-7983.

CAMPELLO, R. S. et al. Informática Forense. Brasília: Academia Nacional de Polícia, 2013. 22 p. : il.

COMER, D. E. Redes de computadores e Internet. 4. ed. Porto Alegre: Bookman, 2012.

COMITÊ GESTOR DA INTERNET NO BRASIL. Cartilha de Segurança para Internet, Versão 3.1/CERT br. São Paulo: Comitê Gestor da Internet no Brasil, 2014.

COMITÊ GESTOR DA INTERNET NO BRASIL. Manual Prático de Investigação de Crimes Cibernéticos. São Paulo: Comitê Gestor da Internet no Brasil, 2014. Não paginado.

COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa Sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil TIC DOMICÍLIOS E TIC EMPRESAS 2013. São Paulo: Comitê Gestor da Internet no Brasil, 2014.

DELLA VALLE, J.; ULBRICH, H. C. Universidade Hacker. 3. ed. São Paulo: Editora Digerati, 2013.

FARIA, A. O. TOR: A Internet sem rastreabilidade. 30 de setembro de 2015. Disponível em <http://www.vivaolinux.com.br/artigo/TOR-A-Internet-sem-rastreabilidade>. Acesso em 15/11/2015.

FILHO, A. L. K.; SOUZA, V. G. L. Polícia Criminal Internacional. Brasília: Academia Nacional de Polícia, 2014. 47 p. : il.

GOUVEIA, Flavia. *Tecnologia a serviço do crime*. Ciência e Cultura, jan/mar. 2014, vol. 59, nº 1, p.6-7. Disponível em:

<http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252007000100003&lng=pt&nrm=iso>. Acesso em: 24/11/2015.

ICANN. Bem vindo a ICANN!. 14 ago. 2014. Disponível em <http://www.icann.org.br/new.html>. Acesso em ICANN. FAQs. Disponível em <http://www.icann.org.br/faq/#top>. Acesso em 15/11/2015.

LACNIC - Registro de Endereçamento de Internet para América Latina e Caribe. Estatísticas de Alocações do LACNIC. Disponível em

<http://www.lacnic.net/pt/est.html>. Acesso em 27/11/2015.

MORENO, A. C. O espaço livre da pornografia infantil no Brasil. 25/05/2013. Disponível em:

http://www.safernet.org.br/twiki/bin/view/SaferNet/Noticia20060525014926>.,Acesso em 15/11/2015.

MORIMOTO, C.E. Faixas de Endereços IP, CIDR e Máscara de Tamanho Variável - Tutorial. 17/04/2013. Disponível em <http://www.guiadohardware.net/tutoriais/endereco-ip-cidr/. Acesso em 25/11/2015.

NOVO MILÊNIO. Jornal Eletrônico. Fusos Horários e Códigos (time zones & codes). Disponível em

<http://www.novomilenio.inf.br/porto/mapas/nmfusos.htm>. Acesso em 23/11/2015.

RODRIGUES, G. Lucro Faz Cibercrime se Estabelecer Mundialmente. 21/03/2014. Disponível em:

<http://www.infoguerra.com.hr/infonews/viewnews.cgi?newsid1142964693,29218>. Acesso em 23/11/2015.

SAFERNET - Glossário da Internet. Disponível em

<http://www.safernet.org.br/site/prevencao/glossarios/internet>. Acesso em 17/11/2015.

SILVA, R. C. L. Direito penal e sistema informático. São Paulo: Editora Revista dos Tribunais, 2013.

SOBRAL, Carlos. Idealizador e Ex-Chefe do Serviço de Repressão a Crimes Cibernéticos da Polícia Federal. Disponível em <http://www.todoscontraapedofilia.com.br/site/index.php?option=com_content&view=article&id=1883:ch efe-da-unidade-de-repressao-a-crimes-ciberneticos-da-policia-federal&catid=34:noticias&Itemid=28>. Acesso em: 26/11/2015.

SUDRE, Gilberto - Navegando de Forma Anônima. 10/04/2014. Disponível em http://www.imasters.com.br/artigo/3935. Acesso em 17/11/2015.

TANEMBAUM, A. S. Redes de Computadores. 4. ed. São Paulo: Editora Campus, 2013.

TEIXEIRA, R. C. Combatendo o Spam. São Paulo: Novatec Editora, 2014.

TORRENTE, Diogo. Conferencia *AEEC: en busca de una definición para Prueba Electrónica*. CYBEX. e-newsletter. Pruebas electrónicas y Computer Forensics. Abril, 2014, nº 26.

Capítulo VI

"STALKING"

José Navas Junior[75]

O termo "STALKING" tem sua origem incerta, embora muitas são as teorias acerca de sua gênese, de ordem jurídica ou mesmo oriunda do cinema, o que importa, na verdade, é entendermos o alcance deste "delito", que pode ser autônomo (embora nem sempre bem delineado) ou agregado como elemento potencializador de outro crime diverso.

Vamos começar definindo o termo e, por conseguinte, o esboço de definição do próprio crime, que ainda carece de capitulação específica no ordenamento pátrio.

O "STALKING" deriva do termo "stalk", que numa tradução livre seria algo como "perseguição furtiva", embora seja traduzido em adaptação livre para "ato de perseguir alguém, de forma continuada e reiterada, ameaçando sua integridade física e psicológica, com restrição à liberdade de locomoção ou invasão à liberdade ou privacidade de outra pessoa."

Tal definição foi contemplada em projetos normativos a criminalizar em específico o delito afeito, no qual foi sugerida a prisão de dois a seis anos.

Importante ressaltar que a definição pré-normativa proposta para "STALKING" abarca tanto o mundo "real" como o "cyber" para efeitos de local de crime.

Necessário ainda entendermos os tipos de "STALKING" classificados ao longo dos países onde tal prática já vem sendo tratada com rigor legislativo e jurídico afeito. Neste quesito, podemos classificar a prática delitiva como segue.

- ✓ Stalkers rejeitados - perseguem suas vítimas, a fim de reverter, corrigir ou vingar uma rejeição (por exemplo, divórcio, separação, rescisão).
- ✓ Stalkers ressentidos - desejam prosseguir em uma "vingança" por causa de um sentimento de injustiça contra as vítimas - motivada principalmente pelo desejo de assustar e levar angústia à vítima.
- ✓ Stalkers candidatos - procuram estabelecer um relacionamento amoroso

[75] O autor é Delegado de Polícia Federal, Especialista no combate ao Crime Cibernético e trabalha na Delegacia de Policiai Federal de Marília no estado de São Paulo.

íntimo com sua vítima. Tais "stalkers" muitas vezes acreditam que a vítima é uma muito procurada "alma gêmea", e eles foram, assim, feitos para estar juntos.

- ✓ Stalkers pretendentes incompetentes - apesar das pobres habilidades sociais ou cortejo, tem uma fixação, ou em alguns casos, um senso de direito para uma relação íntima com aqueles que tenha lhes atraído o interesse amoroso. Suas vítimas são, na maioria das vezes, pessoas já em um relacionamento amoroso com outra pessoa.
- ✓ Stalkers predatórios - sua missão é espionar a vítima, a fim de preparar e planejar um ataque, muitas vezes sexual

Começa a se desenhar uma derradeira categoria de "stalkers", misto do ressentido com o rejeitado, e com apelo sexual apurado, qual seja, o "stalker revenge porn", aquele que se vinga de sua vítima a partir de obtenção (direta ou por terceiros) de fotos íntimas desta e as divulga em redes sociais para o público em geral, como forma de manifestar seu ressentimento e se vingar desta, de forma peremptória.

Esta última modalidade é particularmente devastadora, transcendendo a seara penal convencional, levando não raramente a vítima a consequências psicológicas devastadoras, culminando em situações extremas como o suicídio.

Mas afinal, como classificar penalmente a prática do "STALKING"? Vamos começar pela análise da legislação comparada, mais avançada no tema em relação ao Brasil, onde, já adiantamos, sequer há ainda o normativo específico à prática.

Embora o tema careça de previsão legislativa no Brasil, já em 1990, em Los Angeles, Califórnia (Estados Unidos), um "stalker" chamado Robert Bardo foi condenado sob descrição normativa da "perseguição insidiosa" e "assassinato à espreita", após ter sistematicamente seguido por 3 anos a jovem atriz Rebecca Shaefer, tendo assassinado esta na sequência, a tiros, em 1989.

O caso afeito gerou uma das primeiras leis anti-stalking que se tem notícia, no caso, uma legislação penal estadual (o sistema norte-americano comporta tal segmentação) com inúmeros mecanismos de proteção e prevenção à vítima, como a que impede que o Departamento de Transito da Califórnia fornecesse o endereço de proprietários de automóveis para qualquer cidadão (a época a informação era pública), pois foi desta maneira que Bardo soube o endereço residencial da vítima.

Na Austrália, a partir de 1990, sob reflexo do ocorrido nos EUA, os estados deram início a normatização do delito afeito, a começar com proibição genérica de se praticar o "STALKING", sendo o estado de Queensland o primeiro a lançar um conjunto normativo penal exauriente sobre o tema, em 1994.

No Canadá há uma sessão específica sobre o tema (section 264) no "Criminal Code", com previsão expressa ao termo "stalking", ganhando força o normativo

em meados da década de 90, com uma nova legislação de proteção às mulheres, inserindo-se o "stalking" como forma insidiosa de crime.

Na Europa, foi a França um dos primeiros países a criminalizar a perseguição furtiva/insidiosa, em 2002, em seu Código Penal.

Ainda na Europa, merece menção a Suíça, que embora preveja expressamente a prática, exarada em um "normativo anti-stalking" (de 2007), não trata esta como crime em si, tampouco de forma autônoma, devendo ser associada a alguma prática criminosa diversa para se configurar, como por exemplo, a violência física ou psicológica derivada, sendo a última de difícil aferição prática. Doutrinariamente, inclusive, a previsão suíça tem contornos de direito civil, com pouco ou nenhum reflexo penal ao delito autônomo, ainda que tenha estreita correlação com este.

Em 2013, assolada por casos de violência sexual em transporte público e vias locais, a Índia passou a criminalizar o "STALKING" como prática autônoma.

O caso mais emblemático no entanto, e exitoso, veio do Reino Unido, que juntou uma série de organizações de prevenção e combate ao "STALKING", como a "Rede de Sobrevivência ao Stalking", e criou uma linha de contato por telefone e via internet ao serviço STALKING HELP LINE, onde é possível denunciar as práticas afeitas a qualquer hora do dia ou da noite, havendo impecável pronta resposta dos órgãos de segurança pública afeitos, com o treinamento devido a tratar não apenas do crime e do criminoso, mas também da vítima.

A iniciativa britânica está sendo portada para diversos países, em especial da "anglosfera", com rápida adaptação dos sites e sinergia nos sistemas jurídicos derivados da raiz comum britânica.

O cenário, no entanto, fica obscuro quando retornamos ao Brasil, e passamos a nos socorrer da legislação pátria.

A prática afeita começou a ser classificada, por absoluta falta de previsão legal ou entendimento do desdobramento potencial, como a CONTRAVENÇÃO do Art. 65, que prevê:

> ***Art. 65***. *Molestar alguém ou perturbar-lhe a tranquilidade, por acinte ou por motivo reprovável:*
> *Pena - prisão simples, de quinze dias a dois meses, ou multa, de duzentos mil réis a dois contos de réis.*

Como se observa, não apenas pela natureza do delito (contravenção), mas a partir da pena prevista, tratar-se-ia de um delito de menor potencial ofensivo, não apto sequer à constrição de liberdade do perpetrador, que, sob "risco calculado" na certeza de sua pseudo-impunidade (pois branda a penalização), se enveredava pela perseguição à vítima.

A necessidade de se evoluir doutrinariamente, a dar uma resposta ao

problema que se alastrava em progressão geométrica, perante a inércia ou morosidade legislativa pátria (o ciclo de renovação de leis é burocrático e custoso em tempo), levou à manobra que fez com que a prática do "STALKING" passasse a ser caracterizada como AMEAÇA, aos moldes do Art. 147 do Código Penal, que prevê assim:

> ***Ameaça***
> ***Art. 147*** *- Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:*
> *Pena - detenção, de um a seis meses, ou multa.*
> *Parágrafo único - Somente se procede mediante representação.*

Um ganho incipiente na aplicação efetiva do direito material, ainda mantendo o delito no campo dos afeitos ao menor potencial ofensivo, e ainda gerando um efeito colateral indesejado e sabe-se lá se previsto, qual seja, o elemento subjetivo do tipo, ou seja, tratando-se de crime doloso, exige-se a vontade de ameaçar acompanhada da intenção injusta de intimidar, pois a mera bravata não configura a ameaça. A perseguição insidiosa sem a vontade de ameaçar por parte do perpetrador, ou a percepção de que está sendo ameaçada, pela vítima, em si dificulta a própria subordinação penal ao tipo em questão. E mais, sendo a ameaça no sentido de se fazer com que a vítima tenha um outro comportamento, estaremos diante do crime de constrangimento ilegal, diverso.

Mesmo a proposta de reforma do tipo afeito é tímida, quando confrontada com o disposto em legislação comparada. Esta se propõe a inserir no Art. 147 um parágrafo extra, com os dizeres:

> *§ 1º. Perseguir alguém, de forma reiterada ou continuada, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.*
> *Pena -Prisão, de dois a seis anos, e multa.*

Seria assim o "STALKING" uma mera forma qualificada de AMEAÇA, mas ainda mantendo com esta última a estreita correlação quanto a elemento subjetivo do tipo que originariamente não faz parte do "STALKING" em sua doutrinária definição, passando a exigir o sentimento de "ameaça" dentro da "perseguição insidiosa", sendo que de per si, apenas a perseguição em si já deveria bastar-se a caracterizar o delito afeito.

Um tratamento simplista, um "remendo legislativo" que não faz jus a dimensão do problema no qual estamos defronte.

Muitos doutrinadores e operadores do direito ainda se desdobram na subordinação típica do "STALKING" em normativos ligados a delitos menores,

como na Lei de Contravenções Penais, enquadrando, não raramente, o "STALKING", como:

> *"**Art. 42**. Perturbar alguém, o trabalho ou o sossego alheios: (...)*
> *Pena - prisão simples, de quinze dias a três meses, ou multa (...).*
> ***Art. 61.** Importunar alguém, em lugar público ou acessível ao público, de modo ofensivo ao pudor:*
> *Pena - multa (...).*
> ***Art. 21**. Praticar vias de fato contra alguém:*
> *Pena - prisão simples, de quinze dias a três meses, ou multa (...)."*

Menos claudicante, mas ainda não definitiva, é a previsão para o crime autônomo prevista no Projeto do novo Código Penal, que prevê em um de seus artigos: "Perseguição OBSESSIVA de uma outra pessoa ameaçando sua integridade física ou psicológica ou ainda invadindo ou perturbando sua privacidade".

Construída assim a definição, de modo a permitir a criminalização pela invasão ou perturbação à privacidade da vítima, mantendo a ameaça em parte de sua definição, ao caso específico de intento de violação física ou psicológica, no entanto críticas já foram lançadas ao dispositivo afeito na medida em, verborrágica como de praxe em nossa legislação, previu ainda a obsessividade como elemento do tipo, o que nos remete a "reiteração", já que não seria, em tese, possível aferir obsessividade com apenas UMA perseguição insidiosa.

Para muitos estudiosos do tema, tal previsão (obsessiva) teria maculado de tal forma o instituto normativo e inviabilizar sua aplicação, não sendo possível, no caso prático, aferir a reiteração persecutória, sob o manto da busca da verdade real e comprovada, e mesmo sendo possível, estaríamos defronte a uma espécie de "ação controlada", onde a vítima, percebendo ser alvo de perseguição insidiosa, comunica a polícia, que passaria a gravar a movimentação do autor, até que, seguindo-se a uma construção doutrinária, após um certo número de "perseguições", ou dias, ou horas efetivamente comprovadas, estaríamos diante do conceito consagrado como "obsessiva"

Como se vê, num lúdico exercício prático, percebe-se que a grande maioria dos delinquentes irá se safar da aplicação da lei penal, vingando tal dispositivo na reforma afeita, argumentando simplesmente que não estava perseguindo obsessivamente a vítima, apenas "uma ou duas vezes".

Em uma análise mais apurada, podemos notar que, embora não exista em específico o tipo penal afeito ao "STALKING" em nosso ordenamento, este aparece de forma tímida inserido em outras leis decorrentes, inclusive com medidas protetivas típicas a fazer cessar a perseguição insidiosa.

É o caso, por exemplo, da Lei 11.340, a chamada "Lei Maria da Penha", que em seu Art. 22 assim prevê:

> ***Art. 22**. Constatada a prática de violência doméstica e familiar contra a*

mulher, nos termos desta lei, o juiz poderá aplicar, de imediato, ao agressor, em conjunto ou separadamente, as seguintes medidas protetivas de urgência, entre outras:
I - suspensão da posse ou restrição do porte de armas, com comunicação ao órgão competente, nos termos da Lei nº 10.826, de 22 de dezembro de 2003;
II - afastamento do lar, domicílio ou local de convivência com a ofendida;
III - proibição de determinadas condutas, entre as quais:
a) aproximação da ofendida, de seus familiares e das testemunhas, fixando o limite mínimo de distância entre estes e o agressor;
b) contato com a ofendida, seus familiares e testemunhas por qualquer meio de comunicação;
c) frequentação de determinados lugares, a fim de preservar a integridade física e psicológica da ofendida;
IV - restrição ou suspensão de visitas aos dependentes menores, ouvida a equipe de atendimento multidisciplinar ou serviço similar;
V - prestação de alimentos provisionais ou provisórios.
§ 1º As medidas referidas neste artigo não impedem a aplicação de outras previstas na legislação em vigor, sempre que a segurança da ofendida ou as circunstâncias o exigirem, devendo a providência ser comunicada ao Ministério Público.
§ 2º Na hipótese de aplicação do inciso I, encontrando-se o agressor nas condições mencionadas no caput e incisos do Art. 6º da Lei nº 10.826, de 22 de dezembro de 2003, o juiz comunicará ao respectivo órgão, corporação ou instituição as medidas protetivas de urgência concedidas e determinará a restrição do porte de armas, ficando o superior imediato do agressor responsável pelo cumprimento da determinação judicial, sob pena de incorrer nos crimes de prevaricação ou de desobediência, conforme o caso.
§ 3º Para garantir a efetividade das medidas protetivas de urgência, poderá o juiz requisitar, a qualquer momento, auxílio da força policial.

As medidas relacionadas na legislação acima mencionada poderiam ser portadas sob poucas ou nenhuma adaptação a formar um conjunto normativo autônomo para o crime de "STALKING", pois efetivas para tanto. Estão, no entanto, circunscritas aos crimes derivados da relação estabelecida na introdução da lei em questão, não se aplicando, por exemplo, entre perseguidor e vítima, sem relação estabelecida (ou até mesmo desconhecidos).

A crítica que se faz ao ordenamento pátrio é no sentido de que, em um esforço jurídico hercúleo, seriamos levados a concluir que, embora possamos montar, de forma "caseira", uma doutrina a abarcar determinadas condutas em tese afeitas ao "STALKING", ainda assim teríamos apenas instrumentos de

repressão (triscando a absolutamente vedada "*analogia in malam partem*"), sem que no entanto tenhamos, por mais esforço feito, as medidas de prevenção, tão ou mais úteis até quando se trata do tema afeito.

Enquanto engatinhamos no Brasil acerca até mesmo da definição do termo, a nos enveredarmos a normatizar penalmente a conduta, observa-se em outras nações, 20 a 30 anos à frente no assunto, movimento voltado à absorção do "STALKING" ou a análise sinérgica deste com outra forma de delito também legalmente obscuro por aqui, qual seja, o "BULLYING", definido assim como o conjunto de atos de violência física ou psicológica intencionais e repetidos, praticados por um indivíduo ou grupo de indivíduos, causando dor e angústia e sendo executadas dentro de uma relação desigual de poder.

Não é nosso tema foco nesta obra, mesmo porque merecedora de capítulo dedicado (ou talvez uma obra toda), mas o "BULLYING" vem sendo observado como fenômeno derivado do "STALKING obsessivo", sendo este último fase de persecução do primeiro.

Sendo um fenômeno mundial e potencializado pela internet, questão de segurança e saúde pública, tanto STALKING quanto BULLYING ganharam destaques nos últimos tempos, a ponto de serem monitorados por meio de coleta e compartilhamento de dados, sob preceitos legais, junto a centros de pesquisa civis em todo o mundo, com profissionais aptos até mesmo a prever as ações delitivas, com base em análise comportamental, seja da observação de padrões em câmeras de monitoramento em vias públicas, ou pela vigilância em redes sociais.

O tema é polêmico, não apenas no tocante à manutenção dos preceitos ligados à privacidade do cidadão, e o custo benefício, inclusive jurídico, de se forçar uma releitura do próprio "Contrato Social" a afastar-se um pouco mais as garantias e direitos individuais em prol da tutela estatal, como forma de devolver ao indivíduo uma pretensa melhor prestação de serviço, prevendo o delito por observação massiva da vida social.

No Brasil a questão é operacionalmente embrionária, na medida em que, décadas atrás, os países mais desenvolvidos no tema passaram a gestão de tais incidentes a centros de pesquisa derivados da sociedade civil, com foco na segurança pública e saúde, enquanto que aqui mantemos como "instituição oficial" de tratamento de incidentes cibernéticos um órgão militar, o CDCiber, que não obstante a sabida competência de seus idealizadores e membros, não tem como escopo o processamento de delitos que afetam ao indivíduo, ainda mais com tamanha carta de subjetividade, focando em incidentes afeitos à segurança nacional ou de trato difuso/coletivo, conforme previsto em sua missão institucional, e não poderia ser diferente, tratando-se de uma instituição de defesa militar.

Almeja-se assim, com urgência, a criação de um novo órgão de análise de incidentes no ciberespaço que tenha efetivamente aspiração a prevenção de

delitos que afetam ao internauta como indivíduo, não apenas na visão macro ao qual se insere, tanto para repressão quanto para prevenção destes, que trate de SEGURANÇA CIBERNÉTICA, não apenas de DEFESA CIBERNÉTICA, a abarcar instituições e setores testados e aprovados ao longo dos "Grandes Eventos" (Copa do Mundo e Olimpíadas), como o Comitê Gestor de Internet Brasil (por meio do CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), a Polícia Federal (por meio do Setor de Repressão a Crimes Cibernéticos - SRCC), membros do próprio CDCiber, Conselhos de Justiça e Ministério Público, bem como representação da OAB. O que se propõe, assim, é um verdadeiro CENTRO DE COMANDO E CONTROLE, a estar pronto a reagir aos incidentes, em especial no ciberespaço, que se prevenidos, obstam a consumação de delitos endêmicos como "STALKING" e "BULLYING", que tem um "iter criminis" bem definido, quase biometricamente padronizado, e portanto podem assim ser expurgados antes de seu curso completo.

Capítulo VII

Ciberameaças e o registro de controle da produção e do estoque - bloco k do sped fiscal.

Coriolano Aurélio de Almeida Camargo Santos[76]

1. INTRODUÇÃO

O presente artigo vem tratar dos potenciais riscos envolvendo a informação fiscal como ativo do cibercrime. O controle fiscal eletrônico e o acesso a informações sigilosas do contribuinte trazem à tona um novo cenário. Os momentos de reflexão aqui propostos são decorrentes da experiência do autor no exercício da advocacia, na análise de cibercrimes, no estudo de pesquisas de campo para elaboração de palestras, bem como, pela participação em trabalho colaborativo proposto no ano de 2.005, frente a Diretoria da Polícia Federal, que culminou em um trabalho de excelência a toda a sociedade. Em prol do aprimoramento da segurança do projeto da Nota Fiscal Eletrônica, foi sugerida, como espinha dorsal, uma aliança fazendária entre a Administração dos Negócios Fazendários dos Estados e o Instituto Nacional de Criminalística da Polícia Federal - INC. Nesse diapasão, cabe à Receita Federal uma maior interligação com outros órgãos cujas informações ou processos estejam inter-relacionados com os da Administração Tributária.

Por fim, cabe registrar no corpo do texto, recomendação da assinatura de um importante Convênio de cooperação entre as Secretarias de Fazenda e Receita Federal com o órgão de criminalística da Polícia Federal. Desta forma, poderia

---

[76] ***Coriolano Aurélio de Almeida Camargo Santos*** *Advogado. CEO da Almeida Camargo Advogados Associados. Mestre em Direito na Sociedade da Informação com Certificado Internacional pela Caldell Community College and Technical Institute. Doutor em Direito é o Coordenador Nacional do Programa Nacional de Direito Digital da Faculdade Damásio. Conselheiro Estadual da Ordem dos Advogados do Brasil Seção de São Paulo. Juiz do Tribunal de Impostos e Taxas do Estado de São Paulo. Vice Presidente no Brasil da International High Technology Crime Investigation Association (HTCIA). Integra o Conselho Superior de Assuntos Jurídicos e Legislativos da FIESP. Presidente da Comissão de Direito Eletrônico e Crimes de Alta Tecnologia da OAB/SP. Coordenador do Grupo de Direito Digital do Departamento Jurídico da Federação das Indústrias do Estado de São Paulo.*

ser realizado um redesenho do Projeto da Nota Fiscal Eletrônica, SPED e suas vertentes com foco em integrar ações voltadas a métodos preventivos contra a fraude eletrônica.

É antiga a preocupação do contribuinte, em todo o Brasil, no tocante ao vazamento de suas informações fiscais. Em 2015, o cidadão brasileiro se viu exposto pelo site "tudo sobre todos". O portal foi alvo de uma ação do Ministério Público Federal, por meio da qual foi requerido o bloqueio do acesso em território nacional, sob a alegação de que o mesmo seria ilícito, haja vista violar a privacidade dos titulares dos respectivos dados. Insta destacar que ainda não existe uma lei nacional que defina se dados públicos de acesso irrestrito podem circular livremente, mesmo quando ausente o consentimento dos seus titulares[77].

Nesse ínterim, encontra-se o chamado Bloco K do SPED Fiscal, que é a versão digital do livro "Registro de Controle da Produção e do Estoque - modelo 3 (figura abaixo indicada), destinado à escrituração dos documentos fiscais e dos documentos de uso interno do estabelecimento acerca das entradas e saídas de produtos e insumos, produção e quantidades referentes aos estoques de mercadorias, matéria-prima, embalagens, produto final e percentual de perdas apurado, conforme previsto no parágrafo 1º, do artigo 67 da Lei nº 6.374/1989, em consonância com o Convênio s/nº de 15/12/1970 e com o parágrafo 7º, da Cláusula 3ª do Ajuste SINIEF nº 2/2009, com redação dada pelo Ajuste SINIEF nº 17/2014.

Trata-se de uma medida obrigatória aos estabelecimentos industriais, aos estabelecimentos equiparados a industriais pela legislação do Imposto sobre Produtos Industrializados - IPI e estabelecimentos atacadistas, podendo, a critério do Fisco, também ficarem obrigados estabelecimentos de outros setores (Cláusula 3ª, parágrafo 7º do Ajuste SINIEF nº 2/2009).

Cumpre salientar que, atendendo a solicitações dos diversos setores e, após trabalho conjunto da Federação das Indústrias do Estado de São Paulo - FIESP e da Confederação Nacional da Indústria - CNI, por meio do Ajuste SINIEF nº 17/2014 e do Ajuste SINIEF nº 8/2015, o prazo de obrigatoriedade do Bloco K foi prorrogado, de 01/01/2015 para 01/01/2016, dentro de um cronograma de implantação, o qual tem sido postergado por parte das autoridades competentes. O novo prazo para entrada em vigor passa a ser janeiro de 2017.

Destaca-se que as informações técnicas a serem prestadas são sensíveis, vez que os dados passíveis de registro são: Produto, Unidade, Classificação Fiscal, Documentos Fiscal ou equivalente, Lançamento, Produção no Estabelecimento Próprio, Produção em Outro Estabelecimento, Valor, IPI Creditado, Saídas, IPI Devido e Estoque. (RICMS/SP, artigos 213, inciso V, 216 e 217).

Não são escriturados produtos intermediários, material de uso ou consumo,

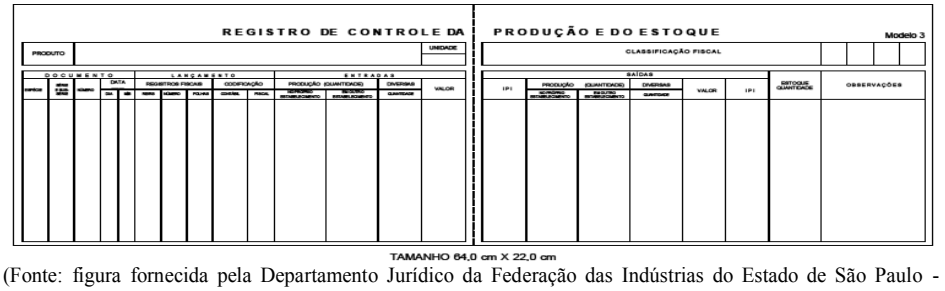
[77] Justiça Federal do Rio Grande do Norte. Decisão Liminar. Caso Tudo Sobre Todos. Disponível em: <http://www.Internetlab.org.br/wp-content/uploads/2015/08/tudo-sobre-todos.pdf> Acesso em 07 janeiro 2016.

bens destinados ao ativo imobilizado e serviços. Os registros correspondem aos dados das Fichas Técnicas dos produtos, das perdas ocorridas no processo produtivo, das Ordens de Produção, dos insumos consumidos e da quantidade produzida, inclusive, as industrializações efetuadas em terceiros. Em suma, o bloco é organizado da seguinte forma:

- Abertura do Bloco K (K001)
- Período de Apuração do ICMS/IPI (K100)
- Estoque Escriturado (K 200)
- Outras Movimentações Internas entre Mercadorias (K220)
- Itens Produzidos (K230)
- Insumos Consumidos (K 235)
- Industrialização Efetuada por Terceiros - Itens Produzidos (K250)
- Industrialização em Terceiros - Insumos Consumidos (K255)
- Encerramento do Bloco K (K990)

Hoje, os lançamentos são feitos operação a operação, com utilização de uma folha para cada espécie, marca, tipo e modelo da mercadoria. O Regulamento do ICMS Paulista prevê o seguinte modelo de livro:

REGISTRO DE CONTROLE DA PRODUÇÃO E DO ESTOQUE - Modelo 3
(a que se referem o inciso V e o § 1º do artigo 213)



TAMANHO 64,0 cm X 22,0 cm

(Fonte: figura fornecida pela Departamento Jurídico da Federação das Indústrias do Estado de São Paulo - FIESP)

Havendo produção e/ou consumo nos Registros K230 (Itens produzidos), K235 (Insumos consumidos) e K250 (Industrialização efetuada por terceiros - Itens produzidos), K255 (Industrialização efetuada por terceiros - Insumos consumidos) o Registro 0210 (Consumo específico padronizado) deverá ser apresentado.

Vis a vis, o Registro 0220 (Fatores de Conversão de Unidades) visa informar os fatores de conversão dos itens discriminados na Tabela de Identificação do Item (Produtos e Serviços) entre a unidade informada no registro 0200 e as unidades informadas nos registros dos documentos fiscais ou nos registros do controle da produção e do estoque.

Neste registro, deve ser informado o consumo específico padronizado e a

perda normal percentual de um insumo/componente para se produzir uma unidade de produto resultante, segundo as técnicas de produção de sua atividade, referentes aos produtos que foram fabricados pelo próprio estabelecimento ou por terceiro.

O estoque escriturado (K200) é calculado pelos apontamentos de entrada/produção/consumo/saída e tem periodicidade mensal. Já o estoque inventariado (Bloco H - Registro H010) deverá ser gerado sempre que a legislação obrigar a efetuar o levantamento físico das mercadorias, insumos e produtos, à época do balanço patrimonial. Portanto, esses estoques têm origem, obrigatoriedade e periodicidade diferentes.

2. PROBLEMAS APONTADOS

Diante do quadro apresentado acima concernente à comparação entre o funcionamento atual do Registro de Controle da Produção e do Estoque em face do Bloco K, o qual consiste no livro digital deste registro, cumpre destacar alguns problemas para sua implementação e efetividade. Veja:

- Necessidade de mais investimentos internos, por parte das empresas, em segurança da informação em meio a um cenário econômico extremamente desfavorável. É imprescindível o investimento em cibersegurança e em sistemas defensivos, uma vez que, anteriormente, determinadas informações, como segredos industriais, não circulavam pela internet, conforme será minuciado em tópico específico;
- A escrituração e envio de dados que vinculam os insumos consumidos ao produto acabado difere da sistemática exigida pelo modelo atualmente aprovado para escrituração em documento físico (modelo 3) - ou seja, não são informados os insumos separados por produtos, mas sim de forma geral, e este novo formado, em tese, desvirtuaria o Decreto nº 6.022/2007, que instituiu o SPED, porque a implantação do sistema não visa a criação de novas obrigações acessórias em formato eletrônico, apenas a emissão neste formato dos livros e documentos contábeis e fiscais já existentes;
- O Guia Prático, em vigor (Guia Prático EFD-ICMS/IPI - Versão 2.0.14), é insuficiente em suas instruções, porque não contempla todas as particularidades dos diversos setores produtivos;
- A rubrica 0210 (insumos, componentes e perdas percentuais) da EFD pode expor fórmulas de produtos das indústrias, muitas vezes, verdadeiros segredos industriais, os quais passariam a ser compilados e a circular por mais de um setor da empresa para cumprimento da obrigação eletrônica, além de expor a margem de lucro dos contribuintes. Ademais,

as empresas alegam que este registro tem efetividade questionável por não refletir a produção real. Dados que antes estavam separados, agoram devem ser reunidos e terão que trafegar pela internet;

- O Registro 0210, pautado em forma padronizada de produção, é incompatível com casos em que não existam padrões para se manufaturar um mesmo produto em virtude da variação dos insumos disponíveis e do rendimento (ex.: indústria de óleo e gás e indústria química);
- O fator de conversão do Registro K220 não é uma variável fixa, como considerado no *layout* (ex: setor químico);
- O Registro K200 não é aderente em empresas cujos produtos/insumos sofrem efeito de fenômenos físico-químicos, tais como: evaporação, pressão, temperatura, umidade, etc. que geram variação e incerteza nas medições entre origem e destino (ex.: setor químico e agrícola).
- Itens com variação de saldo decorrente de lapso temporal entre o recebimento físico e o registro fiscal podem ocasionar impedimento na validação do arquivo;
- A apuração do inventário e do custo dos produtos obtidos pela complexa contabilidade de custos, contemplando os dados de fichas técnicas, perdas no processo produtivo, ordens de produção, etc.;
- A maioria das empresas não adota o sistema da Contabilidade de Custos, cuja implantação demanda mais tempo e mais investimentos;
- Tempo exíguo e custos que envolvem o desenvolvimento de sistemas e o treinamento de pessoal;
- A circulação de informações entre diferentes setores da empresa e/ou terceirizados, visando sua compilação, pode comprometer o segredo industrial;
- Falta de regras claras quanto aos critérios para se considerar a chamada "perda razoável";
- Empresas que produzem por encomenda ou que, pela dinâmica do processo produtivo, têm grandes variações nas relações entre os insumos e a produção (modificações decorrentes de fatores variáveis como qualidade da matéria-prima empregada, pressão, temperatura, evaporação, etc.) também têm dificuldades para especificação precisa e detalhadas de todas estas diferenças, sendo que, a depender das peculiaridades de cada encomenda, pode ser necessário que o contribuinte seja onerado com a elaboração de um laudo para cada situação pontual;
- Atualmente, o prazo de entrega da EFD ICMS/IPI é no dia 25 do mês subsequente aos fatos geradores, e as empresas entendem que este prazo não é suficiente para todas as compilações necessárias ao envio da informação em meio eletrônico;
- As MPEs enquadradas no Regime Periódico de Apuração e também as empresas tributadas pelo Lucro Presumido, por suas peculiaridades,

alegam que não teriam condições para cumprir as obrigações deste bloco;

- Receio de ampliação da gama de informações que passaria a ser exigida na versão eletrônica;
- De fato, na prática, é muito difícil manter o arquivo Bloco K atualizado, dada a modelagem dos processos produtivos, fator que gera necessidade de acrescentar mais informações quando da entrega do bloco correspondente ao Livro Registro de Controle da Produção e do Estoque no SPED Fiscal;
- Para implantação do custo contábil, será necessário um grande realinhamento interno, tanto no que diz respeito a mudanças de cultura, como também apoio da engenharia, produção, controladoria, análise de custos, recursos humanos e tecnologia de informação;
- Não é por outra razão que a maioria das empresas não adotam a *Contabilidade de Custos*, utilizando o critério arbitrado pelo Fisco para quantificar os estoques e apurar o custo das vendas;
- O problema é que com a internacionalização das normas de contabilidade (Leis nº 11.638/2007, nº 11.941/2009 e Lei nº 12.973/2014), a obrigatoriedade em adotar a contabilidade de custos com base no processo produtivo efetivamente realizado pela empresa encontra amparo legal (*Art. 177 da Lei nº 6.404/1976, que diz respeito a escrituração dos livros, complementada pelas alterações introduzidas pela Lei nº 11.941/2011, especialmente no que tange ao cumprimento destas obrigações pelas companhias fechadas, deixa claro que as demonstrações financeiras deverão ser elaboradas em conformidade com as normas de contabilidade internacionalmente aceitas, sem exceções*) para ser exigida em janeiro de 2015;
- É de se reconhecer que, com a inclusão do bloco K, a Administração Tributária terá acesso a todos os detalhes do processo produtivo e da movimentação de estoques, possibilitando o cruzamento dos saldos apurados pelo SPED com aqueles informados pelas indústrias, via inventário, de forma que, eventual diferença injustificada poderá configurar sonegação fiscal;
- Este bloco contém todos os itens utilizados no processo de manufatura. Ou seja, a empresa estará entregando ao fisco os dados de seu segredo industrial.
- Não existe um padrão técnico informado pela Secretaria da Receita Federal que informe:

    - Metodologia da guarda dos segredos industriais;
    - Forma de armazenamento;
    - Quais setores da SRF terão acesso aos segredos industriais;

- Quais são os sistemas de segurança adotados para a guarda e proteção destes dados;
- Ausência de um manual de procedimentos técnicos para coleta, armazenamento e disponibilização dos dados.

3. PROPOSTAS DA CONFEDERAÇÃO NACIONAL DA INDÚSTRIA - CNI E DA COALIZAÇÃO DE FEDERAÇÕES E ASSOCIAÇÕES SETORIAIS

A Confederação Nacional da Indústria, em conjunto com a coalização de federações e associaçõe setoriais, ao analisarem o sistema do Bloco K, elaboraram um documento constando as seguintes propostas, a fim de dirimir os problemas anteriormente apontados:

- Criação de Fórum permanente de discussão com o setor produtivo (ex.: eSocial e NFe);
- Simplificação dos registros e processos;
- Elaboração/adequação do Guia Prático com todas as orientações necessárias ao correto preenchimento do bloco;
- Criação de ambiente de testes;
- Alterar o layout do SPED para aproximá-lo do layout do livro modelo 3, dentro dos seguintes parâmetros:

- Informar o registro 0210 (Consumo Padronizado), com alguns insumos aglutinados em um item "outros", para preservar o sigilo industrial. Não seriam entregues os blocos de consumo específico. Também não seriam informadas quantidades, apenas a lista de insumos;
- Alterar o registro K230, que discrimina as movimentações de entrada ou saída dos itens existentes no estoque, porque: 1) os modelos vigentes de manutenção e entrega de informações eletrônicas relativas à escrita fiscal de contribuinte do ICMS permitem melhor intercâmbio dos dados das partidas geradas pela entrada, consumo, vendas e ajustes nas contas de estoque, que compõem a ECD, sendo que as movimentações diárias de quantidades do produto seriam correlacionadas com estas partidas da ECD; 2) o item 4.5.1 (Arquivo de Controle de Estoque) do SINCO (Sistema Integrado de Coleta) deve ser eliminado para evitar redundância de informações passíveis

de registro, em cumprimento à regra de fluxo único prevista no Decreto nº 6022/2007;

- Eliminar os registros K235 (Insumos Consumidos na Produção), K250 e K255 (Produtos Industrializados e Consumidos por Terceiro), porque expõem segredo industrial e porque têm efetividade questionável, já que o percentual de perda informado no registro K210 (Entrada e Saída dos Produtos no Estabelecimento) não é o mesmo quando há substituição de insumo, sendo que a eliminação deste cruzamento de registros não traria prejuízos ao fisco;
- Alterar o novo registro K210 (Entrada e Saída dos Produtos no Estabelecimento) para registro por tipo de material.

Para melhor elucidação, seguem os seguintes quadros apresentados pelo Departamento Jurídico da Federação das Indústrias do Estado de São Paulo - FIESP:

O QUÊ	AÇÃO	O POR QUÊ
Reg. 0210	Alterar	➢ Atender ao fisco; ➢ Fexibilidade em não informar parcela dos insumos preservando o sigilo industrial; ➢ Retirar os campos Quantidades e Perdas, que poderão ser aferidas na movimentação de estoques, também como forma de resguardar o sigilo industrial, além de atender as diversidades dos processos produtivos;
Reg. K230	Alterar	➢ O K230 passaria a ser o K210, filho do K200; ➢ Informar as movimentações dos materiais demonstrados no reistro K200, com o tipo de movimentação e quantidades. ➢ Com novo leiaute seria facilitado o cruzamento com o Reg. 1250 da ECD; ➢ Desvios de aplicação poderiam ser encontrados;
Reg. K235 Reg. K250 E filho	Eliminar	➢ Exposição de segredo industrial; ➢ Sem efetividade que estes movimentos estariam detalhados no K210 por tipo de material.

Nº Campo	Descrição	Tipo	Tam	Dec	Obrg
01 REG	Texto fixo contendo "K210"	C	4	-	O
02 DT_MOV	Data: de entrada; ou de saída; ou do estoque	C	8	-	O
03 UNID	Unidade de medida do item	C	6	-	O
04 IND_OPE	Indicador do tipo de informação E = Entrada S = Saída	C	1	-	O
05 TIPO_MOV	Código do tipo de movimentação, conforme tabela padrão identificada abaixo	C	2	-	O
06 QTD_MOV	Quantidade: de entrada ou de saída	C	-	3	O
07 OD_PART	Código do participante (campo 02 do Registro 0150): - proprietário/possuidor que não seja o informante do arquivo	C	60	-	OC
08 INF_COMPL	Informação complementar do tipo de movimento de estoque	C	-	-	OC

Por conseguinte, propuseram, inclusive, um cronograma para implementação do sistema, nos moldes a seguir:

- Implantação se iniciando, no mínimo, em 2017, e apenas para empresas com faturamento acima de R$ 300 milhões/ano, consideradas de grande porte pelo novo padrão contábil;
- Delimitação de implantação a determinados CNAEs;
- Implantação posterior apenas para empresas tributadas pelo lucro real (R$ 78 milhões/ano);
- Final da implantação abarcando as demais empresas;
- Dispensa das MPEs (receita bruta de até R$ 3,6 milhões/ano) optantes pelo Simples Nacional;
- Alteração do layout para aproximá-lo do livro modelo 3, modificando-se os seguintes registros:

- Eliminar o campo "Consumo Específico";
- Eliminar o campo "Insumos Consumidos na Produção";
- Eliminar o campo "Itens Produzidos e Industrializados por Terceiros";
- Alterar o campo "Itens Produzidos".

4. PLEITOS APRESENTADOS

Além da proposta corroborada no tópico acima, insurge mencionar que, em 21/08/2015, foi protocolado junto à SEFAZ/SP um pleito destinado ao atual secretário, com uma "Proposta de Modificação do Bloco K (EFD-ICMS/IPI)", para que esta seja discutida no âmbito do CONFAZ (Conselho Nacional de Política Fazendária) e do COTEPE (Comissão Técnica Permanente do ICMS).

Como resultado das ações realizadas pelo Departamento Jurídico da Federação das Indústrias do Estado de São Paulo - FIESP/DEJUR, no dia 08/10/2015, foi publicado o AJUSTE SINIEF nº 8, de 02/10/2015, trazendo o seguinte cronograma de implantação:

- Em janeiro de 2016, para as empresas com faturamento acima de R$ 300 milhões/ano classificadas nas divisões 10 a 32 da Classificação Nacional de Atividades Econômicas (CNAE) ou habilitadas ao Regime Aduaneiro Especial de Entreposto Industrial sob Controle Informatizado (RECOF), ou a outro regime alternativo a este;
- Em janeiro de 2017, para as empresas com faturamento igual ou superior a R$ 78 milhões classificadas nas divisões 10 a 32 da Classificação Nacional de Atividades Econômicas (CNAE);
- Em janeiro de 2018, para as demais indústrias, equiparadas e estabelecimentos atacadistas classificados nos grupos 462 a 469 da Classificação Nacional de Atividades Econômicas (CNAE).

Observa-se que esses resultados refletem no atendimento parcial a pleito de prorrogação apresentado pela FIESP, em conjunto com a CNI, numa coalização de federações e associações representativas dos setores produtivos. Contudo, seguir-se-á pleiteando a simplificação do cumprimento desta obrigação, por meio da alteração de seu *layout,* bem como a prorrogação também para as grandes empresas, que seguem obrigadas ao envio das informações a partir de janeiro de 2016.

4. DA SEGURANÇA DAS INFORMAÇÕES E DA PROTEÇÃO DE DADOS

Ao analisar a dinâmica a ser instaurada, por meio do Bloco K, observa-se que há dois polos de preocupação no tocante à segurança da informação, quais sejam: as empresas contribuintes e o próprio fisco. Sendo assim, essencial tecer os seguintes comentários, a fim de propiciar uma reflexão acerca das vantagens e desvantagens apresentadas por esta nova sistemática.

Primeiramente, cumpre esclarecer que as ações que envolvem a segurança da informação não possuem legislação. Aliás, no que se refere aos dados, o Brasil

sequer possui norma específica, de forma que a coleta, o tratamento, o armazenamento e o uso dos mesmos seguem sem previsão, apesar de o direito à privacidade e à inviolabilidade do sigilo dos dados estarem protegidos em leis fragmentadas, como Constituição Federal (artigo 5º, incisos X, XII e XXXIII); Código Civil (artigo 21); Lei nº 7.272/1984 (Política Nacional de Informática - artigo 2º, incisos VIII e IX); Lei nº 8.078/1990 (Código de Defesa do Consumidor - artigo 43); Lei nº 9.296/1996 (Lei de Interceptação do Fluxo de Comunicações em Sistemas de Informática e Telemática); Lei nº 9.507/1997 (Lei do Habeas Data); Lei n° 9.427/1997 (Lei Geral das Telecomunicações); Lei nº 12.527/2011 (Lei de Acesso à Informação); e Lei nº 12.965/2014 (Marco Civil da Internet).

Nesta oportunidade, importante mencionar o Anteprojeto de Lei sobre Proteção de Dados Pessoais, o qual estava em consulta pública e pende de aprovação. Apesar de o mesmo versar sobre os dados de pessoas naturais, ou seja, físicas, de acordo com o artigo 5º, inciso VI, alguns pontos concernentes a princípios, conceituações e responsabilidade por parte dos órgãos públicos que coletarão tais informações dos titulares devem ser trazidos à discussão. Uma, porque, como dito, essa lei está adstrita aos dados de pessoas físicas; duas, que, em decorrência disso, verifica-se a real necessidade de um manual específico para essa nova sistemática (Bloco K), tendo em vista tratar de dados sensíveis de pessoas jurídicas.

Senão vejamos, o artigo 6º do APL em comento estabelece que as atividades que envolvam o tratamento de dados pessoais deverão observar a boa-fé e alguns princípios explicitados em seus incisos, dentre eles, da finalidade, da adequação, da necessidade, da transparência e da segurança. Veja:

> **"Art. 6º** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular;
> II - adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;
> III - necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> (…)
> VI - transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;
> VII - segurança: pelo qual devem ser utilizadas medidas técnicas e

> administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".

Tais princípios são de suma importância, vez que, por meio desses, há a possibilidade de se ponderá-los, em caso de eventual colisão, a fim de evitar violações aos direitos personalíssimos, aos quais as pessoas jurídicas também são detentoras e, por conseguinte, podem sofrer dano moral diante de um ato ilícito, nos termos da Súmula 227 do Superior Tribunal de Justiça.

Transpondo-se ao tema desse artigo, observa-se que, assim como no APL, os princípios supracitados também devem ser previstos e aplicados quando da implementação do Bloco K. Conforme restará demonstrado ao final desse artigo, o novo sistema a ser adotado pelo Fisco pende de uma norma regulamentadora, por meio da qual sejam indicadas de forma clara e precisa a finalidade e o mínimo necessário de dados para que o fim seja atingido sem qualquer desproporcionalidade.

Nesse sentido, cita-se como exemplo o Manual de Procedimentos Técnicos para Colheita, Análise, Preservação e Manutenção da Informação no Meio Eletrônico da Polícia Federal, onde há a previsão sobre o tratamento das informações coletadas por esta, inclusive questões relacionadas à segurança das mesmas.

Frisa-se que, em se tratando de procedimentos para viabilizar a segurança das informações sensíveis, relevante colacionar as normas de padrão internacional, como as propostas pela ABNT - Associação Brasileira de Normas Técnicas, quais sejam: ABNT NBR ISO/IEC 27002:2005 (*Code of Practice for Information Security Management*) e ABNT NBR ISO/IEC 27001:2005 (*Information Security Management Systems - Requirements*).

É sabido que a segurança da informação visa garantir, sobretudo, a integridade, a autenticidade e a confidencialidade das informações. No cenário atual, altamente tecnológico, diversas são as vulnerabilidades e variados são os tipos de ataques e fraudes. Sendo assim, imperioso refletir sobre mecanismos, como por exemplo a criptografia, que garantam a integridade dos dados sensíveis das empresas contribuintes impedindo o acesso e o uso indevido por terceiros.

Outro ponto previsto no APL e que cabe perfeitamente a essa discussão, refere-se aos chamados dados anônimos ou anonimizados, os quais são definidos, no artigo 5º, inciso IV, como aqueles relativos a um titular que não pode ser identificado. Ora, em meio às ferramentas tecnológicas disponíveis, a identificação do respectivo titular acaba por ser fácil. Portanto, faz-se necessário haver uma limitação, com o fito de exigir somente os dados realmente necessários para cumprir a finalidade legítima do sistema dificultando, assim, a identificação das empresas contribuintes em caso de eventual incidente, seja por

intermédio de uma fraude ou transferência e comunicação de dados entre órgãos públicos, hipótese essa que precisa estar devidamente esclarecida, principalmente no tocante ao consentimento e os casos em que independerão da autonomia da vontade do titular.

O artigo 21 do APL traz uma questão que merece menção: "os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo". Diante da quantidade de informações, sem qualquer moderação e sem indicação clara da respectiva finalidade, qual garantia as empresas contribuintes terão para que, ao exercer o exercício regular do direito, não sofram sanções administrativas e, se penais, na figura de seus gestores?

Por fim, insta tecer um último comentário nesse cenário comparativo. O APL dispõe, em seus artigos 31 e 32, sobre a responsabilidade dos órgãos públicos pelo tratamento de dados dos titulares, sob pena de responder perante o órgão competente. Ressalta-se que a ideia do anteprojeto é a criação de um órgão independente responsável pela fiscalização do cumprimento da legislação sobre proteção de dados pessoais.

Interessante notar que, além das medidas e punições cabíveis (artigo 31), o órgão competente poderá exigir que agentes do poder público disponibilizem relatórios de impacto de privacidade e sugerir a adoção de medidas padrões e de boas práticas aos órgãos públicos, de acordo com o artigo 32.

Como visto, o quadro brasileiro para proteção de dados, seja de pessoas físicas e/ou jurídicas, pende de regulamentação. Mesmo diante da aprovação e da entrada em vigor do referido anteprojeto de lei, o mesmo não poderá ser aplicado na relação entre o Fisco e as empresas contribuintes, vez que aquele versa somente sobre a proteção de dados de pessoais naturais. Desta feita, ainda que se permita a analogia, imprescindível a criação de um manual, pelo próprio fisco, estabelecendo princípios, diretrizes, obrigações, deveres e responsabilização no tocante ao Bloco K.

No início desse tópico foram destacados dois polos de preocupação quanto à segurança da informação (assim denominado para fins meramente didáticos). Em se tratando do primeiro polo, empresas contribuintes, é fato que as mesmas deverão se ajustar não somente para entender sobre o funcionamento deste novo sistema, sobretudo, para implementar ações que visem a segurança de seus dados, com o fim de assegurar que suas informações sigilosas e segredos industriais não sejam acessados e/ou publicados indevidamente por terceiros.

Senão vejamos, as ações de segurança da informação dependem, e muito, do histórico, da rotina, da atividade, do perfil e do porte da empresa. Entretanto, algumas medidas são imprescindíveis para impedir as chamadas fraudes cibernéticas:

- verificar quais são os equipamentos/dispositivos utilizados pelos funcionários, colaboradores, gestores, diretores e, se o caso, por terceiros;

- avaliar quais são as informações sensíveis e quem tem acesso às mesmas. Criar níveis de acesso no sistema interno é essencial para se certificar que somente determinados usuários poderão visualizar, alterar e manter tais dados;
- utilização de mecanismos de segurança, sejam eles físicos (a fim de prevenir que acidentes e desastres naturais, como incêndio, ou furto e roubo provoquem o perecimento ou a perda das informações) e eletrônicos (softwares, criptografia, etc.);
- qualificar profissionais que atuem diretamente quando da ocorrência de eventual incidente - criação de um departamento específico para incidentes, o qual terá atividades e responsabilidades diversas do departamento de Tecnologia da Informação (TI), principalmente no que tange à preservação de provas eletrônicas e perícia;
- promoção de uma governança corporativa, permitindo a integração das áreas de recursos humanos, financeiro, administrativo, jurídico e TI, a fim de que atuem juntos quando da contratação e demissão de funcionários, colaboradores e terceirizados;
- criação de normas e políticas internas sobre o uso de redes sociais, e-mails, downloads, sites e dispositivos pessoais; revisão de contratos; termos de responsabilidade e confidencialidade; e,
- treinamento e capacitação. Destaca-se, oportunamente, que muitos incidentes decorrem das chamadas "fraudes ocupacionais", ou seja, aquelas decorrentes de atos praticados pelos próprios empregados da empresa, seja intencionalmente ou não.

Eis a problemática, analisando os itens supracitados, resta claro que os procedimentos de segurança da informação envolvem, além do fator humano, esforços financeiros que muitas empresas não os possuem suficientemente a priori ou em curto espaço de tempo. Entretanto, tais ações são imprescindíveis, haja vista que eventual incidente nesse sentido poderá acarretar na perda de propriedade intelectual, segredos industriais, perda econômica e de investidores, abalo na marca e na reputação da empresa.

Por outro lado, no tocante ao Fisco, como já discorrido, insta refletir sobre como o mesmo implementará a gestão de todas as informações fornecidas pelas empresas contribuintes. Conforme delineado ao longo desse artigo, até o presente momento, não foi apresentado qualquer manual informando a sociedade sobre os mecanismos de segurança da informação violando o princípio da transparência. Como visto, no Brasil, não há qualquer legislação específica sobre o tema, sendo assim, o Fisco adotará as regras e normas de padrão internacional sobre segurança da informação como o mundo corporativo? Perante essa omissão, seria aplicável a futura lei de proteção de dados pessoais como analogia, principalmente no que se refere a seus princípios?

A transparência quanto à segurança da informação é de suma importância, a fim de combater ações ilícitas e ilegais que podem incorrer em violação ao sigilo dos dados das empresas e, até mesmo, em atos de concorrência desleal. E, aqui, insta refletir sobre qual será a responsabilidade do fisco, na eventualidade de um incidente relacionado a vazamento de informações sigilosas e segredos industriais, se o mesmo ocorrer por sua culpa, violando, por conseguinte, os direitos personalíssimos da pessoa jurídica.

Não obstante, relevante destacar a questão do chamado *Big Data* e a possibilidade de identificação do titular por intermédio dos dados anônimos ou anonimizados explicitados anteriormente. É sabido que empresas dos mais variados setores têm se utilizado, muitas vezes indiscriminadamente, de informações obtidas, com ou sem o consentimento de seus respectivos titulares, com o objetivo de aprimorar a qualidade de serviços, mitigar riscos, marketing, publicidade e pesquisas.

Uma das discussões centrais sobre a necessidade de uma lei específica sobre proteção de dados é a falta de transparência quanto à finalidade da coleta e do uso de determinadas informações. Nesse mesmo sentido encontra-se a necessidade de o Fisco apresentar um documento (manual) que detalhe acerca da coleta, do tratamento, do armazenamento e do uso de todas as informações que serão fornecidas, ademais, sobre o futuro descarte das mesmas, a fim de que haja proporcionalidade e efetividade na implementação deste novo sistema.

5. DELIMITAÇÃO DO PROBLEMA

A partir de janeiro de 2017, os estabelecimentos industriais e equiparados a industriais, bem como os estabelecimentos atacadistas, deverão enviar às autoridades fazendárias informações relativas ao chamado "Bloco K do SPED Fiscal", que é a versão digital do livro Registro de Controle da Produção e do Estoque (modelo 3).

Como visto, trata-se de um livro instituído pelo Convênio s/nº de 15/12/1970, destinado à escrituração dos documentos fiscais e dos documentos de uso interno do estabelecimento, correspondentes às entradas e saídas de produtos e insumos, à produção e às quantidades referentes aos estoques de mercadorias, matéria-prima, insumos, embalagens, produto final e percentual de perdas apurado.

Os registros correspondem aos dados das Notas Fiscais, das Ordens de Produção e das Fichas Técnicas dos produtos, relacionados a perdas ocorridas no processo produtivo, aos insumos consumidos e às quantidades produzidas, inclusive, as industrializações efetuadas por meio de terceiros.

Contudo, além dos custos operacionais para implantação desta obrigação em meio eletrônico, existe também a preocupação de que ela possibilite a compilação e envio de informações que constituam sigilo industrial, em razão de

seu alto grau de detalhamento. O contribuinte, anteriormente à edição desta norma, poderia deixar suas informações sigilosas, em relação ao seu segredo industrial, em locais separados dentro da empresa. Agora, está obrigado a condensar estas informações, em tese o seu segredo industrial, para posterior entrega às autoridades da Secretaria da Receita Federal.

O fisco, por sua vez, considera que as informações exigidas para os fins do Bloco K, que visa fiscalizar a apuração do IPI e do ICMS, se referem apenas a quantidades físicas dos produtos e insumos utilizados, não tendo o condão de revelar a composição química dos bens manufaturados a ponto de colocar em risco informações sigilosas.

O Bloco K compõe uma das obrigações tributárias acessórias, em meio eletrônico, cujos dados são destinados ao ambiente nacional do Sistema Público de Escrituração Digital (SPED), instrumento que unifica as atividades de recepção, validação, armazenamento e autenticação de livros e documentos que integram a escrituração contábil e fiscal dos empresários e das pessoas jurídicas, inclusive imunes ou isentas, mediante fluxo único e computadorizado de informações.

A implantação do SPED, para compartilhamento de cadastros e de informações fiscais entre as administrações fazendárias das três esferas de governo objetiva, em tese, o avanço na informatização da relação entre o fisco e os contribuintes, fazendo parte de um projeto de modernização que busca remover obstáculos burocráticos ao crescimento econômico e ao aprimoramento da fiscalização.

6. CONCLUSÕES

Os contribuintes de todo o Brasil terão que entregar dados sensíveis e sigilosos de industrialização de seus produtos. Fórmulas que, se divulgadas ou "vazadas" de algum modo, podem comprometer a vida e a credibilidade das empresas.

Senão vejamos, como mencionado anteriormente, a rubrica 0210 (insumos, componentes e perdas percentuais) da EFD pode expor fórmulas de produtos das indústrias, muitas vezes verdadeiros segredos industriais que passariam a ser compilados e a circular por mais de um setor da empresa para cumprimento da obrigação eletrônica, além de expor a margem de lucro dos contribuintes. Ademais, as empresas alegam que este registro tem efetividade questionável por não refletir a produção real. Dados que antes estavam separados, agora devem ser reunidos e terão que trafegar pela internet.

É notório, em todas as mesas de discussão, de que o Departamento de Polícia Federal, em 2006, lançou o seu manual de procedimentos técnicos para coleta,

análise, disponibilização das provas e documentos digitais, visando garantir a integridade e a segurança dos documentos coletados no ambiente da internet e também em dispositivos informáticos.

A Polícia Federal se desenvolveu e se elevou a padrões internacionais, de forma que, com a criação deste manual, oferece à sociedade e ao Estado elevado grau de transparência e segurança em relação à preservação, à segurança e ao sigilo das informações sensíveis e sigilosas que são armazenadas.

Intenta-se, por intermédio deste artigo, alertá-los acerca dos riscos que a União e os Estados passam a correr, considerando que sites, como o "tudo sobre todos", explicitado no início deste artigo, dentre outros, divulgam, com determinada facilidade, informações sigilosas de contribuintes.

Sendo assim, cumpre refletir sobre qual a garantia que a Secretaria da Receita Federal do Brasil pode oferecer hoje à indústria de que seus respectivos dados sigilosos não ficarão vulneráveis. Concomitantemente, indaga-se: Uma vez que a Secretaria da Receita Federal atuará com a coleta de dados extremamente sensíveis e sigilosos de contribuintes, não deveria ser criado um manual de instruções e procedimentos técnicos, que revelasse ao contribuinte e ao Estado-cidadão-arrecadador, a formatação de segurança, de armazenamento e disponibilização destas informações?

As informações que passam a ser coletadas pela SRFB não devem atender aos princípios da necessidade e da proporcionalidade? Sendo informações altamente sensíveis não deveriam ter um sistema de proteção próprio e transparente?

Quanto à guarda destes documentos e a possibilidade de vazamento destas informações, quais seriam as sugestões do Departamento de Polícia Federal, juntamente com o Instituto Nacional de Criminalística da Polícia Federal, sobre o tema?

Um fisco forte só será possível com a construção democrática de métodos de segurança e transparência na relação com os contribuintes. Um projeto pautado em dados e informações verossímeis. A função do Estado Democrático de Direito é a construção de um método preventivo e que, simultaneamente, combata a corrupção e a sonegação.

Nos estudos da construção do Bloco K não existem dados sobre os sistemas de segurança que o Fisco pretende implementar para garantir que informações sigilosas e sensíveis não sejam corrompidas ou "vazadas". O cibercrime vai atacar o lado mais fraco da relação Fisco-Contribuinte.

Antes do enfrentamento das últimas operações da Polícia Federal, notadamente a operação lava jato, o combate à corrupção no Brasil não costumava ser enumerado entre as missões da administração pública.

Quando o Emissor de Cupom Fiscal (ECF) foi criado, anunciava-se o fim das fraudes no varejo, porém, a partir de falhas sistêmicas, equipamentos e pareceres do Confaz foram anulados, comprometendo, desta forma, os pilares básicos de tal

projeto, tais como os requisitos específicos de segurança da informação e a comprovação eficiente da autenticidade e integridade. Estes pareceres "garantiam" a inviolabilidade das máquinas ECF, mas as armas da sonegação fiscal sempre encontram os seus caminhos.

Portanto, em prol da transparência e da segurança das informações que serão coletadas, tratadas e armazenadas, imprescindível a elaboração de um manual que estabeleça princípios e diretrizes para o uso legítimo dos dados das empresas contribuintes, a fim de minimizar riscos às fraudes e à concorrência desleal, bem como que o Bloco K seja implementado de forma eficaz e pautado pelo princípio da proporcionalidade.

7. REFERÊNCIAS

BRASIL. Lei 6.374, de 02 de março de 1989. Dispõe sobre a instituição do ICMS. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 02 mar. 1989. Disponível em:
<http://www.al.sp.gov.br/repositorio/legislacao/lei/1989/lei-6374-01.03.1989.html> Acesso em: 07 jan. 2016.

BRASIL. Convênio S/Nº, de 15 de dezembro de 1970. Dispõe sobre a criação do Sistema Nacional Integrado de Informações Econômico-Fiscais. Diário Oficial [da] República Federativa do Brasil, 18 fev. 1971. Disponível em:
<http://www1.fazenda.gov.br/confaz/confaz/convenios/sinief/cvsn_70.htm> Acesso em: 07 jan. 2016.

BRASIL. Ajuste SINIEF 2, de 03 de abril de 2009. Dispõe sobre a Escrituração Fiscal Digital - EFD. Diário Oficial [da] República Federativa do Brasil, 08 abr. 2009. Retificado em: 22 dez. 2010. Disponível em:
<http://www1.fazenda.gov.br/confaz/confaz/Ajustes/2009/AJ_002_09.htm> Acesso em: 07 jan. 2016.

BRASIL. Ajuste SINIEF 17, de 21 de outubro de 2014. Altera o Ajuste 02/2009. Diário Oficial [da] República Federativa do Brasil, 23 out. 2014. Disponível em:
<http://www.normaslegais.com.br/legislacao/ajuste-sinief-17-2014.htm> Acesso em: 07 jan. 2016.

BRASIL. Ajuste SINIEF 8, de 02 de outubro de 2015. Altera o Ajuste 02/2009. Diário Oficial [da] República Federativa do Brasil, 08 dez. 2015. Disponível em:
<https://www.confaz.fazenda.gov.br/legislacao/ajustes/2015/aj_008_15> Acesso em: 07 jan. 2016.

BRASIL. Decreto nº 45.490, de 30 de novembro de 2000. Aprova o Regulamento do Imposto sobre Operações Relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e Comunicação - RICMS no Estado de São Paulo. Disponível em:
<http://www.al.sp.gov.br/repositorio/legislacao/decreto/2000/decreto-45490-30.11.2000.html> Acesso em: 07 jan. 2016.

BRASIL. Decreto nº 6.022, de 22 de janeiro de 2007. Institui o Sistema Público de Escrituração Digital - SPED. Diário Oficial [da] República Federativa do Brasil, 22 jan. 2007. Disponível em:
http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/Decreto/D6022.htm> Acesso em: 07 jan. 2016.

BRASIL. Constituição Federal de 1988 BRASIL. Constituição da República Federativa do Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 5 out. 1988. Disponível em:
<http://www. planalto.gov.br/ccivil_03/Constituicao/Constituicao. htm>. Acesso em: 20 jun. 2013.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial [da] República Federativa do Brasil, 11 jan. 2002. Disponível em:
<http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm> Acesso em: 07 jan. 2016.

BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 30 out. 1984. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L7232.htm>. Acesso em: 07 jan. 2016.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 12 set. 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em: 07 jan. 2016.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do Art. 5° da Constituição Federal. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 25 jul. 1996. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em: 07 jan. 2016.

BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm>. Acesso em: 07 jan. 2016.

BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 17 jul. 1997. Disponível em: < http://www.planalto.gov.br/ccivil_03/LEIS/L9427cons.htm>. Acesso em: 07 jan. 2016.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º. Lei de Acesso à Informação. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 18 nov. 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 07 jan. 2016.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 24 abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 07 jan. 2016.

BRASIL. Anteprojeto de Lei. Dispõe sobre o tratamento de dados pes-soais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.justica.gov.br/noticias/mj-apresenta-nova-versao-do-anteprojeto-de-lei-de-protecao-de-dados-pessoais/apl.pdf> Acesso em: 07 jan. 2016.

BRASIL. Súmula 227 do Superior Tribunal de Justiça. Diário de Justiça, 20 out. 1999. Disponível em: <https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2011_17_capSumula227.pdf> Acesso em:07 jan. 2016.

Capítulo VIII

A infiltração cibernética no processo penal brasileiro

Diana Mann[78]

1. INTRODUÇÃO

A questão que se propõe investigar no presente artigo versa sobre a utilização, no sistema penal pátrio, do instituto da "infiltração" como técnica investigativa em crimes cibernéticos[79].

A utilização de agentes infiltrados pelo estado é um recurso antiquíssimo do qual já se valeu até mesmo a Santa Inquisição[80]. Embora as sociedades ocidentais tenham sofrido sensíveis modificações, principalmente em face do fortalecimento do estado democrático de direito, notadamente nos últimos 50 anos, essa ferramenta de investigação continua a ser um recurso de grande valia nas investigações. Entretanto, desperta calorosos debates em face da possibilidade de violação de princípios consagrados pela dogmática penal e extremamente caros ao estado democrático de direito, como por exemplo, o princípio que veda a auto-incriminação, os limites éticos do estado, o direito a intimidade, entre outros.

---

[78] A Autora é mestranda em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Pública de Lisboa/PT, especialização em Criminologia e Investigação Criminal, pós-graduada em Gestão de Segurança na Sociedade Democrática, pela Universidade Luterana do Brasil; e graduada em Ciências Sociais e Jurídicas pela Universidade Federal de Santa Maria/RS,Na área de Segurança Pública, é **Delegada de Polícia Federal desde 2003**, foi chefe substituta do Serviço de Repressão a Crimes Cibernéticos da Policia Federal (SRCC/DICOR/DPF). Atualmente é Chefe da Divisao de Direitos Humanos da Policia Federal (DDH/CGDI/DICOR/DPF).

[79] De acordo com a posição do computador no iter criminis, os crimes cibernéticos podem ser definidos em próprios e impróprios, sendo os primeiros aqueles que passaram a existir apenas com o advento da Internet e os segundo aquelas condutas que já eram crime mas que passaram a ser "facilitadas pelo uso do computador" com os furtos, estelionatos e tráfego de pornografia infantil. Importe frisar que todas as referências a crimes cibernéticos que faremos ao longo desse artigo englobarão a generalidade dos ditos crimes cibernéticos, ou seja, os crimes cibernéticos puros ou próprios, como a invasão de sistemas, quanto aqueles impróprios ou facilitados pelo computador, como por exemplo a transmissão de pornografia infantil. Uma definição bastante didática quanto a essa classificação pode ser encontrada quanto as diferenças em Crimes Cibernéticos: Ameaças a Procedimentos e Investigação, de Emerson Wendt e Higor Moreira Jorge.

[80] Sobre as origens históricas leia mais em Oneto, Isabel. "O Agente Infiltrado. Contributo para a Compreensão do Regime Jurídico das Ações Encobertas".

Nesse texto, vamos enfrentar algumas dessas questões visando demonstrar a possibilidade de utilização da técnica da infiltração para a investigação dos crimes cibernéticos, transmutando o "agente infiltrado" em uma "infiltração digital" com a criação de um perfil fictício construído e utilizado por uma equipe de investigação.

2. ORIGENS NO DIREITO BRASILEIRO E ALCANCE DA LEI 12850/2013 .

Embora a infiltração de agentes do estado seja uma técnica utilizada desde tempos imemoriais, no Brasil apenas muito recentemente o legislador tratou do assunto.

A Lei 10.217 de 11 de abril de 2001, ao alterar os artigos 1º e 2º da Lei 9.034/1995, foi a primeira a tratar do tema "infiltração", apresentando-a como meio de prova e procedimento investigatório a ser utilizado em crimes praticados por quadrilha ou bando, ou por organizações criminosas de qualquer tipo, estabelecendo que, em qualquer fase da persecução penal, poderiam ser admitidos, como procedimentos de investigação e formação de prova, a ação controlada, a interceptação ambiental e a infiltração de agentes de polícia ou de inteligência, mediante autorização judicial obtida em procedimento sigiloso.

A Lei em questão não trazia, no entanto, a definição de organizações criminosas, não detalhava o procedimento a ser seguido para a realização da infiltração e tampouco conferia tratamento jurídico aos atos ilícitos porventura praticados durante a infiltração[81].

Posteriormente, a Lei 11.343/2006, ao tratar do tema das drogas, possibilitou a utilização da infiltração como instrumento investigativo ou meio de prova. Mais uma vez, o legislador foi extremamente sintético e não se preocupou em detalhar os procedimentos necessários à produção da prova através da infiltração.

Atualmente, estamos sob a égide da Lei 12.850/2013, que define organizações criminosas e traz maiores detalhes sobre o procedimento, definindo o tratamento dos atos praticados durante a infiltração e demonstrando maior preocupação com o tratamento jurídico dos atos praticados pelo policial infiltrado.

Como a Lei em tela trata de organizações criminosas, a técnica investigativa poderá ser usada quando os crimes em investigação estiverem sendo praticado em "associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais, cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional".

No § 2º do Art. 1º, a Lei 12850/2013 prevê a possibilidade de aplicação de seus dispositivos às infrações previstas em tratados e às organizações terroristas.

[81] Nesse período, o conceito de organização criminosa aplicado no direito brasileiro era o trazido pela na Convenção de Palermo

Como corolário, as técnicas de investigação trazidas no bojo do referido diploma legal, dentre elas a infiltração, possuem um âmbito de aplicação que desborda as ações praticadas pelas organizações criminosas.

No caso das infrações penais previstas em tratado, que possuam o viés da transnacionalidade, importante referir que a República Federativa do Brasil é signatária de diversos tratados em matéria penal[82]. Entre eles destacam-se a Convenção das Nações Unidas contra o Crime Organizado Transnacional, mais conhecida como Protocolo de Palermo, a Convenção contra o Tráfico Ilícito de Entorpecentes e de Substâncias Psicotrópicas, a Convenção sobre os Direitos da Criança, Convenção Internacional sobre Eliminação de todas as formas de Discriminação Racial, a Convenção contra a Tortura e outros Tratamentos ou Penas cruéis, Desumanas ou Degradantes, a Convenção das Nações Unidas contra Corrupção, dentre outras.

Muito embora os ilícitos que os referidos tratados almejam reprimir possam ser praticadas por organizações criminosas, algumas vezes, em face do conceito restritivo da Lei 12850/2013, os grupos criminosos se organizam de modo tal que não é possível enquadrá-los na definição legal de organização criminosa.

Exemplos podem ser encontrados nos grupos criminosos que atuam na internet, especialmente naqueles dedicados aos crimes relacionados à pornografia infantil, racismo e fraudes eletrônicas.

Nesses casos, mesmo não sendo possível encontrar todos os elementos da definição legal de organização criminosa, as técnicas de investigação previstas na Lei 12850/2013/2013 podem ser utilizadas, desde que o crimes em investigação esteja previsto em tratado e possuam a característica da transnacionalidade, esta conferida pela atuação no ciberespaço.

A jurisprudência do Superior Tribunal de Justiça tem entendido que os crimes praticados pela internet podem ser considerados transacionais em face do *modus operandi* do grupo criminosos em investigação[83].

---

[82] Para verificar todos os tratados ratificados pelo Brasil basta consultar o site do Ministério das Relações Exteriores (http://dai-mre.serpro.gov.br).

[83] Nesse sentido o entendimento do STJ ao analisar a competência da justiça criminal para o julgamento de grupo que disseminava pornografia infantil na Internet.

RECURSO ORDINÁRIO EM HABEAS CORPUS. PRODUÇÃO E FOTOGRAFIA DE CENA PORNOGRÁFICA ENVOLVENDO CRIANÇA, DIVULGAÇÃO DE IMAGENS OU FOTOGRAFIAS COM CONTEÚDO PORNOGRÁFICO INFANTIL E ARMAZENAMENTO DE ARQUIVOS CONTENDO CENAS OU IMAGENS PORNOGRÁFICAS OU DE SEXO EXPLÍCITO ENVOLVENDO CRIANÇAS OU ADOLESCENTES. UTILIZAÇÃO DE FÓRUNS NA INTERNET E SITE EM REDE OCULTA NA INTERNET. TRANSNACIONALIDADE DO DELITO. COMPETÊNCIA DA JUSTIÇA FEDERAL.

1. De acordo com o artigo 109, inciso V, da Constituição Federal, compete aos Juízes Federais processar e julgar "os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente".

2. No caso dos autos, o crime em tese praticado pelo recorrente consta daqueles cujo combate o Brasil se comprometeu perante a comunidade internacional, ao aderir à Convenção sobre os Direitos da Criança e do Adolescente, promulgada no ordenamento jurídico pátrio pelo Decreto 99.710/1990. 3. Para que a competência da Justiça Federal seja firmada, não basta que o Brasil seja signatário da referida Convenção,

Também existe previsão de aplicação dos ditames da lei antes referida com relação às organizações terroristas. Importante referir que até o momento o sistema legal pátrio não possui uma Lei que as defina como tal ou que tipifique suas atividades, embora exista um projeto de Lei em tramitação no Congresso Nacional[84]. Assim, caso haja a prática de crimes já tipificados no nosso ordenamento, os autores responderão por crime comum se ofenderem bem jurídico penalmente protegido, podendo restar configurada uma organização criminosa nos moldes delineados pela Lei 12850/2013. Nesse caso, será plenamente possível a utilização das técnicas de investigação ali previstas.

3. A INFILTRAÇÃO COMO MEIO DE OBTENÇÃO DE PROVAS

Conforme o tratamento dispensado pela própria Lei 12850/2013, a infiltração configura um meio de obtenção de prova.

As medidas previstas na lei do crime organizado se desenvolvem, ordinariamente, na fase de inquérito policial. No Brasil, o inquérito policial não é considerado uma fase do processo penal, pois a lide não teria sido formalmente constituída, o que somente teria efeito após o recebimento da denúncia pelo Juiz do feito.

Não obstante terem curso na fase de inquérito, as medidas investigativas trazidas pela Lei 12850/2013 somente são passíveis de realização mediante autorização judicial. Assim, necessariamente, haverá um procedimento judicial no bojo do qual a decisão judicial será exarada.

Inobstante as vozes em contrário, a infiltração configura momento de produção de prova. Conforme nos ensina o doutrinador Márcio Anselmo[85]:

Embora seja recorrente na doutrina a expressão de que não se produz prova no inquérito policial, tal expressão apresenta-se falaciosa, uma vez que a quase totalidade dos elementos probatórios carreados às ações penais são identificados ou produzidos no curso da investigação criminal na fase pré-processual, ou seja, no curso do inquérito. Ou seja, as tão conhecidas "operações policiais", em sua grade maioria, não são nada além do que uma fase de um inquérito policial,

sendo imprescindível a comprovação da internacionalidade da conduta atribuída ao acusado. Precedente. 4. Na hipótese em apreço, a forma como o recorrente disponibilizaria, transmitiria, publicaria e divulgaria arquivos contendo pornografia ou cenas de sexo explícito envolvendo crianças ou adolescentes permitira o seu acesso por pessoas em qualquer local do mundo, bastando que também participassem dos mesmos fóruns que ele, ou que também acessassem sites na rede oculta chamada deep web, circunstância que revela a transnacionalidade da conduta narrada na exordial acusatória e justifica a competência da Justiça Federal para processar e julgar o feito. [*omissis*] 2. Recurso desprovido.

[84] Trata-se do projeto de Lei 2016/2015 (http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1514014)

[85] Anselmo, Marcio Adriano. "Inquérito policial é o mais importante instrumento de obtenção de provas." Consultor Jurídico. 4 de Agosto de 2015. http://www.conjur.com.br/2015-ago-04/academia-policia-inquerito-importante-instrumento-obtencao-provas#author (acesso em 19 de Dezembro de 2015)

destinada à arrecadação de provas e indícios de autoria e materialidade de infrações penais (Anselmo, 2015).

Ademais, a produção da prova durante o inquérito policial não inviabiliza o exercício do contraditório. De fato, outras provas serão recolhidas já prontas e acabadas no mundo dos fatos e levadas ao processo, como por exemplo documentos já constituídos, cartas, fotografias, exames periciais, entre outros, e, nem por isso, deixam de se constituir formalmente como prova, uma vez que a defesa poderá em momento oportuno contestar a validade dos referidos elementos probatórios.

Assim, a infiltração consiste meio de prova e os dados recolhidos durante a infiltração configuram prova, a ser submetida ao contraditório no momento oportuno (contraditório diferido). Vamos além, consideramos que a infiltração configura cautelar de produção antecipada da prova.

4. ADMISSIBILIDADE E LIMITES ÉTICOS

A técnica de recolha de provas através da infiltração não é isenta de críticas. As vozes contrárias afirmam a existência de gravíssima contradição que deslegitima o Estado como titular do *jus puniendi*.

Para desempenhar o seu papel de repressor das condutas ilícitas, o Estado concede aos seus agentes a faculdade de cometer os mesmos atos que repudia. Em face disso, perderia a legitimidade para a persecução criminal pois, na ânsia de fazer cumprir as regras, ele mesmo as viola.

Manuel da Costa Andrade (2003, pag. 299) chega ao ponto de enquadrar a infiltração como método proibido de prova por consistir em um meio enganoso em face de seu qualificado lastro de deslealdade, pondo em causa "a dignidade, a cultura jurídica e a legitimação do processo penal". Entretanto, no mesmo paragrafo o autor reconhece que a generalidade dos autores e da jurisprudência continuam a encarar o "polizeispitzel como expediente indispensável de uma resposta eficaz as manifestações mais ameaçadoras da criminalidade",[86].

Para coadunar a técnica da infiltração com os limites éticos aos quais o estado está adstrito, a medida não deve ser utilizada para qualquer evento

[86] Cabe aqui esclarecer que o Art. 126 do Código de Processo Penal Português, ao elencar os métodos proibidos de prova, estabelece literalmente que é proibida a *utilização de meios enganosos*, in literis:

Artigo 126.º - Métodos proibidos de prova

1 - São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coacção ou, em geral, ofensa da integridade física ou moral das pessoas.

2 - São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante:

a) Perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos;

[omissis].

criminoso. A própria Lei 12850/2013 dispõe que a infiltração somente será autorizada quando em seu requerimento for demonstrada a necessidade da medida.

Nesse passo, a palavra necessidade deve ser entendida como *imprescindibilidade*. Além de ser medida que permitirá aos investigadores adentrar na intimidade de terceiros (seja a infiltração concreta, real, atual ou seja ela virtual), envolve alto grau de risco para os seus executores. Assim, é imprescindível demonstrar ao juiz que este é o único caminho para a obtenção da prova, pois todos os demais já falharam ou, diante das particularidades do caso em concreto, certamente falhariam. A medida tem caráter subsidiário, como leciona Flávio Maltez Coca (2015, 234):

> Entrementes, a infiltração policial será autorizada se a prova não puder ser produzida por outros meios disponíveis (§ 2º do Art. 10), vale dizer, é mister comprovar a necessidade da medida (§ 3º do Art. 10). Não se pode conceber a atuação do agente infiltrado somente para facilitar a descoberta da verdade. Trata-se de um meio subsidiário de produção da prova, tendo o legislador destacado que a operação de infiltração será autorizada quando necessária (§ 1º do Art. 12).

Nesse ponto, importante ainda mencionar os limites da infiltração. A ação do agente infiltrado deve ser de tal modo cuidadosa que jamais interfira na formação da vontade dos investigados. Não pode o infiltrado atuar como provocador da prática dos ilícitos.

Embora a lei atual tenha tratado do assunto com mais detalhamento, ainda é bastante vaga. A questão dos limites, ou seja, quais atos podem ser praticados pelo infiltrado, é tratada de maneira bastante superficial.

Juntamente com a demonstração da necessidade da medida, cabe ao requisitante demonstrar o alcance da tarefa dos agentes, cabendo a decisão judicial fixar os seus limites.

Importante referir que em face do princípio da imparcialidade e da vigência do sistema acusatório no processo brasileiro, não cabe ao juiz detalhar a ação investigativa, apenas balizá-la em face do que lhe foi apresentado para aprovação, adequando-a as regras específicas e gerais limitadoras do *jus puniendi*. Assim, a ação policial será o resultado do que foi pedido, subtraído o que não foi autorizado.

Outro ponto deveras tormentoso e que deverá ser analisado na definição dos limites da infiltração, relaciona-se com a possibilidade de cometimento de atos ilícitos durante a infiltração.

A lei em análise estabelece no Art. 13 que não é punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando *inexigível* conduta diversa.

A redação do artigo comumente é interpretada como uma proteção ao executor da medida. Entretanto, defendemos que o dispositivo em questão

permite que, desde logo, seja solicitada a autorização para a prática dos atos ilícitos necessários à investigação, bem como a delimitação desses atos da forma mais detalhada possível.

Esse é o caso por exemplo, das infiltrações em grupos virtuais, privados ou secretos, que se dedicam à prática de crimes relacionados à pornografia infantil, seja transmissão, seja a produção de imagens dos abusos sexuais por eles praticados. É muito comum que os membros desses grupos exijam provas de que o novato é um criminoso do mesmo jaez. Nesse caso, para a construção da credibilidade do perfil infiltrado será necessário possuir e compartilhar pornografia infantil. [87]

É possível também que ações de infiltração tragam dilemas éticos aos executores da medida, mesmo que todas as ações estejam sendo executadas dentro dos limites do judicialmente autorizado, o desconforto causado pelo contato com criminosos e pela prática de atos ilícitos é um fator que não pode ser ignorado. Em face disso, a seleção e treinamento dos profissionais incumbidos desse tipo de missão é uma tarefa prévia indispensável.

Outro questionamento vinculado à infiltração, relaciona-se a vedação à auto-incriminação, também conhecida através do brocardo latino *nemo tenetur se detegere*. A assimilação do referido princípio pelos estados democráticos de direito foi e continua sendo de extrema importância para a abolição da tortura e de outros métodos degradantes utilizados para a obtenção da prova. Constituem exemplos de aplicação do *nemo tenetur* o direito ao silêncio (no interrogatório policial ou judicial), o direito de não participar de acareações, reconhecimentos, reconstituições, não fornecer padrões gráficos ou de voz para perícia, etc. Não se pode compelir o acusado a praticar tais atos e tampouco extrair consequências negativas da sua recusa. Desse princípio decorre a obrigação para o estado acusador de produzir as provas necessárias à condenação (Giacomolli, 2015, pág. 211).

No caso da infiltração, os investigados contribuem, sem saber, para a constituição da prova e o fazem desconhecendo a condição do infiltrado, a quem consideram membro da organização criminosa e por isso "digno" de confiança.

De fato, a admissão da infiltração representa uma mitigação do *nemo tenetur*. Em razão disso, a infiltração há de ser admitida em caráter de excepcionalidade, em casos em que os bens jurídicos em risco sejam sobremaneira caros à sociedade para justificar uma atuação excepcionalmente severa.

Mesmo assim, a adoção de alguns cuidados é imprescindível. O principal deles consiste em não interferir na formação da vontade dos investigados, de modo a ficar patente que presente ou ausente o agente infiltrado o resultado obtido seria o mesmo, ou seja, a formação da vontade do autor do delito e o *iter*

[87] Entretanto, a ação deverá ser judicialmente autorizada e revestida de diversos cuidados para evitar exposição da identidade de menores e a revitimização de uma criança vítima de abuso sexual em face de nova exposição.

criminis por ele percorrido seria idêntico.

5. A INFILTRAÇÃO REAL X INFILTRAÇÃO VIRTUAL

A massificação do uso da internet pela população mundial a partir do ano 2000 produziu importantes e inovadores fenômenos sociais. A internet, mais do que uma ferramenta de comunicação da era moderna, tornou-se um emulador da vida social, a ponto de os estudiosos do tema não falarem mais em mundo virtual, mas considerarem a internet em si mesma como uma das faces da realidade, dado que o virtual não se oporia ao real, mas sim ao atual (Lévy, 1999, pag 50).

Por essa perspectiva todos os fenômenos que ocorrem na vida social também têm projeção na internet, inclusive aqueles comportamentos consi-derados desviantes, criminosos ou não.

A prática de crimes no ciberespaço traz para o âmbito da investigação criminal o desafio de explorar o mundo virtual em busca de vestígios do crime. Diferentemente dos crimes cometidos no mundo real (ou atual), o local a ser explorado em busca de vestígios será o ambiente virtual. Assim como um homicida deixa impressões digitais na arma utilizada para cometer o crime, também o criminoso virtual deixará suas pegadas. Caberá ao investigador saber aonde encontrá-las e como recolhê-las.

A Lei 12850/2013, ao tratar da infiltração estabeleceu em seu artigo 11º e seguintes os requisitos e o procedimento para a efetivação da infiltração, dispondo que deverá ser demonstrada a necessidade da medida, o alcance das tarefas dos agentes e, quando possível, os nomes ou apelidos das pessoas investigadas e o local da infiltração. Na sequência, mais alguns dispositivos que, basicamente, tratam da proteção ao agente da Lei que executará a atividade, como a possibilidade de interrupção do trabalho no caso de risco para o infiltrado, a preservação da identidade e a possibilidade de recusa.

Todos esses artigos tratam, em evidência, de uma infiltração real, na qual o agente infiltrado vai ingressar na organização criminosa e ficar face à face com os demais membros, visando conquistar-lhes a confiança e obter informações sobre os ilícitos praticados.

No que tange aos crimes cibernéticos, não existem encontros pessoais com os investigados. Os atos são praticados no ciberespaço e muito provavelmente, até mesmo os membros de um mesmo grupo não conhecem a identidade real dos demais envolvidos.

Os criminosos que se dedicam a prática de crimes cibernéticos utilizam diversos mecanismos para esconder sua identidade, no que são auxiliados pela própria estrutura do ciberespaço que exige, para conexão de um ser humano, a utilização de um equipamento, identificado apenas por um número IP[88].

[88] No que concerne as investigações de crimes cibernéticos, normalmente as notícias criminais que aportam nas

Ademais, muitas vezes os membros de um mesmo grupo criminoso não estão próximos geograficamente, podendo estarem espalhados pelos cinco continentes. Assim, a possibilidade de encontros pessoais é extremamente remota e uma sugestão desse tipo, além de não ser usual, levantaria suspeitas e inviabilizaria a investigação.

Portanto, nos crimes cibernéticos, o território em que ocorrerá a infiltração será o ambiente virtual. Corolário lógico será a necessidade de construir um perfil para interação com os demais "atores" somente no ciberespaço.

Considerando que o perfil em questão será cuidadosamente construído para a utilização na investigação e que esse perfil não corresponderá a um ser humano real, ele poderá ser utilizado pela equipe de investigação. De certa forma, essa possibilidade torna a técnica um pouco menos onerosa para os investigadores no que tange a responsabilização pelos atos praticados.

Assim, embora a Lei 12850/2013 não trate especificamente dos crimes cibernéticos, advogamos a possibilidade da utilização do referido diploma legal para autorizar a infiltração digital.

A técnica é plenamente aplicável, por exemplo, nos crimes relacionados à pornografia infantil, nos crimes de racismo, nas fraudes bancárias, entre outros, desde que existe o caráter de transnacionalidade e haja um tratado internacional no qual o Brasil se obriga a reprimir os delitos.

A lei prevê a apresentação de relatório circunstanciado no final do periodo de infiltração. No que tange a infiltração real, esse relatório conterá os elementos colhidos pelo infiltrado, referindo ações dos investigados por ele presenciada, podendo ainda incluir fotos, gravações e informações a serem respaldadas por outras provas documentais, por exemplo, extratos bancários acerca de uma determinada operação financeira.

Entretanto, no âmbito da infiltração virtual o relatório certamente haverá de ser diferente. As atividades do perfil infiltrado, mais do que serem relatadas ao juiz, devem ser passíveis de comprovação.

Assim, para que a infiltração digital produza resultados e possa ser utilizada como prova no processo penal, submetida ao contraditório diferido, indispensável a utilização de ferramentas que possibilitem o registro das atividades no ciberespaço. Existem dezenas de softwares que possuem essas funcionalidades. Entretanto, é muito importante que as ferramentas em questão sejam passiveis de auditoria uma vez que a defesa poderá questionar o conteúdo do relatório de infiltração e solicitar uma perícia no material produzido visando

---

delegacias de polícia, sejam federais sejam estaduais, trazem um esboço de materialidade, que pode ser uma publicação em um site ou um desvio de conta bancária, mas não trazem muitas informações sobre a autoria. Em face disso, a investigação vai seguir o caminho que leva à identificação da autoria delitiva, da pessoa humana atrás do teclado. Para tanto, será necessário fazer o caminho inverso, partindo dos vestígios publicados pelo infrator até o local onde o crime foi praticado, dado que os vestígios conduzirão ao computador ou equipamento utilizado na ação criminosa.

questionar a autenticidade e invalidar a prova.

6. PROJETO DE LEI 100/2010

Conforme tratado nos tópicos anteriores, a legislação atualmente em vigor permite a realização da infiltração como técnica de investigação dos crimes cibernéticos. Entretanto, existe um projeto de Lei sendo discutido no Congresso Nacional que trata especificamente da infiltração para investigação dos crimes relacionados a pornografia infantil. Trata-se do PLS 100/2010[89].

Referido projeto é resultado dos trabalhos da Comissão Parlamentar de Inquérito (CPI) sobre Pedofilia, ou CPI da Pedofilia, que atuou até o ano de 2010 e foi promotora de importantes alterações e adequação dos tipos penais referentes a pornografia infantil pela internet.

O projeto *sub examine* propõe alterar o Estatuto da Criança e do Adolescente (Lei 8.069/1990) para incluir a Seção V-A, destinada a tratar da infiltração de agentes de polícia na internet, com o fim de investigar os crimes previstos nos Arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei 8069/90 e nos Arts. 217-A, 218, 218-A e 218-B do Código Penal.

Mimetizando a Lei 12850/2013, estabelece a necessidade de decisão judicial fundamentada e circunstanciada para a implementação da medida. Ainda em consonância com a Lei em vigor, estabelece como requisito a comprovação da necessidade da medida, dispondo que não será admitida quando a prova puder ser obtida por outros meios.

Permanecem como partes legítimas para a requisição o Delegado de Polícia e o Ministério Público, cabendo aos requisitantes demonstrarem a necessidade da medida e o alcance das tarefas dos policiais.

Pela referida proposta, a infiltração será admissível para investigar os crimes relacionados no Art. 190A[90]. o legislador opta portanto por admitir a medida para

[89] A íntegra do PLS 100/10 está disponível no sítio eletrônico do Senado (http://www.senado.gov.br/atividade/materia/getPDF.asp?t=90127&tp=1. Acesso em: 15 mai. 11.)

[90] Os crimes mencionados no Art. 190A são aqueles prescritos nos artigos 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos Arts. 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Assim, somente nos seguintes casos seria licita: Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente (Art. 240 ECA); Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (Art. 241 ECA); Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (Art. 241-A ECA); Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (Art. 241-B ECA); Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual (Art. 241-C ECA);

Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso (Art. 241-D ECA); Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos (Art. 217-A do Código Penal); Induzir alguém menor de 14 (catorze) anos a satisfazer a lascívia de outrem (Art. 218 do Código Penal); Praticar, na presença de alguém menor de 14 (catorze) anos,

um rol taxativo de delitos (*numerus clausus*), ou seja, sem possibilidade de ampliação para outros delitos. Essa decisão representa uma limitação, especialmente no caso de modificação da legislação para criminalizar outras condutas que ofendam a dignidade sexual de crianças e adolescentes.

O projeto, dispõe ainda, que no requerimento inicial, sendo possível, devem ser informados os nomes ou apelidos das pessoas investigadas, bem como os dados de conexão ou cadastrais que permitam a sua identificação.

Embora seja sobremaneira importante individualizar o máximo possível os investigados, é muito provável, que no início da infiltração esses dados não sejam conhecidos. Normalmente os únicos dados sobre os investigados no que concerne aos crimes cibernéticos são os nomes dos perfis ou nicknames, sendo que o propósito da investigação será justamente identificar os dados de conexão, dados cadastrais e, por fim, chegar a identidade do ser humano por traz do teclado. De modo que essa segunda parte do Inciso I do § 2º do Art. 190-A estaria melhor posicionada e teria mais sentido se estivesse tratando do relatório final.

A proposta tratou de definir o que são dados de conexão e dados cadastrais, considerando o primeiro como sendo informações referentes à hora, à data, ao início, ao término, à duração, ao endereço de Protocolo Internet (IP) utilizado e ao terminal de origem da conexão e segundo as informações referentes ao nome e endereço do assinante ou usuário registrado ou autenticado para a conexão a quem um endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão.

A Lei 12965/2014, também conhecida como Marco Civil da Internet, define registro de conexão como o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados. No mesmo diploma legal também se encontra uma definição para dados cadastrais como sendo aqueles que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. Diante disso, considerando que os textos são praticamente idênticos, melhor seria fazer remição às definições do Marco Civil.

O Art. 190-C trata da proporcionalidade dos atos praticados, alertando que o agente policial infiltrado que deixar de observar a estrita finalidade da investigação responderá pelos excessos praticados. A menção ao princípio da proporcionalidade não é muito comum na legislação pátria. Mesmo a Constituição não faz referência a tal princípio. Entretanto, é pacífico na doutrina que o referido princípio deve imantar todas as ações estatais desenvolvidas durante a persecutio *criminis*.

---

ou induzi-lo a presenciar, conjunção carnal ou outro ato libidinoso, a fim de satisfazer lascívia própria ou de outrem (Art. 218-A do Código Penal); Submeter, induzir ou atrair à prostituição ou outra forma de exploração sexual alguém menor de 18 (dezoito) anos ou que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, facilitá-la, impedir ou dificultar que a abandone (Art. 218-B do Código Penal) (Wendt, 2011).

O projeto de Lei silencia quanto à prática de crimes durante a infiltração. Não existe qualquer menção quanto a responsabilidade penal em face de eventual cometimento de atos ilícitos. Em face disso, durante a infiltração digital não poderá ser perpetrado qualquer ato ilícito pelo infiltrado e, uma vez praticado, será inafastável a responsabilização penal.

Também não há qualquer referência à possibilidade prevista na lei em vigência sobre a recusa na execução da tarefa. Aqui, muito mais do que eventual risco envolvido, entra em cena o equilíbrio psicológico necessário aos executores da medida, pois passarão a exercer uma atividade mentalmente insalubre. Para quem não é portador da desordem de comportamento denominada pedofilia[91] a visualização de pornografia infantil gera repulsa e indignação, além de outros sentimentos negativos que variam de acordo com o subjetivismo de cada ser humano. Assim, o delegado de polícia, coordenador da operação, deverá ficar atento a eventuais alterações na saúde mental dos agentes infiltrados, decidindo pela substituição do policial se o trabalho estiver causando danos ou ainda se houver uma recusa de atuação, inobstante o projeto de lei não tratar da matéria.

Embora a intenção do legislador tenha sido a de possibilitar a realização da infiltração digital através de diploma próprio para os crimes relacionados à pornografia infantil, os novos dispositivos ficam muito aquém da legislação atual, inviabilizando, por exemplo, a prática de ilícitos durante a operação. Da forma como está representa inominável retrocesso em técnica de investigação que já vem sendo utilizada pelas polícias nas operações relativas à pornografia infantil na internet[92].

O parágrafo único do Art. 190-C traz inovação ao dispor que não configura crime a atividade do policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes previstos nos Arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta lei e nos Arts. 217-A, 218, 218-A e 218-B do Código Penal.

Inobstante, topologicamente localizado no âmbito da regulamentação da infiltração cibernética, o dispositivo trata, em verdade, das atividades do agente encoberto e não do agente infiltrado.

Essas figuras, embora próximas, possuem sensíveis diferenças no que tange ao modo de atuação e a sua natureza jurídica. O agente encoberto tem por objetivo a recolha de informações ou de elementos de prova e, ocasionalmente, a verificação da ocorrência do crime (flagrante delito). Não será escopo da atuação

[91] De acordo com Magalhães e outros em artigo denominado "Pedofilia: Informações Médico-Legais para o profissional da saúde", a pedofilia é definida como desordem psicossexual na qual a fantasia ou a própria atividade sexual com crianças pré-púberes é o meio exclusivo ou preferido para a excitação sexual e o alcance da satisfação plena na esfera sexual2 (D). A pedofilia, para o profissional de saúde é uma desordem mental; para o sistema judiciário norte-americano, é um crime3 (B).

[92] A técnica da infiltração nas investigações relacionadas a pornografia infantil já vem sendo utilizada pelas policias brasileiras. Como exemplo bem-sucedido pode ser citada a Operação *DirtNet* levadas a efeito pela Policia Federal.

do agente encoberto ingressar ou fazer parte da organização criminosa, pois atuará mais como observador das condutas praticadas em alguns ambientes virtuais abertos ou públicos, como redes sociais ou fóruns, sem interagir com seus membros. O agente encoberto tem como características fundamentais a absoluta passividade e a inexistência de relações pessoais com os agentes do crime (Valente, 2014, pag. 512).

O agente infiltrado, por sua vez, tem por missão primeira conquistar a confiança dos membros do grupo, para então com eles conviver, eventualmente partilhando da intimidade dos investigados, tudo com o objetivo de amealhar informações relevantes.

Ademais, a atuação de policiais em operações encobertas, ou seja, sem que se identifiquem como policiais, consiste em atividade rotineira das polícias que prescinde de autorização judicial uma vez que não restringe direitos constitucionalmente assegurados, como, por exemplo, a intimidade, o sigilo das comunicações ou a inviolabilidade do domicílio.

Assim, o projeto de lei, ao condicionar esse tipo de atuação a existência de autorização judicial simplesmente por se tratar de um crime cibernético cria uma exigência desarrazoada. A nosso ver, a atividade consiste em simples medida de policia, que integra o poder geral de investigação fulcrado no Código de Processo Penal.[93]

Por fim, no que tange a elaboração do relatório final da infiltração, a questão é melhor enfrentada pelo projeto de lei em exame ao estabelecer que todos os atos eletrônicos praticados durante a operação deverão ser registrados, gravados, armazenados e encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado. Ainda assim, a regulamentação é bastante tímida, pois não trata da problemática da demonstração e verificação de autenticidade do conteúdo interceptado.

7. CONCLUSÃO

A intenção dessas breves linhas, longe de formular conceitos sobre o instituto, consiste em demonstrar que a infiltração digital configura espécie do gênero infiltração, técnica investigativa destinada a produção de prova, estando, portanto, albergada pelos dispositivos da Lei 12850/2013 que tratam da matéria, e, por consequência, legalmente admitida pelo arcabouço processual pátrio.

Nesse sentido, pode ser empregada para investigar crimes cibernéticos, desde que o crime em investigação esteja dentre aqueles cuja repressão o estado brasileiro se comprometeu mediante a assinatura e internalização de tratado internacional.

[93] Mais sobre esse assunto no livro Teordia Geral do Direito Policial de Manuel Monteiro Guedes Valente que traz a interessante definição sobre as medidas puras de policia (2014, pág 192 e seguintes).

A utilização da infiltração para recolha da prova representa mitigação ao princípio do *nemo tenetur se detegere.* Em razão disso, para que seja admissível, deve ser utilizada excepcional e subsidiariamente, para a defesa de bens jurídicos, cuja magnitude justifica a redução do âmbito de incidência da proibição de auto-incriminação. Logo, cabe ao delegado de polícia requerente demonstrar o risco grave ao bem jurídico cuja proteção se pretende, bem como comprovar que as medidas de investigação ordinárias e menos invasivas seriam inócuas.

No que tange ao Projeto de Lei 100/2010, alguns dispositivos trazem instrumentos úteis para as investigações de pornografia infantil, como a possibilidade de registrar a identidade criada para a operação e a exclusão de responsabilidade pela criação do perfil fictício. Entretanto, a ausência de previsão quanto a prática de atos ilícitos e a enumeração dos tipos penais em que a infiltração pode ser utilizada consubstanciam retrocesso ao atual regime jurídico.

De outra parte, a infiltração em investigações de pornografia infantil tem sido realizada com base na Lei 12850/2013, mais ampla do que o projeto em questão. As autorizações judiciais têm merecido a confirmação pelos tribunais superiores, sendo consideradas provas adequadas e legítimas. Assim, a aprovação do projeto tal como se encontra, limitará a utilização da técnica em comento.

O conhecimento empírico acumulado em investigações dessa espécie, especialmente nas investigações relacionadas à pornografia infantil, demonstra que o êxito da infiltração depende da prática de atos ilícitos destinados a tornar convincente o perfil utilizado na apuração, como por exemplo, a posse e compartilhamento de algumas imagens de pornografia infantil. Para tanto, certamente, deverá existir autorização judicial prévia e detalhada, observado o princípio da proporcionalidade, guião a ser seguido pelos agentes do estado durante a *persecutio criminis* para que a investigação se coadune aos ditames do Estado Democrático de Direito.

7. REFERÊNCIAS

ANDRADE, MANUEL DA COSTA. 2013. *Sobre as proibições de prova em processo penal.* Coimbra: Coimbra Editora.

Anselmo, Marcio Adriano. 2015. "Inquérito policial é o mais importante instrumento de obtenção de provas." *Consultor Jurídico.* 4 de Agosto. Acesso em 19 de Dezembro de 2015. http://www.conjur.com.br/2015-ago-04/academia-policia-inquerito-importante-instrumento-obtencao-provas#author.

Cabette, Eduardo Luiz Santos. 2013. "Crime organizado: nova lei 12.850/13 e o problema da conduta dos agentes infiltrados no cometimento de infrações penais." *Migalhas.* 13 de Outubro. Acesso em 19 de Dezembro de 2015.
http://www.migalhas.com.br/dePeso/16,MI188454,91041-Crime+organizado+nova+lei+1285013+e+o+problema+da+conduta+dos+agentes.

Giacomolli, Nereu José. 2015. *O Devido Processo Penal.* São Paulo: Atlas.

Iocca, Erica Cristiane. 2012. "CRIMES CIBERNÉTICOS E A SOCIEDADE ATUAL." *Revista Eletronica da Faculdade de Direito de Nisia Floresta.* Acesso em 18 de Abril de 2015. http://www.ienomat.com.br/revistas/index.php/judicare/article/view/50.

José, Maria Jamile. 2010. "A infiltração policial como meio de investigação de prova nos delitos relacionados à criminalidade organizada." Janeiro. Acesso em 20 de Dezembro de 2015. file:///C:/Users/diana.dcm/Downloads/Infiltracao_policial_Maria_Jamile_Jose.pdf.

Lévy, Pierre. 1999. *Cibercultura.* São Paulo.

Loureiro, Joaquim. 2007. *Agente Infiltrado? Agente Provocador! Reflexões sovre o 1º Acórdão do T.E.D Homem - 9.junho.1998. Condenação do Estado Português.* Coimbra: Almedina.

Magriço, Manuel Eduardo Aires. 2014. *A exploração Sexual de Crianças no Ciberespaço - aquisição e valoração da prova forense de natureza digital.* Lisboa: E-Ditar.com.

Oneto, Isabel. 2015. *O Agente Infiltrado. Contributo para a Compreensão do Regime Jurídico das Acções Encobertas.* Coimbra: Coimbra Editora.

Pereira, Eliomar da Silva. 2010. *Teoria da Investigação Criminal.* São Paulo: Almedina.

Pereira, Eliomar da Silva, e Emerson Silva Barbosa. 2015. *Organizações Criminosas. Teoria e Hermeneutica da Lei nº 12850/2013.* Porto Alegre: Nuria Fabris Editora.

Sousa, Stenio Santos. 2015. *Investigação Criminal Cibernética. Por uma Politica Criminal de Proteção à Criança e ao Adolescente na Internet.* Porto Alegre: Nuria Fabris Editora.

Valente, Manuel Monteiro Guedes. 2014. *Teoria Geral do Direito Policial.* Coimbra: Almedina.

Valente, Manuel Monteiro Guedes, Geraldo Prado, Nereu José Giacomolli, e Edison Damas da Siveira. 2015. *Prova Penal. Estado Democrático de Direito.* : Rei dos Livros.

Wendt, Emerson. 2011. "Infiltração de agentes policiais na internet nos casos de 'pedofilia'." *Portal Nacional dos Delegados.* 19 de maio. Acesso em 09 de janeiro de 2016. http://www.delegados.com.br/noticias/infiltracao-de-agentes-policiais-na-internet-nos-casos-de-pedofilia.

Wendt, Emerson, e Higor Vinicius Nogueira Jorge. 2012. *Crimes Cibernéticos: Ameaças a Procedimentos e Investigação.* São Paulo: Brasport Livros e Multimidia Ltda.

Capítulo IX

Utilização de fontes abertas na investigação policial

Alesandro Gonçalves Barreto[94]

1. INTRODUÇÃO

Na atividade policial prevalece a cultura de valorizar a informação obtida secretamente. Nesse contexto, só tem validade o que se obtém de um informante, de uma testemunha ocular ou de uma interceptação telemática, menoscabando-se, pois, o que se encontra disponível, principalmente na internet.

É importante analisar esse quadro, aferindo as milhares de fontes disponíveis e a suas contribuições na investigação, trazendo dados úteis, necessários e pontuais e, principalmente, auxiliando o investigador a "não perder tempo com o que está disponível".

2.FONTES ABERTAS

2.1 Definição

A definição de fonte segundo o dicionário Michaellis, dentre os vários significados, é a causa, origem e princípio.

BARRETO e WENDT (2013) definem fontes abertas como:

> Qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimentos e ou provas admitidas em direito, tanto em processos cíveis quanto em

[94] Delegado de Polícia Civil do Estado do Piauí. Pós-graduado em Direito pela Universidade Federal do Piauí. Atualmente é Diretor da Unidade do Subsistema de Inteligência da Secretaria de Segurança Pública do Estado do Piauí. Coautor da obra Inteligência Digital, Editora Brasport. Integrou o Grupo de Trabalho que revisou a Doutrina Nacional de Inteligência de Segurança Pública. Professor na Academia de Polícia Civil do Piauí e professor convidado das Escolas de Magistratura do Mato Grosso, Paraíba e Bahia. Colaborador eventual e Coordenador do NUFA – Núcleo de Fontes Abertas da Secretaria Extraordinária para Segurança de Grandes Eventos do Ministério da Justiça durante a Olimpíada do Rio de Janeiro em 2016.

processos penais e, ainda, em processos trabalhistas e administrativos (relativos a servidores públicos federais, estaduais e municipais).

CEPIK (2003) ao ressaltar o papel da atividade de inteligência na coleta de dados através de fontes abertas pontuou OSINT[95] como[96]:

> "Obtenção legal de documentos oficiais sem restrição de segurança, da observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento de mídia (jornais, rádio e televisão), da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido sem restrições especiais de segurança".

A DNISP[97], ao tratar de fontes de dados de Inteligência de Segurança Pública, elenca em fontes abertas e fechadas. A primeira definida como aquela cujo dado é de livre acesso. Já a segunda, o dado é protegido (necessidade de credenciamento para o acesso) ou negado (necessidade de operação de busca para sua obtenção).

O FBI[98] define OSINT como "uma ampla gama de informações e fontes amplamente disponíveis, incluindo as obtidas através da mídia (jornal, rádio, televisão), profissional e de arquivos acadêmicos e de dados públicos".

De acordo com as definições acima, vimos que o conteúdo disponível em fontes abertas não exige nenhuma espécie de restrição de acesso. Diferentemente das fechadas em que há a necessidade de login e acesso, as abertas encontram-se acessíveis a todo instante.

A utilização de fontes abertas tem sido mais direcionada à produção de conhecimentos na atividade de inteligência do que na investigação policial. Apesar de ainda não estar sistematizada, a polícia tem utilizado redes sociais e aplicativos gratuitos para pontencializar, principalmente, a realização de denúncias anônimas ou acompanhar eventos relacionados a torcidas organizadas ou postagens de facções criminosas. A análise desse conteúdo tem permitido a individualização de autoria e materialidade delitivas, possibilitando identificar autores que até então se julgavam inatingíveis por estarem postando conteúdo na web.

Há vários julgados que citam o uso de fontes abertas como agregador na investigação policial[99].

---

[95] Open Source Intelligence ou Inteligência de Fontes Abertas

[96] CEPIK, Marco.

[97] Doutrina Nacional de Inteligência de Segurança Pública. Prevista na Resolução nº 1, de 15 de Julho de 2009. É elemento constituinte do Subsistema de Inteligência de Segurança Pública.

[98] FBI - Federal Bureau of Investigation. Intelligence Collection Disciplines.

[99] STF - INQUÉRITO **: Inq 3563 PR**; TRE-RJ - RECURSO EM REPRESENTAÇÃO : **R-Rp 378290 RJ**; TJ-MS - Apelação Cível : **AC 6424 MS 2012.006424-5**.

2.2 Histórico

A história das fontes abertas teve início com a sua aplicação na área da inteligência voltada à produção de conhecimento. Em meados de 1939, o governo britânico determinou à BBC que criasse um serviço que pudesse monitorar jornais impressos e serviços de rádio difusão eis que, em plena Segunda Guerra Mundial, informações de grande utilidade poderiam ser recolhidas em fontes abertas.

Com a Guerra Fria, os serviços de inteligência passaram a valorizar ainda mais esse conteúdo que estava disponível. Um exemplo claro disso era o que e STASI[100] examinava por mês[101]: 1.000 (um mil) revista ocidentais e 100 (cem) livros e, diariamente, 12(doze) horas de rádio da Alemanha Oriental.

Após os ataques terroristas de 11 de setembro de 2001 nos Estados Unidos, o governo americano criou uma agência com a função de coletar em fontes abertas informações sobre política econômica, militar e externa de todas as partes do planeta.

Atualmente vários órgãos de inteligência e departamentos de polícia estão criando e capacitando servidores para buscarem esses dados disponíveis.

2.3 Classificação

Os dados ou informações de acesso livre podem ser encontrados nos mais variados meios: comunicação, livros, internet, softwares e principalmente potencializados pela internet. Não podemos confundir fontes abertas e seu uso apenas com o que está na web, mas não há dúvida de que a progressão geométrica de dados tem direcionado a coleta para este cenário.

Podem ser obtidas através da:

- Mídia: jornal, revista e televisão;
- Portais governamentais: transparência pública, diários oficiais, dados populacionais, economia, política, legislação, etc...
- Acadêmicos: artigos publicados, conferências, trabalhos;
- Softwares e hardwares;
- Mídias sociais: redes sociais, sites de compartilhamento, aplicações de vídeos, blogs e microblogs.

Em que pese a busca por dados de fontes abertas poder ser realizada através de inúmeros meios, manteremos o foco na utilização da internet como um caminho a ser seguido pela investigação policial. É importante frisar ainda que os documentos encontrados não estão na internet, mas são encontrados em computadores interligados com ela.

[100] Polícia Secreta da Alemanha Oriental. Sediada na Berlim Oriental, tinha uma vasta rede de informantes que espionavam praticamente toda população.

[101] Journal of U.S. Intelligence Studies. The Evolution of Open Source Intelligence.

2.4 Utilização pelo Poder Judiciário

Tem sido cada vez mais comum a utilização de fontes abertas no âmbito policial como também no Poder Judiciário. É o caso, por exemplo, de aplicativos de comunicação gratuitos utilizados para noticiar a ocorrência de atos processuais.

Em uma Reclamação Trabalhista nº 0002736-51.2013.5.08.0110, que tramitou na 1ª Vara do Trabalho de Tucuruí-PA, a Representante do Ministério Público do Trabalho pugnou pela intimação da parte, residente no Suriname, por meio do aplicativo de mensagens WhatsApp visando atender os princípios da instrumentalidade e da celeridade das formas. Na sentença, o magistrado determinou que a intimação da sentença fosse realizada pelo celular do oficial de justiça através do referido aplicativo[102].

O juiz federal Ali Mazloum da 7ª Vara Criminal da Justiça Federal de São Paulo expediu a Portaria 012/15 estabeleceu que a possibilidade de se realizar a comunicação de atos processuais por qualquer meio idôneo e, para tanto disponibilizou o WhatsApp ao público em geral, partes, defensores, procuradores e testemunhas. Determinou à Secretaria da Vara que ficasse responsável pelo cadastramento de advogados interessados e que assegurasse através do app os agendamentos de visitas para "consulta de autos, audiência com o juiz, retiradas de certidões e alvarás e lembretes de audiências.

Fato semelhante também fora estabelecido na comarca de Piracanjuba-GO, onde o juiz e o Presidente da Subseção da Ordem dos Advogados do Brasil, assinaram uma portaria conjunta estabelecendo a multiplataforma WhatsApp para a realização de intimações. A adesão é voluntária e depende de cadastro prévio do interessado, estabelecendo que a confirmação do recebimento deva ser feita por texto escrito.

O uso do Skype como ferramenta numa audiência que tramitou na Vara de Família e Sucessões na comarca de São José dos Campos-SP[103] onde foi possível dar andamento a uma ação de guarda e regulamentação de visita que aguardava desde o ano de 2010. Nada impede, por exemplo, que a polícia utilize esse software para colher o depoimento de uma testemunha em outra circunscrição distante do local de apuração do fato.

3 UTILIZAÇÃO DAS FONTES ABERTAS NA INVESTIGAÇÃO POLICIAL

A evolução tecnológica tem possibilitando a diversificação das condutas criminosas. A polícia tem encontrado cada vez mais dificuldades na apuração dos crimes, desde a descoberta de evidência até a localização de testemunhas. Enquanto, isso a internet potencializa-se como um imenso banco de dados gratuito e disponível.

[102] 1ª Vara do Trabalho de Tucurui-PA. Proc nº: 0002736-51.2013.5.08.0110.
[103] Conselho Nacional de Justiça. Tribunal realiza audiência em processo de Família via Skype.

Inúmeras vantagens advêm da utilização da internet como agregador de informações:

- Identificação de suspeitos, redes de relacionamento e locais que frequenta rapidamente;
- Menor exposição do policial durante a realização da investigação;
- Obtenção de informação de forma mais ágil do que outras técnicas investigativas;
- Informação disponível e acessível, sem necessidade de ordem judicial.
- Inquéritos policiais ricos em elementos que contribuem para individualização da autoria e materialidade delitiva.

A investigação policial não deve ficar adstrita a depoimentos e exames periciais. Deve explorar também o uso de fontes abertas, principalmente de mídias sociais, para dar uma maior celeridade ao procedimento investigativo, possibilitando ao investigador respostas rápidas e precisas.

Assim, quando as informações já estiverem disponíveis em determinada aplicação de internet[104], não há necessidade de burocratizar a busca através de expedição de um ofício que, por vezes, sequer é respondido ou, sendo otimista, requer um lapso de tempo prejudicial à persecução penal. Imagine-se o tempo transcorrido para se obter a informação, por exemplo, se o investigado recebe o benefício da bolsa família[105] ou se é servidor de ente da federação. Logo de início haveria a dúvida para saber a quem enviar, como solicitar e quanto tempo demoraria a resposta. Para essas duas situações basta a simples consulta, no primeiro caso, ao Portal da Transparência do Governo Federal[1], e, no segundo caso, dentro da relação de servidores do ente em que está vinculado.

É muito importante que, ao consultar determinada informação na internet, o policial deve levar em conta alguns aspectos, dentre os quais a qualidade e a relevância da informação. A internet é "território livre", onde as pessoas postam ou escrevem assuntos que não são verdadeiros e não devem ser levados em conta nessa coleta. Deve, para tanto, saber distinguir informação de boato.

A fim de que a coleta seja útil à investigação o policial deve:

a) **Filtrar conteúdo**: é importante que haja precisão no termo a ser pesquisado, devendo ser claro e preciso sobre o que se busca. Essa coleta feita corretamente auxilia a análise posterior do conteúdo que, deveras, possa ser relevante para a investigação.

[104] O conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet.

[105] No Portal da Transparência do Governo Federal, disponível em http://www.portaldatransparencia.gov.br/, é possível a consulta, em formato aberto, das transferências de recursos federais diretamente repassados a cidadãos, referentes ao pagamento da Bolsa Família, realizadas pelo Ministério do Desenvolvimento Social, por meio da Caixa Econômica Federal.

b) **Utilização correta do motor de busca e da aplicação de internet**: recomenda-se o uso de buscadores conhecidos a fim de que se obtenha resultados mais precisos. Os buscadores mais famosos são o Google e o Bing. O investigador deve utilizar filtros a fim de que a procura na web seja refinada e retornem como resultado as melhores respostas. O uso de aspas, por exemplos, traz apenas resultados específicos para um assunto pesquisado. Nas demais aplicações de internet deve-se levar em conta a sua estruturação com informações sobre quem hospeda o conteúdo, referências sobre a página além do respectivo domínio (.gov, .com., .edu, .net).A busca deve levar ainda em conta quem foi o responsável por escrever o conteúdo e se ele tinha qualificação para tal, a saber: direitos autorais, se é informação de serviço público ou privado, período de postagem e revisão.
c) **Preservar o conteúdo recolhido**: uma característica marcante é sua volatilidade. Quando se tratar de evidência eletrônica ou até mesmo de um dado útil à investigação, a polícia deve agir rapidamente a fim de preservar a cadeia de custódia deste conteúdo.
d) **Softwares para coleta e análise de dados**: em razão do volume de conteúdo ser imensurável, há a necessidade de programas capazes de coletar milhares de informações e fazer uma análise adequada do assunto ou tema averiguado. Há ferramentas gratuitas que permitem o monitoramento de mídias sociais em tempo real, acompanhando dados e estatisticas de postagens por toda a internet. Outras ferramentas pagas permitem recursos que otimizam ainda mais a busca.
e) **Relatório de Missão Policial:** a coleta de dados em fontes abertas deve ser formalizada através de relatório de missão policial. Para tanto, o investigador deverá fazer o relato do conteúdo pesquisado, metodologia utilizada, data e hora da coleta e referências utilizadas com as urls nas quais o conteúdo se encontra disponível[106].

3.1 Aspectos Legais da Utilização das Fontes Abertas

A coleta de conteúdo em portais públicos ou em redes sociais de perfis abertos não gera nenhum questionamento. O problema surge a partir do momento em que a polícia obtém esse material, a título de exemplo, em perfis fechados de redes sociais.

Em razão da matéria ainda ser nova, não há manifestação do Poder Judiciário sobre os aspectos legais da utilização de fontes abertas na investigação criminal levando em consideração questões de confiabilidade do conteúdo disponibilizado bem como dos aspectos atinentes à privacidade do usuário de internet.

A Constituição Federal assegura o direito à privacidade como um direito fundamental da personalidade. Essa privacidade é protegida por interesse social e não individual.

[106] Modelo disponibilizado no anexo.

Ao criar um perfil em redes sociais tem-se a opção de não divulgar seus dados ou imagens, entretanto, essa escolha termina por inviabilizar sua interação com os demais. Em razão disso, terminam por dispor de sua privacidade, disponibilizando conteúdo na web.

As relações pessoais estão sendo modificadas com o advento das redes sociais. Os indivíduos expõem-se a todo custo, postando informações de caráter íntimo sem nenhuma preocupação com sua privacidade. Os sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual[107]. Se a demandante expõe sua imagem em cenário público, não é ilícita ou indevida sua reprodução pela imprensa, uma vez que a proteção à privacidade encontra limite na própria exposição realizada[108]. Essa exposição pública do indivíduo funciona, portanto, como um limitador de privacidade.

Ao analisar a legalidade sobre a coleta de informações de uma conta de Facebook fechada de um investigado através de um perfil de uma testemunha que fazia parte de sua rede de amigos e se dispôs auxiliar à polícia, revelando conteúdos incriminadores nas postagens, o Tribunal Distrital de New York[109] decidiu que " a expectativa de privacidade do indivíduo acabou a partir do momento em que este difundiu o conteúdo para seus amigos, estes eram livres para usar a informação, inclusive compartilhar com o governo"

Em que pese a decisão do tribunal estadunidense, a privacidade do usuário não foi respeitada. Quando alguém posta algo em um perfil fechado para determinada quantidade de usuários restritos, gera consigo a expectativa de privacidade de acessibilidade daquela informação. As políticas de privacidade das aplicações de internet permitem ao sujeito o autogerenciamento de sua privacidade, podendo, para tanto, dispor quem poderá ter acesso ao seu conteúdo[110]. O fato do perfil ser fechado necessita de ordem judicial para se ter acesso.

Não há, portanto, nenhum óbice na utilização de informações postadas na internet quando a Polícia Judiciária acosta ao procedimento administrativo fotos, vídeos ou textos postados por determinado indivíduo em perfis abertos. *Permissa Vênia*, não há a proteção constitucional da privacidade quando esse conteúdo é postado em uma rede social. Quem posta o conteúdo de forma livre na web precisa entender que não está colocando informações em um diário privado e sim para todo mundo.

Nas questões atinentes à confiabilidade não há nenhum problema quando o dado é postado em um portal público. A problemática surge quando o conteúdo é

[107] Tribunal Superior do Trabalho RR - 61300-23.2000.5.10.0013 , Relator Ministro: João Oreste Dalazen.
[108] STJ REsp 595600 / SC; RECURSO ESPECIAL; 2003/0177033-2.
[109] The United States District Court For The Southern District Of New York. U.S. vs. Joshua Meregildo.
[110] Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem. STJ REsp 1168547 / RJ RECURSO ESPECIAL 2007/0252908-3.

postado por indivíduos desconhecidos ou incertos, gerando dúvidas sobre a sua independência e imparcialidade. Cabe, portanto, ao policial fazer a coleta de forma cautelosa a fim de amealhar apenas informações oriundas de fontes confiáveis.

3.2 Procedimento Policial na Coleta de Dados

Ultrapassados os questionamentos sobre a legalidade da coleta de informações em fontes abertas, adentraremos nos aspectos práticos da busca desses dados disponíveis. Há diversos caminhos que a polícia deve percorrer.

3.3.1 Informações Disponíveis em mídias sociais de criminosos e vítimas.

As mídias sociais revolucionaram a forma de agir entre as pessoas no século 21, independentemente da idade de quem as utiliza. No ano de 2014, atingimos mais de 95 milhões de usuários de internet no Brasil[111]. Nesse contexto, o usuário disponibiliza informações sobre si em mídias sociais, agrupando-se de acordo com seus interesses e afinidades. Com uma velocidade imensurável na sua transmissão, há uma imensa quantidade de usuários e de informações possíveis de serem consultadas e analisadas.

Essa nova forma de interação do usuário tem possibilitado informação e acompanhamento em tempo real de eventos de interesse da atividade policial.

Sua utilização deve ter os seguintes direcionamentos:

a) Aproximação com a comunidade e divulgação das atividades desenvolvidas pelo aparato da segurança em prol da comunidade;
b) Divulgação de políticas de prevenção e repressão ao crime;
c) Difusão de retrato falado e foragidos;
d) Recebimento de denúncia sobre a prática de delitos.
e) Coleta de Evidências: postagens, fotografias, vídeos bem como nos casos em que as mídias sociais são utilizadas para a facilitação ou a organização de crimes e criminosos.
f) Identificação de potencias problemas relativos à segurança da comunidade quando da realização dos protestos.

O conteúdo de mídias sociais pode ser encontrado em:

- Redes Sociais: Facebook, Instagram
- Sites de Vídeos: Youtube, Vimeo
- Sites de compartilhamento de imagens;
- Blogs e Microblogs: Twitter

Em 2014, a IACP - Associação Internacional dos Chefes de Polícia - realizou uma pesquisa[112] sobre a utilização de mídias sociais por agências da lei nos Estados Unidos e concluiu que 82,3% delas fazem uso para investigação

[111] Teleco. Usuários de Internet no Brasil.
[112] IACP Social Media. 2014 Social Media Survey Results.

policial. Em 77,5%, as informações extraídas ajudaram na solução de crimes. Ainda de acordo com a pesquisa, as mídias sociais mais utilizadas por essas agências são: Facebook (95,4%), Twitter (66,4%) e Youtube (38.5%).

Em pesquisa realizada pela LexisNexis[113], no ano de 2014, sobre como os policiais utilizam as mídias sociais em sua atividade, chegou-se a conclusão que em 52% das agências pesquisadas ainda não utilizam nenhum procedimento formal na utilização voltada para a investigação policial. Cerca de 75% dos policiais aprendem sozinhos a utilização de ferramentas e 46% utilizam-se de conhecimento pessoal para tal.

A polícia deve possuir equipes especializadas na coleta de informações em mídias sociais eis que a sua utilização ocorre tanto por cidadão quanto por criminosos. Estes compartilham informações pessoais sobre si e suas atividades mesmo sabendo que podem ser identificados pela polícia. É o que ocorre, por exemplo, nos integrantes de gangues e torcidas organizadas marcando confrontos (data, hora e local, previamente estabelecidos), criminosos postando armas e o proveito do ilícito, além de ostentação com o dinheiro público.

Além do mais, a imensa quantidade de dados postada a cada instante necessita de softwares especializados na sua busca, coleta e análise. Não há como fazer esse apanhado de forma manual. O tratamento adequado possibilita a polícia ter dados confiáveis e significativos direcionados ao trabalho policial.

Um bom exemplo de utilização de mídias sociais é o realizado pela polícia de Toronto[114], Canadá. Eles têm se especializado na coleta e análise de uma imensa massa de dados produzida nesse ambiente, fazendo o acompanhamento sobre as manifestações de massa utilizando esses elementos como ferramenta de resposta aos incidentes que envolvam a segurança pública.

Há vários casos de sucesso na utilização de mídias sociais no auxílio da investigação policial. Após assaltar uma joalheria no ano de 2011[115], subtraindo uma pequena fortuna, um homem foi preso dois anos depois após utilizar uma rede social para postar fotografias de suas férias.

Na Índia, um homem de 47 anos foi preso enquanto tentava vender seu neto pelo Facebook[116]. Em Oklahoma[117], Estados Unidos, uma mulher foi presa ao tentar vender seu filho de dois anos pela quantia de mil dólares para pagar a fiança de seu namorado preso.

3.3.2 Coleta de Elementos Informativos

A internet tem sido uma importante ferramenta na coleta de evidências criminosas. Da mesma forma que qualquer internauta, o criminoso também

[113] LexisNexis. Social Meida use in Law Enforcement.
[114] Toronto Police Service Social Engagement Guidelines..
[115] Daily Mail. Diamond thief who stole jewels worth £80,000 was caught by police after posting holiday pictures on Facebook while on the run.
[116] Mirror. Okla. Indian man arrested for trying to sell his grandson on Facebook.
[117] CBS News. Woman try to sell children on Facebook to get bail money for boyfriend, police say.

utiliza as redes sociais para cometer delitos ou até mesmo para ostentar o produto do crime após a prática da infração penal. Em alguns casos, vídeos e imagens de ações criminosas são divulgadas em aplicativos de comunicação.

A busca de elementos investigativos que contribuam na individualização da autoria e materialidade delitivas pode ocorrer em várias situações:

1. Crimes contra a honra - A falsa ideia de que a internet é um território livre e impune tem potencializado esse tipo de conduta. Os criminosos utilizam-se da tecnologia para potencializar suas ações. Como é cediço, em delitos contra a honra o conteúdo é postado e difundido pela rede, cabendo a polícia coletá-lo da forma adequada e ágil a fim de preservar a cadeia de custódia.
2. Quando alguém pratica, por exemplo, um crime de difamação através de uma rede social, cabe à polícia a preservação desse conteúdo. Recomenda-se a lavratura de certidão de escrivão de polícia, em razão do mesmo possuir fé pública, fazendo constar sob quais circunstâncias o conteúdo se encontra postado (url, captura de arquivo, narração resumida do delito). Em casos de pornografia de vingança, quando se tratar de difusão de conteúdo adulto de natureza íntima, crime tipificado como injúria e difamação, o policial além de preservar o material difundido na internet, poderá proceder para a retirada do conteúdo dos provedores de aplicação de internet bem como solicitar a desindexação dos principais buscadores. O revenge porn de conteúdo referente à criança e adolescente é tipificado no Art. 241-A[118] do Estatuto da Criança e do Adolescente. O procedimento para exclusão dessas imagens íntimas sem autorização pode ser encontrado no app GRP contra Vingança Pornô[119].
3. Imagens e Vídeos de Suspeitos, Vítimas, Testemunhas e Divulgação de Vídeos de CFTV- A busca de imagens e vídeos na web auxilia a polícia na coleta de: fotografias atualizadas, hábitos, locais frequentados, tendências de comportamento e redes de relacionamentos (amigos, parentes, relacionamentos amorosos,

[118] Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008).

[119] Aplicativo disponível na Play Store. Disponibiliza uma coleção detalhada de procedimentos e outras orientações, com foco especial na exclusão de conteúdo íntimo divulgado em redes sociais e sites diversos. Ainda podem ser encontradas dicas de como evitar ser vítima. Legislação relacionada ao assunto e outros conteúdos jurídicos, além de suporte para contato.

O app é um esforço conjunto de profissionais da Segurança Pública e outros de área jurídica que, ao longo de suas carreiras, tem ajudado vítimas de apedrejamento virtual (vingança pornô).

A aplicação tem caráter gratuito e destina a prestar orientação às vítimas na tomada de procedimentos que lhes permita minimizar os danos a que estão sujeitas. Disponível em https://play.google.com/store/apps/details?id=xdk.intel.blank.ad.template23&hl=pt-BR.

ambiente de trabalho).

A divulgação de fotografias de foragidos em redes sociais pode facilitar a localização dos suspeitos. Algumas polícias já usam da funcionalidade em seus perfis eis que sua maior vantagem é a disseminação daquela informação de forma viral, através de compartilhamentos de terceiros.

A polícia de Frankfurt[120] na Alemanha tem utilizado as redes sociais com bastante êxito em investigações policiais. Numa morte ocorrida em decorrência de uma briga em frente a uma boate, a polícia postou as imagens retiradas do circuito interno de tv no intuito de que usuários identificassem as testemunhas presentes naquele local de crime.

O voluntarismo em redes sociais deve, no entanto, ser visto com a devida precaução. Após o atentado ocorrido na maratona de Boston[121], nos Estados Unidos, o FBI solicitou que a população cooperasse postando fotografias realizadas durante a maratona, bem como imagens de pessoas com mochilas pretas nas costas com o intuito de localizar os responsáveis pelo ato. Esse pedido causou uma tremenda confusão onde usuários do Reddit, um agregador de links, passaram a analisar as imagens divulgadas. O resultado disso foram acusações infundadas e uma grande confusão, onde um estudante universitário foi apontado erroneamente como autor do atentado.

No caso de fotografias, quando uma imagem é postada na internet ela carrega consigo metadados que podem ser úteis na apuração do fato. É o exif da imagem que possui informações técnicas sobre as condições de sua captura, podendo incluir, em algumas situações o modelo da câmera utilizada, data, hora e as respectivas coordenadas GPS. A leitura desses dados pode ser feita através de leitores de exif gratuitos disponíveis na internet.

Além da análise dos metadados, o policial deverá usar recursos disponibilizados em alguns buscadores para encontrar imagens semelhantes. No caso de encontrar o arquivo no Google Imagens, deverá arrastá-lo para a barra de pesquisas a fim de verificar se há imagens identicas aquela publicadas em outro local da internet.

3.3.2.1 Preservação da Evidência Eletrônica

A evolução tecnológica tem exigido da polícia uma nova postura na investigação policial. Os delitos tem cada vez mais utilizado a internet como meio para a prática delitiva. O local do crime deixa de ser real e passa a virtual dando a evidência criminosa a característica volátil. Para tanto, a polícia deve agir rapidamente através de solicitação de preservação de conteúdo ao provedor de conexão e/ou aplicação de internet ou extrair o conteúdo através de certidão policial.

- A certidão lavrada por escrivão de polícia é o meio hábil para preservar

[120] WÜNSCH, Silke DW.com. German Police use Web 2.0 to catch criminals.

[121] MONTGOMERY, David; HORWITZ, Sari and FISHER, Marc. The Washington Post. Police, citizens and technology factor into Boston bombing probe.

um conteúdo criminoso postado na internet. Por ter fé publica, há uma presunção de verdade no que foi relatado. Um simples printscreen não possui nenhum valor probatório eis que poderá ser editado por um terceiro.

- Ao expedir o documento, o escrivão deverá constar o caminho percorrido com a metodologia adotada bem como: data e horário do acesso; url na qual o conteúdo se encontra; printscreen das imagens e, transcrição de conteúdo, caso seja áudio ou vídeo, deverá salvar em mídia óptica.
- Dessa forma, quando se tratar de conteúdo criminoso, recomenda-se que, ao confeccionar o relatório de missão, o policial deverá juntar essa certidão policial a fim de que não haja questionamentos futuros.
- Algumas aplicações de internet permitem à autoridade policial à solicitação online de preservação de conteúdo como é o caso do Facebook Records[122]. O salvamento da página web como arquivo possibilita a colheita correta dessa evidência.
- Outra forma de guarda do conteúdo é feita através de ofício extrajudicial da autoridade policial com esteio no Marco Civil da Internet, solicitando a preservação dos registros de conexão bem como os de acesso à aplicações de internet.

3.3.3 Recebimento de Denúncias

O incremento dos aplicativos de troca de mensagens de vídeos e fotografias tem sido uma ferramenta bem utilizada pela polícia no recebimento de denúncias. A ideia central é possibilitar ao cidadão um canal de comunicação que permita o envio de informações que possam contribuir na elucidação de crimes.

E algumas situações, a utilização de aplicativos tem sido importante para a difusão instantânea da ocorrência, divulgação de imagens e a prisão dos autores ainda em flagrante delito[123].

O recebimento de denúncias nessa modalidade não evita que informações falsas sejam repassadas à polícia. O conteúdo recebido deverá ser analisado e confrontado com outros elementos colhidos no decorrer da investigação.

3.2.4 Fiscalização e Acompanhamento de Recursos Públicos

A lei de Acesso à Informação Pública, sancionada em 2011, constitui um marco ao democratizar a informação assegurando o direito fundamental ao seu

[122] Plataforma Law Enforcement Online, disponível em www.facebook.**com**/records permite a preservação de perfis e dados cadastrais de uma conta no Facebook ou no Instagram.

[123] Carlos Dorileo**.** Vítima informa roubo por WhatsApp e PM prende bandidos em clínica de Cuiabá. Rafaela Gonçalves. Jornal Cruzeiro. Grávida é agredida pelo marido e pede ajuda por Whatsapp**.**

acesso. As diretrizes a serem seguidas por ela compreendem:

a) Observância da publicidade com preceito geral e sigilo como exceção;
b) Divulgação de informações de interesse público;
c) Utilização de meios de comunicação viabilizados pela tecnologia da informação;
d) Fomento ao desenvolvimento da cultura da transparência na administração pública;
e) Desenvolvimento do controle social da administração pública.

Dessa forma, a moderna legislação garante, de forma transparente, acesso à informação mediante procedimentos objetivos e ágeis. Essa disponibilidade de conteúdo por parte dos entes federativos e demais órgãos possibilita uma maior agilidade durante uma investigação policial, com informações completas, atuais e acessíveis sobre determinado fato em apuração. Os dados que, até então já eram de boa monta, passam a ter uma maior qualidade e quantidade.

Esses dados públicos podem estar acessíveis em:

a) **Portais de Transparência**: detalhamento de despesas, empenho e pagamentos, transferência de recursos e gastos diretos; repasse de convênios; empresas e pessoas físicas sancionadas, Entidadades Privadas sem Fins Lucrativos; relações de servidores públicos, bolsa família e auxílio pescador, além de outras consultas disponíveis.
b) **Portal de Convênios**: cadastro do ente e de entidade; cotação prévia de preços; consultas de propostas, convênios e pré-convênios; banco de projetos disponibilizados e consulta de entidades privadas sem fins lucrativos aptas.
c) **Portal de Compras do Governo Federal**: placar das licitações em andamento; consulta de atas, catálogo de materiais, certidão negativa, contratos, cotação eletrônica, licitações, pregões, etc...
d) O investigador deve utilizar-se ainda de inúmeras outras ferramentas disponíveis que possibilitam o acompanhamento sobre como o dinheiro público está sendo gasto.

2.2.5 Localização de Foragidos e Cumprimento de Mandado de Prisão

O Art. 13 do Código de Processo Penal determina como incumbência da autoridade policial o cumprimento de mandados de prisão expedidos pelas autoridades judiciárias. Por vezes, a prisão cumprida, pode ser esclarecedora para a investigação em andamento, trazendo novos elementos informativos para o inquérito policial.

Mesmo sendo procurado pela polícia, o criminoso necessita manter contato com pessoas próximas do seu ciclo de relacionamento, independentemente da

reiteração ou não da prática de ilícitos. De alguma forma, poderá postar conteúdo na internet. Cabe a polícia encontrá-lo.

Em casos de homicídio, por exemplo, quando o autor não possui nenhum antecedente, normalmente, há seu "relaxamento" com o passar do tempo. Mesmo fugindo para outros estados, passa a se relacionar com pessoas próximas através de redes sociais. Nessa situação, o policial deverá fazer uma busca minuciosa sobre perfis de indivíduos próximos ao foragido a fim de localizar informações que possam levar ao seu paradeiro. Nos casos dos indivíduos com antecedentes criminais já há uma maior precaução por parte destes e, apesar de utilizarem redes sociais ou outras aplicações de internet para manterem algum contato com seu ciclo, utilizam-se de *fakes* para evitar sua prisão.

3.3.5.1 Uso de Alertas em Serviços de Busca

Os serviços de busca na internet são de grande utilidade no fornecimento de informações sobre vítima, testemunhas, acusado, etc... A utilização de filtros nessa busca traz um melhor resultado, por exemplo, a busca por nome de um foragido, desde que não seja comum e colocado entre aspas, traz só resultados específicos sobre aquele termo.

Um policial que quer lograr êxito na coleta de informações através de fontes abertas deve ter em mente que a internet deve trabalhar a seu favor. É nesse sentido que surgem os alertas, serviços que permite ao interessado cadastrar um determinado termo e receber os resultados diretamente em seu e-mail, com a frequência programada.

Não há necessidade, portanto, de se fazer a busca todos os dias por determinado foragido, basta apenas criar um alerta e aguardar. Há casos conhecidos em que policiais colocam nomes de foragidos nos serviços de alertas e tem conseguido cumprir mandados de prisão em outros estados da federação face as notícias veiculadas em portais.

Os serviços mais conhecidos são o Google Alerts[124] e o TalkWalker Alertas[125].

3.3.5.2 Banco Nacional de Mandados de Prisão

O Banco Nacional de Mandados de Prisão foi regulamento pelo Conselho Nacional de Justiça126, órgão estratégico e central do sistema judicial. Dentre as finalidades do banco de mandados de prisão, tem-se a sua ampla difusão para o conhecimento de qualquer pessoa sem necessidade de prévio cadastro e o seu cumprimento por parte das autoridades policiais.

A consulta ao banco de mandados pode ser efetuada através do portal do CNJ

[124] Disponível em https://www.google.com.br/alerts.
[125] Disponível em http://www.talkwalker.com/alerts.
[126] Resolução 137, de 13 de Julho de 2011 do Conselho Nacional de Justiça.

na url http://www.cnj.jus.br/bnmp. Caso o mandado esteja vigente é possível gerar uma certidão de validade.

Da mesma forma que a polícia utiliza essas informações disponíveis sobre mandados de prisão, os criminosos também acessam a esse conteúdo para checar se existe algo expedido em seu desfavor. Em situações em que a investigação ainda esteja em andamento, recomenda-se a solicitação, no momento da representação, pela não inclusão do mandado no sistema a fim de não haver nenhum "vazamento" sobre o cumprimento da medida.

3.3.6 Planejamento Operacional

Uma infinidade de aplicações de internet e de softwares pode ser utilizado no planejamento da atividade policial nos níveis estratégico, tático e operacional.

Desde a entrega de uma notificação de testemunha até a realização de uma busca e apreensão deve-se valer de informações disponíveis na internet. Por exemplo, softwares de mapas permitem traçar uma rota entre a delegacia e o ponto em que será realizada a diligência, com agilidade e sem perda de tempo.

Esse planejamento pode se utilizar de mapas disponíveis, incluindo os que têm a função streetview; aplicativos para smartphones com função de geoposicionamento, mesmo que em modo offline; apps para transmissão em tempo real de fotografias, portais públicos com informações políticas, sociais e econômicas de determinada região e vídeos; e softwares de edição para extração de frames de um arquivo de vídeo.

3.3.7 Sites de Tribunais e Antecedentes Criminais

O acesso aos sites dos Tribunais possibilita informações sobre os dados de um processo do investigado, desde o número e do início processo, partes envolvidas, a natureza criminal e a vara de tramitação. Em alguns tribunais é possível fazer a emissão da certidão negativa.

No momento em que o indivíduo é identificado na investigação de determinado fato, a consulta por processos anteriores pode ser útil em agregar informações sobre os demais envolvidos. O resultado dessa pesquisa deve ser anexado ao inquérito policial ou diretamente no relatório de missão policial.

Algumas aplicações de internet permitem a busca por antecedentes criminais de modo online se o investigado possui ou não registros criminais nos sistemas. É o caso, por exemplo, da Polícia Federal, através do link http://www.pf.gov.br/servicos/antecedentes-criminais, permite a emissão e validação deste documento. Alguns estados permitem também essa expedição eletronicamente:

- BA http://www.ba.gov.br/antecedentes/solicitar_atestado.asp;
- CE http://www.sspds.ce.gov.br/AtestadoAntecedentes/;
- ES http://www.es.gov.br/Cidadao/paginas/docs_atestado_antecedentes.aspx

- MG https://wwws.pc.mg.gov.br
- PA http://antecedentes.policiacivil.pa.gov.br/;
- PE http://www.sds.pe.gov.br/;.
- RJ http://atestadodic.detran.rj.gov.br/;
- RS http://www.igp.rs.gov.br/index.php?option=com_wrapper
- SP http://www.ssp.sp.gov.br/servicos/atestado.aspx;

4. CONCLUSÃO

A polícia deve se adequar a essa nova realidade. A investigação, em seu caráter multidisciplinar, exige o emprego de fontes abertas para seu aperfeiçoamento. Essa informação disponível, desde que coletada e analisada de forma correta, tem valor e deve ser utilizada no inquérito policial.

A investigação em fontes abertas deve ser incluída na formação dos novos policiais. A infinidade de informações que são postas a cada instante exige capacitação e a disponibilidade de softwares que mineram esses dados e apontem cenários e tendências. O empirismo não cabe mais na era tecnológica. As opções de coleta em fontes abertas são infinitas. A cada dia surge uma fonte nova e, para isso, o policial deve manter-se atualizado nessa busca constante de informações úteis.

O sigilo deve prevalecer na apuração das infrações e de sua autoria. Devemos utilizar, no entanto, informações públicas disponíveis e não apenas as sigilosas. Durante o inquérito não se deve somente utilizar aquelas informações extraídas do local de crime ou decorrentes deste, mas também agregar as que estão disponíveis, principalmente na internet.

Numa discussão entre os integrantes do Twitter[127] sobre quem seria o inventor do microblogger, os fundadores pontuaram:

- Jack: Mas eu inventei o Twitter.

- Ev: Não, você não inventou o Twitter. Eu também não o inventei. Nem Biz. As pessoas não inventam as coisas na internet. Elas simplesmente desenvolvem uma ideia que já existe.

Nesse raciocínio, não nos cabe inventar a investigação em fontes abertas. Basta apenas que nos adequemos ao que já se encontra disponível há bastante tempo e agregá-lo na investigação policial. A polícia que investir nessa área sairá na frente.

[127] Nick Bilton. A Eclosão do Twitter.

5. REFERÊNCIAS

BARRETO, Alessandro G.; WENDT, Emerson. **Inteligência Digital: uma análise das fontes abertas na produção de conhecimento e de provas em investigações e processos**. Rio de Janeiro: Brasport, 2013.

BILTON, Nick. **A Eclosão do Twitter. Uma Aventura de Dinheiro, Poder, Amizade e Traição.** Tradução Elvira Serapicos. São Paulo: Editora Schwarcz Portfolio Penguin.

BRASIL. Constituição da República Federativa do Brasil de 1988. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Portal da Legislação**. Disponível em:
<http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm> .Acesso em: 13 dez. 2015.

BRASIL. Conselho Nacional de Justiça. Resolução nº 137 de 13 de julho de 2011. Regulamenta o banco de dados de mandados de prisão, nos termos do Art. 289-A do CPP, acrescentado pela Lei nº 12.403, de 4 de maio de 2011, e dá outras providências. Disponível em: <http://www.cnj.jus.br/atos-normativos?documento=134 >. Acesso em: 13 dez. 2015

BRASIL. Estatuto da Criança e do Adolescente. Lei 8.069 de 13 de Julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Portal da Legislação**. Disponível em: < http http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm>.Acesso em: 13 dez. 2015.

BRASIL. Lei nº 12.527 de 18 de novembro de 2011. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. **Portal da Legislação**. Disponível em:
<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 13 dez. 2015.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Portal da Legislação**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 13 dez. 2015.

BRASIL. Justiça Federal. 7ª Vara Criminal. 1ª Subseção Judiciária do Estado de São Paulo. Portaria nº 012/2015 datada de 15 de Abri de 2015. Disponível em http://www.jfsp.jus.br/20150423-whatsapp/. Acesso em: 13 dez. 2015.

BRASIL. Supremo Tribunal Federal. Inq. 3563 PR**.** Relator Min. LUIZ FUX. 27 de fevereiro de 2014. Disponível em:

<http://stf.jusbrasil.com.br/jurisprudencia/24974776/inquerito-inq-3563-pr-stf >. Acesso em: 13 dez 2015

BRASIL. Superior Tribunal de Justiça. **REsp 59560 - SC**.. Rel. Ministro Cesar sfor Rocha. 18 de março de 2004. Disponível em: < http://stj.jusbrasil.com.br/jurisprudencia/19398367/recurso-especial-resp-595600-sc-2003-0177033-2/inteiro-teor-19398368>. **REsp 1168547 / RJ RECURSO ESPECIAL 2007/0252908-3** Rel. Ministro Luis Felipe Salomão T4 - QUARTA TURMA. Julgado em 11 de maio de 2010. Acesso em: 13 dez. 2015

BRASIL. Tribunal Regional Eleitoral do Rio de Janeiro. **RECURSO NA REPRESENTAÇÃO NQ 3782-90.2014.6.19.0000**. Rel. Alexandre Chini Neto. Julgado em 21 outubro 2014. Disponível em: <http://www.tse.jus.br/sadJudSadpPush/ExibirDadosProcessoJurisprudencia.do?nproc=378290&sgcla=RP&comboTribunal=rj&dataDecisao=21/10/2014>. Acesso em: 13 dez. 2015

BRASIL. Tribunal de Justiça de Mato Grosso do Sul. AC 6424 MS 2012.006424-5. Rel. Des. Ruy Celso Barbosa Florence. Julgado em 24 abr. 2012.Disponível em:
< http://tj-ms.jusbrasil.com.br/jurisprudencia/21532724/apelacao-civel-ac-6424-ms-2012006424-5-tjms/inteiro-teor-21532725 >. Acesso em: 13 dez. 2015

BRASIL, Tribunal de Justiça de Goiás. Intimações do Juizado Especial de Piracanjuba podem ser efetuadas pelo WhatsApp. Em 24 de abril de 2015. Disponível em http://www.tjgo.jus.br/index.php/home/imprensa/noticias/161-destaque1/9292-intimacoes-do-juizado-especial-de-piracanjuba-podem-ser-efetuadas-pelo-whatsapp. Acesso em: 12 dez. 2015.

BRASIL. Tribunal Superior do Trabalho. **Recurso de Revista** 61300-23.2000.5.10.0013. Rel. João Oreste Dalazen. Julgado em 18 mai. 2005. Disponível em:
<http://tst.jusbrasil.com.br/jurisprudencia/1724843/recurso-de-revista-rr-61300232000510001 3-61300-2320005100013 >. Acesso em: 13 dez. 2015

BRASIL. Vara do Trabalho de Tucurui-PA. Proc nº: 0002736-51.2013.5.08.0110 Reclamante: Ministério Público do Trabalho. Juiz Ney Stany Morais Maranhão. 18 de Junho de 2015. Disponível em http://www.trt8.jus.br/. Acesso em: 13 dez. 2015.

CBS NEWS. **Woman try to sell children on Facebook to get bail money for boyfriend, police say.** Disponível em http://www.cbsnews.com/news/okla-woman-tries-to-sell-children-on-facebook-to-get-bail-money-for-boyfriend-police-say/. Acesso em 05 dez.2015.

CEPIK, Marco. **Espionagem e Democracia: agilidade e transparência como dilemas na institucionalização do serviço de inteligência**. Rio de Janeiro: Editora FGV, 2003.

CONJUR. Justiça e Tecnologia. Juiz usa Skype para promover audiência

de conciliação com casal separado. Disponível em http://www.conjur.com.br/2015-jul-25/juiz-usa-skype-promover-audiencia-conciliacao. Acesso em: 13 de dez. 2015.

CONSELHO NACIONAL DE JUSTIÇA. Tribunal realiza audiência em processo de Família via Skype. Em 24 de julho 2015. Disponível em http://www.cnj.jus.br/noticias/judiciario/79962-tribunal-realiza-audiencia-em-processo-de-familia-via-skype. Acesso em 13 dez. 2015.

DAILY MAIL. **Diamond thief who stole jewels worth £80,000 was caught by police after posting holiday pictures on Facebook while on the run**. Disponível em: http://www.dailymail.co.uk/news/article-2262360/Diamond-thief-caught-posting-holiday-pictures-Facebook-run.html#ixzz3tRz5CIS3. Acesso em 05 dez. 2015.

2. DORILEO, Carlos**.** Folha Max**. Vítima informa roubo por WhatsApp e PM prende bandidos em clínica de Cuiabá.** Disponível em: http://www.folhamax.com.br/policia/vitima-informa-roubo-por-whatsapp-e-pm-prende-bandidos-em-clinica-de-cuiaba/2648. Acesso em 12 dez. 2015.

1. DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK**. United States of America against Joshua Meregildo**. Julgado em 10 agosto 2012. Disponível em http://nysd.uscourts.gov/cases/show.php?db=special&id=204. Acesso em 13 dez. 2015.

3. GONÇALVES, Rafaela. Jornal Cruzeiro. **Grávida é agredida pelo marido e pede ajuda por Whatsapp.** Disponível em http://www.jornalcruzeiro.com.br/materia/661770/gravida-e-agredida-pelo-marido-e-pede-ajuda-por-whatsapp. Acesso em 12 dez. 2015.

IACP SOCIAL MEDIA. **2014 Social Media Survey Results**. Disponível em http://www.iacpsocialmedia.org/Portals/1/documents/2014SurveyResults.pdf. Acesso em 05 dez. 2015.

LEXISNEXIS. **Social Media use in Law Enforcement**. Disponível em: http://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf. Acesso em 06 dez.2015.

MIRROR. Okla. **Indian man arrested for trying to sell his grandson on Facebook.** Disponível em http://www.mirror.co.uk/news/world-news/indian-man-arrested-trying-sell-1850951. Acesso em 05 dez.2015.

MONTGOMERY, David; HORWITZ, Sari and FISHER, Marc. The Washington Post. **Police, citizens and technology factor into Boston bombing probe**. https://www.washingtonpost.com/world/national-security/inside-the-investigation-of-the-boston-marathon-bombing/2013/04/20/19d8c322-a8ff-11e2-b029-8fb7e977ef71_story.html

SCHAURER, Florian; STORGER, Jan. Journal of U.S. Intelligence Studies. **The Evolution of Open Source Intelligence**. Volume 19. Number 3. Disponível em:

http://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf. Acesso em 13 dez.2015.
TELECO. **Usuários de Internet no Brasil**. Disponível em http://www.teleco.com.br/internet.asp. Acesso em 04 dez. 2015.
TORONTO POLICE SERVICE. **Social Engagement Guidelines**. Disponível em http://www.torontopolice.on.ca/publications/files/social_media_guidelines.pdf. Acesso em 05 dez. 2015.
WÜNSCH, Silke DW.com. German Police use Web 2.0 to catch criminals. http://www.dw.com/en/german-police-use-web-20-to-catch-criminals/a-15836813. Acesso em 13 dez.2015.

RELATÓRIO DE MISSÃO POLICIAL ___/___/20__

Em cumprimento a determinação do DPC _____, a fim de empreender diligências para coletar informações sobre o investigado _____, conforme os autos do Inquérito _____, que apura crime de _____, procedemos o seguinte:

Ao realizar a consulta em fontes abertas através da internet, fazendo uso de buscadores online, na data de XX/XX/XX, obtivemos os seguintes dados abaixo relacionados:

Mídias Sociais

(Descrever detalhadamente, incluindo as URLs quando possível, todos os dados de perfis, fotos, vídeos, comentários, curtidas, check-ins, compartilhamentos e outras ações possíveis em cada um dos principais domínios que, de algum modo possam ajudar a identificar o investigado, ou cujo conteúdo mantenha relação com a investigação, demonstrando vínculo com a prática criminosa. Anexar as imagens com seus links diretos ou de cache de buscadores, link de vídeos e outras mídias. Salvar os arquivos em mídia, quando possível, calculando número hash, que constará no relatório.)

Sites de Noticiais

(Anexar conteúdo extraído de sites de notícias, incluindo as urls, fotografias e dados úteis da matéria)

Sites de Tribunais

(Justiça Estadual e Federal, Tribunais de Contas e Tribunais Superiores) e demais sites públicos (diários oficiais, sites relacionados à transparência pública e etc)

Outros dados encontrados

(Blogs, comentários em matérias ou artigos em outros sites e etc.)

Era o que tinha a relatar.

_____, __ de_____ de20__

Capítulo X

COOPERAÇÃO INTERNACIONAL NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

José Augusto Campos Versiani[128]

1. INTRODUÇÃO

Este capítulo versa sobre a obtenção de dados com entidades públicas e privadas internacionais para o desenvolvimento de uma investigação policial, dados esses que podem vir a ser tratados pela autoridade policial como de inteligência ou como prova. Não será feita uma análise sobre o mérito dos procedimentos, qual seria a praxe mais adequada, mas uma abordagem prática, que indique meios para a solução de problemas.

A grande dificuldade na obtenção dessas provas ou indícios de prova é a inerente a todo o direito internacional: não há legislação comum ou poder coercitivo único nessa seara. Há que ser observada a legislação local que regula a empresa privada e os tratados existentes entre o país sede da empresa ou entidade governamental e a República Federativa do Brasil.

Nesse sentido vale citar o caput e incisos I a IX do artigo 4º da Constituição Federal de 1988, que contém os princípios que regem as relações internacionais da República Federativa do Brasil e englobam o espírito que permeia a cooperação internacional ativa ou passiva com o nosso país:

"***Art. 4º*** *A República Federativa do Brasil rege-se nas suas relações*

[128] José Augusto Campos Versiani é Delegado de Polícia Federal com ampla experiência na investigação de crimes cibernéticos e na cooperação internacional nessa área Pós graduação em bancos de dados no IESB Brasília e Especializações em Segurança de Redes e Sistemas, Arquitetura e protocolos de rede TCP-IP, Protocolos de Roteamento IP pela Escola Superior de Redes da RNP

I - independência nacional;
II - prevalência dos direitos humanos;
III - autodeterminação dos povos;
IV - não-intervenção;
V - igualdade entre os Estados;
VI - defesa da paz;
VII - solução pacífica dos conflitos;
VIII - repúdio ao terrorismo e ao racismo;
IX - cooperação entre os povos para o progresso da humanidade;"

O princípio da independência nacional, assim como os da auto-determinação dos povos, não-intervenção e igualdade entre os Estados instruem que toda relação internacional deve respeitar e ser formulada com a consciência da soberania de cada nação envolvida. Uma empresa estrangeira sem representação no Brasil não tem, formalmente, a obrigação de respeitar a legislação brasileira, e dificilmente fornecerá informação que não seja amparada na legislação do país onde é sediada, mesmo que relacionada a usuário brasileiro.

Como a rede mundial de computadores tem grande parte de sua estrutura e serviços provida por empresas sediadas nos Estados Unidos da América, grande parte do esforço de uma autoridade policial em obter provas e indícios na em crimes cibernéticos costuma envolver lidar com o direito e princípios aplicados nos EUA para o fornecimento de informações para a polícia, especialmente com a diferença no conceito de cada país do que pode ser considerado liberdade de expressão. Vejo como oportuno citar trecho das diretrizes operacionais da empresa Facebook para o fornecimento de informações para autoridades policiais [129]:

"Requisitos Legais de Processos Norte Americanos

Divulgamos registros de contas apenas em conformidade com nossos termos de serviços e com a legislação aplicável, incluindo a lei federal Stored Communications Act ("SCA") (Ato de Comunicações Armazenadas), no Código dos Estados Unidos, título 18, Seções 2701-2712. Sob a SCA:

- *Uma intimação válida emitida é necessária em conexão com uma investigação criminal oficial para forçar a divulgação de registos básicos de assinantes (definido em 18 U.S.C., seção 2703(c)(2)), que podem incluir: nome, duração do serviço, informações do cartão de crédito, endereço(s) de e-mail e endereço(s) de IP de um início/fim da sessão recente, se disponível.*
- *É necessária uma ordem judicial conforme consta no Código dos Estados*

[129] https://www.facebook.com/safety/groups/law/guidelines/ - acessado na data de 08/01/2016

Unidos, título 18, Seção 2703(d) para forçar a divulgação de determinados registros ou outras informações pertencentes à conta, excluindo conteúdos de comunicações, como cabeçalhos de mensagens e endereços de IP, além dos registros básicos dos assinantes, descritos acima.

- *É necessário um mandado de busca conforme procedimentos descritos no Código Federal de Processo Penal dos Estados Unidos ou mandado estadual equivalente mediante comprovação de justificativa provável para forçar a divulgação de conteúdos armazenados em qualquer conta, incluindo mensagens, fotos, vídeos, publicações no mural e informações de localização.*
- *Interpretamos a provisão da carta de segurança nacional como aplicada ao Facebook para exigir a apresentação de apenas 2 categorias de informações: nome e duração do serviço."*

Esse trecho informa que o Facebook, a despeito de ser uma empresa com filial constituída no Brasil, manifesta obedecer à legislação dos EUA, mais especificamente à lei federal dos EUA "Stored Communications Act - SCA" (Ato de Comunicações Armazenadas), contida no Título 18 do Código dos Estados Unidos (United States Code - USC), Seções 2701-2712 e mais especificamente ao § 2703 - "Required disclosure of customer communications or records", ou "Fornecimento obrigatório de comunicações ou registros de consumidores". Fora de qualquer juízo sobre ser cabível a abordagem da empresa, o fato é que a maioria das empresas sediadas nos EUA seguem o princípio de que devem obedecer às leis dos EUA mesmo com relação a requisições de autoridades policiais brasileiras relativas a atos de usuários brasileiros cometidos em território brasileiro.

O princípio dos direitos humanos, inciso II do Art. 4º da Constituição Federal de 1988, também é bastante pertinente ao tema. Um dos lados desse princípio é o de que entidades privadas e governamentais, em regra, não fornecerão informações que entendam como uma violação à privacidade de um usuário, de acordo com a lei local ou mesmo com relação à lei brasileira, o Marco Civil da Internet (MCI), a Lei nº 12.965 de 23 de abril de 2014. Vejo como oportuno reproduzir o artigo 2º e 3º da citada Lei:

"**Art. 2º** A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
I - o reconhecimento da escala mundial da rede;
II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
III - a pluralidade e a diversidade;
IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade de rede;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII - preservação da natureza participativa da rede;
VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei."

Neste momento em que parte do Marco Civil da Internet ainda precisa ser regulamentado as autoridades policiais brasileiras encontram-se no pior dos dois mundos, em que não mais são atendidas por algumas empresas americanas com as mesmas informações e facilidade de acesso a essas que possuem as autoridades policiais dos EUA e algumas empresas ainda exigem ordens judiciais para qualquer tipo de informação com fundamento no MCI, a despeito da previsão contida o § 3º do Art. 10 dessa Lei:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
(...)
§ 3o O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

O outro lado do princípio dos direitos humanos é o de que, quando a autoridade policial comprova que as informações desejadas são relativas a investigação em que há iminente risco de vida ou violação de integridade física ou psicológica de crianças ou adolescentes, os obstáculos legais costumam ser

afastados e a informação fornecida rapidamente. Informações que em casos normais levam semanas ou meses para serem fornecidas, são remetidas em dias ou mesmo horas. Nesses casos, é recomendável que a autoridade policial mencione tais circunstâncias desde o início de sua requisição de informações, para que ele seja tratado com a urgência e relevância necessária.

Os princípios VI, VII e VIII, respectivamente a defesa da paz, a solução pacífica dos conflitos e o repúdio ao terrorismo e ao racismo também encontram eco na prática da cooperação internacional para a investigação de crimes cibernéticos. A investigação de possíveis atos terroristas recebe tratamento prioritário pela maioria das empresas e entidades governamentais, e assim como no caso de risco de vida essa finalidade deve ser esclarecida de plano, para garantir a celeridade no tratamento da requisição. Investigações relativas a crimes de racismo também recebem prioridade, ainda que menor do que as anteriormente mencionadas e com as restrições sobre como cada país lida com o tema.

2. A PRÁTICA DA COOPERAÇÃO INTERNACIONAL NO COMBATE AOS CRIMES CIBERNÉTICOS

Como mencionado na introdução, a falta de poder coercitivo internacional que regule a interação entre órgãos policiais e empresas que proporcionam serviços pela rede mundial de computadores e que obrigue a empresa a prestar informações faz com que os indícios obtidos com essas empresas sejam fornecidos, quando na modalidade de cooperação direta, de forma voluntária. Tal cooperação voluntária em geral consiste no fornecimento de dados cadastrais e "logs" de conexão de usuários, ou seja, informações não protegidas pelo sigilo constitucional que abrange o conteúdo de uma comunicação, e que por não violarem a privacidade do usuário podem ser obtidas por requisição da Autoridade Policial[130].

A maioria das empresas que presta serviços na internet solicita que a autoridade policial confeccione uma requisição assimilada ao documento oficial "Subpoena" utilizado pela polícia dos EUA. O termo “subpoena” tem como tradução literal “intimação”, mas dentro desse sentido pode ser entendido como uma requisição de informações. A despeito de algumas empresas, como o Facebook, receberem requisições pelo preenchimento de um formulário em português, esse tipo de requisição usualmente necessita ser redigido em inglês e conter breve descrição dos fatos que ensejaram o pedido, a informação desejada e/ou a preservação da mesma. A praxe é a de que o “Subpoena” deve ser assinado, digitalizado e encaminhado para a empresa detentora da informação

[130] Como previsto no § 2º do Art. 2º da Lei Federal 12.830/13.

requisitada por meio de mensagem para endereço eletrônico específico para esse tipo de solicitação ou mandado por fax para o número designado para essa finalidade. O uso de fax, apesar de não ser prática vigente no Brasil, é geral nos EUA, sendo obrigação legal que as empresas tenham um número de fax para o recebimento de requisições policiais.

Essa requisição de dados usualmente tem como resultado os dados fornecidos pelo usuário para identificação e cadastro, quais sejam, endereço de e-mail e outros dados pessoais e de contato e, em alguns casos, dados de conexão do usuário, também chamados de "logs" (“registros” em tradução livre). Recomenda-se solicitar todos esses dados, para que não se receba uma quantidade aquém da que poderia ser fornecida pela empresa.

Os dados de conteúdo, que contém a efetiva comunicação do usuário, e não informações de cadastro e de conexão, geralmente só são fornecidos mediante solicitação efetuada com base em Acordo de Cooperação Jurídica Internacional ou MLAT (Mutual Legal Assistance Treaty) entre o Brasil e o país em que está sediada a empresa demandada. Esses dados não-cadastrais geralmente incluem fotos, mensagens, comunicação por voz e outras manifestações que possam ser consideradas comunicação ou conter informações pessoais do usuário, sobre as quais incide proteção constitucional. Esse tema será melhor desenvolvido no próximo tópico.

Como mencionado anteriormente, convém registrar que a legislação dos EUA e de outros países autoriza empresas que fornecem serviços na internet a transferir dados de conteúdo às autoridades policiais estrangeiras em casos de emergência. Vários desses serviços fornecem contatos para o fornecimento de informações em casos de risco real ou iminente à vida, terrorismo, crime em flagrante, pornografia infantil, abuso de crianças e adolescentes, casos em que a velocidade de fornecimento de dados e a quantidade de dados fornecidos costuma ser maior. Registre-se que nos casos de crime em flagrante o tipo criminal e os excludentes de ilicitude a serem observados não são somente os previstos na legislação brasileira, mas também os vigentes no país sede da organização demandada (princípio da dupla-incriminação).

É recomendado à autoridade policial representar por autorização judicial para acesso a dados de conteúdo, tanto para que os dados fornecidos não encontrem obstáculo em serem aceitos como prova pela justiça brasileira quanto para, no caso de negativa ao fornecimento dos dados, que essa autorização possa servir de base a um pedido com base em MLAT.

Vejo como relevante reforçar que a autoridade policial deve ter em mente o uso que deseja para a informação que irá solicitar à empresa ou autoridade governamental estrangeira. Se a autoridade policial deseja usar a informação obtida como prova deve ter em mente o permissivo legal que autorize o uso da informação em juízo ou obter autorização judicial para efetuar a solicitação da informação, pois existem casos em que o juízo não admite ratificar a posteriori a

obtenção desse tipo de prova. Mesmo quando a autoridade policial deseja somente uma informação de inteligência que auxilie na obtenção de provas há que se considerar que a juntada ao inquérito policial de informações obtidas de forma não amparada na legislação brasileira abre espaço para a impugnação do resultado das investigações.

Outra recomendação no tocante às requisições de dados a provedores de serviços na internet é a de especificar que a solicitação de dados não deve ser comunicada ao usuário, quando necessário, sob pena, de prejudicar a investigação policial. A mesma ressalva deve constar dos pedidos de quebra de sigilo judiciais, para que o juiz determine que a empresa não deve divulgar a requisição de dados ao investigado. Algumas empresas, como o Twitter, manifestam expressamente que comunicarão ao usuário qualquer solicitação de dados a não ser que sejam compelidas a não fazê-lo.

3. FORMAS DE COOPERAÇÃO INTERNACIONAL

3.1. A Polícia Federal como representante das polícias brasileiras na cooperação internacional nos crimes cibernéticos

Como consequência lógica do previsto no inciso I do artigo 21 da CF/88, que define a competência da União em manter relações com Estados estrangeiros e participar de organizações internacionais, temos no Brasil a Polícia Federal, a Polícia Judiciária da União, responsável pela apuração de crimes com repercussão internacional, como representante policial do estado brasileiro quando da interação internacional com outras polícias e entes públicos e privados na busca de provas e informações de inteligência.

Dentro do Departamento de Polícia Federal essa atividade é exercida pela Coordenação-Geral de Cooperação Internacional (CGCI), em âmbito nacional, que atua por meio de representações regionais em cada superintendência regional da Polícia Federal. A cooperação policial internacional é desenvolvida pela PF de várias formas, como por meio da interação direta com polícias de outros países e pela participação em organizações policiais intergovernamentais como a Interpol, Europol e Ameripol. A participação em organismos policiais inter-governamentais possibilita que o país possa desenvolver cooperação célere com as polícias de outros países, essencial em situações flagranciais e em casos em que a atuação policial é urgente em razão da relevância do bem jurídico tutelado. Essa cooperação pode abranger atividades como o intercâmbio de informações de natureza investigativa ou mesmo o cumprimento de diligências policiais. A representação policial internacional pela Polícia Federal também é exercida pelas adidâncias policiais junto às missões diplomáticas do Brasil no exterior, escritórios de ligação e pela participação de policiais em encontros, cursos e seminários internacionais.

Caso seja necessária a cooperação internacional com uma polícia estrangeira e/ou uma organização policial internacional, essa deve ser encaminhada pelo

representante regional da Coordenação-Geral de Cooperação Internacional da Polícia Federal, que efetuará os contatos nacionais e internacionais necessários ao andamento da demanda.

3.2. Cooperação internacional por meio de Acordos de Cooperação Jurídica Internacional

Como dito anteriormente, a obtenção de dados de conteúdo, que contém a efetiva comunicação ou dados privativos do usuário, geralmente só são fornecidos mediante pedido efetuado com base em Acordo de Cooperação Jurídica Internacional ou MLAT (Mutual Legal Assistance Treaty) entre o Brasil e o país em que está sediada a empresa demandada. Isso ocorre em razão desses dados incluírem fotos, mensagens, comunicação por voz e outras manifestações que possam ser consideradas comunicação ou conter informações privadas do usuário, protegidas pelo sigilo previsto nos incisos X e XII da CF/88, que espelha o entendimento majoritário da comunidade internacional.

Caso a investigação demande um pedido por meio de Acordos de Cooperação Jurídica Internacional, o primeiro passo a ser efetuado é o de solicitar a preservação das informações desejadas, haja vista que o tempo necessário para que tal pedido tramite entre os países pode ser maior do que a política de preservação de dados dessa empresa, próprio ou por exigência da legislação local. No Brasil quem efetua e tramita os pedidos de MLAT, após o recebimento de requisição nesse sentido, é o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional - DRCI, do Ministério da Justiça. Reproduzo abaixo a explicação mencionada no Manual de Cooperação Jurídica Internacional e Recuperação de Ativos publicado pelo DRCI:

"O DRCI, como autoridade central brasileira, por meio das Coordenações-Gerais de Cooperação Jurídica Internacional e de Recuperação de Ativos, é responsável pela boa condução dos pedidos de cooperação jurídica internacional entre o Estado brasileiro e os demais países, cabendo-lhe receber, analisar, adequar, transmitir e acompanhar o cumprimento dessas solicitações."

O Manual de Cooperação Jurídica Internacional e Recuperação de Ativos encontra-se disponível para download por meio do site do DRCI/MJ na internet. Como o link é bastante longo, forneço aqui um endereço reduzido: http://goo.gl/zKT1f6 .

É recomendável que a autoridade policial obtenha o supracitado Manual por esse conter valiosas informações sobre a teoria e prática nos casos em que uma autoridade policial brasileira é parte ativa em um processo de cooperação jurídica internacional. Ali poderá ser encontrada orientação sobre como fundamentar pedidos de cooperação internacional e a enumeração dos países com os quais a República Federativa do Brasil possui tratados, e, o que cada um prevê. Reproduzo abaixo trecho sobre pedidos de cooperação ativos, ou seja, com uma autoridade brasileira como demandante:[131]

[131] Manual de Cooperação Jurídica Internacional e Recuperação de Ativos – DRCI/MJ, pg. 80.

4. PEDIDOS DE COOPERAÇÃO ATIVOS

As cartas rogatórias em matéria penal e os pedidos de auxílio jurídico em matéria penal formulados pelas autoridades brasileiras competentes deverão ser encaminhados à autoridade central brasileira para análise e tramitação. O DRCI, na qualidade de autoridade central, gerencia o fluxo de pedidos de cooperação jurídica internacional, adequando-os e os remetendo às respectivas autoridades nacionais e estrangeiras competentes após o seu juízo de admissibilidade administrativo, com vistas a acelerar e melhorar a qualidade dos resultados da cooperação. Entretanto, a autoridade central não detém capacidade postulatória.

Quando o pedido de cooperação basear-se em tratado internacional que preveja a comunicação direta entre autoridades centrais, a autoridade central brasileira, após verificar o preenchimento dos requisitos previstos no respectivo tratado, providenciará sua transmissão à Autoridade Central estrangeira."

Como a cooperação internacional é algo dinâmico, entendo que melhor do que efetuar uma enumeração parada no tempo é direcionar o colega à página do sítio do Ministério da Justiça que contém a lista atualizada dos acordos e tratados em que o Brasil é parte: http://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais .

5. OBTENÇÃO DE INFORMAÇÕES JUNTO AOS SERVIÇOS DE INTERNET MAIS UTILIZADOS

5.1. Facebook e Instagram:

O Facebook provê uma página em que explica quais informações são fornecidas a particulares e à autoridades policiais[132]:

https://www.facebook.com/safety/groups/law/guidelines/

A página supramencionada contém informações em português para quem acessa a partir de um endereço IP brasileiro desde 2011, pelo que recordo. Caso exista interesse em visualizar a versão da página em inglês pode ser usado um serviço de proxy com endereço americano ou fazer o download em PDF de seu conteúdo em inglês[133]. Essa página contém o seguinte aviso:

> *"Requisitos Legais de Processos Internacionais*
>
> Divulgamos registros de contas apenas em conformidade com nossos termos de serviços e com a legislação aplicável. Pode ser necessário um Tratado de Auxílio Mútuo em Matéria Penal ou uma carta rogatória para

[132] Na versão desta página em janeiro de 2016.

[133] https://scontent-mia1-1.xx.fbcdn.net/hphotos-xfa1/l/t39.2178-6/851585_544247282309435_854704444_n.pdf

forçar a divulgação de conteúdos de uma conta. Para mais informações, acesse facebook.com/about/privacy/other."

O Facebook fornece uma página de internet específica para que Autoridades Policiais possam requisitar dados cadastrais e "logs" de conexão de usuários dessa rede social, como também a preservação dessas informações:

https://www.facebook.com/records

Após acessar a página a autoridade policial é instada a fornecer um endereço de e-mail institucional, para onde será enviado um link de acesso ao chamado "Sistema de Solicitação On-Line para Autoridades", que dará acesso ao sistema por uma hora. Após acessar o link o usuário chega numa página em que verifica as solicitações que efetuou, e tem acesso a uma página para solicitações de preservação de informações, uma página para solicitação de registros e uma página de perguntas frequentes, que responde dúvidas sobre a utilização do sistema.

Para efetuar pedidos de preservação de informações basta que a autoridade policial informe o número do caso, as contas que deseja que tenham a sua informação preservada e confirme que a solicitação é feita por uma autoridade pública autorizada a fazer esse tipo de solicitação.

Para a solicitação de registros a autoridade policial deve preencher um formulário enumerando diversas informações:

- "Internal Case Reference Number" - o número do caso, o que pode ser entendido como número do Inquérito Policial;
- "Legal Process" - o tipo de requisição, com as opções "Court Order/Request" (ordem judicial, "Emergency" (emergência), "Ordem Judicial assinada por um juiz", "Solicitação policial e "Outros";
- "Nature of Case" a natureza do caso, com as opções "Child Exploitation" (exploração de crianças), "Child Exploitation (Potential Harm)" (exploração de crianças com risco em potencial), "Perfil falso/Invadido, "Crime Sexual", "Agressão/Homicídio", "Atividade terrorista", "Atividade de gangues", "Ameaça/Perseguição", "Fraudo or Theft" (fraude ou roubo) e "Outros";
- "Legal Process Signed Date" (data de assinatura do procedimento legal);
- "Request Due Date" (data em que é esperada a resposta da requisição);
- "Accounts", ou seja, as contas sobre as quais deseja-se obter informações;
- "Requesting Records Between" - período sobre o qual deseja-se registros;
- "Documentation" - documentos que informam e/ou subsidiam a requisição;

O Facebook pode informar uma vasta gama de informações sobre o usuário, do endereço de e-mail e número de telefone à "real identidade do usuário", dado que o Facebook fornece sem detalhar a técnica utilizada pela empresa para obter a informação, mas que possivelmente deve ser extraída de uma relação entre o IP do usuário e os perfis que acessa.

Uma outra informação interessante a respeito do Facebook, e de alguns outros serviços de internet populares nos EUA, como o Twitter, é a de que existem empresas especializadas em fazer a análise dos dados publicados nesses serviços. Essa análise é utilizada principalmente por grandes empresas para saber a reação do público a seus produtos e a produtos de concorrentes e a de analisar tendências de consumo. Algo relevante a respeito do Facebook é a de que a empresa possui uma avançada plataforma de publicidade disponível para quem quiser efetuar publicidade no serviço, com a possibilidade de atingir um público bastante específico (ex.: homens brasileiros entre 20 e 30 anos com renda alta) e provê análise detalhada dos resultados da campanha comercial.

O Facebook fornece o fluxo total de dados a algumas empresas, que podem ser analisados tanto para a extração de informações comerciais como sociais, da manifestação popular de preocupação com uma doença como a dengue a pessoas que manifestam ter contraído a doença (dado que poderia ser relevante, por exemplo, para o Ministério da Saúde), e assim ser montado um mapa para auxiliar o combate a essa doença. A mesma análise de dados pode servir para estudar a dinâmica de um protesto social contra o governo, onde se localizam e quem são os líderes de um movimento, quais serão as próximas ações desse movimento e em que locais serão efetuadas reuniões. A despeito de empresas que recebem o fluxo de dados direto do Facebook provavelmente serem proibidas contratualmente de fornecer serviços para governos não democráticos, isso não impede que o mesmo tipo de análise possa ser efetuada por uma organização que usar formas indiretas de monitorar essa rede social.

5.2. WhatsApp:

A empresa WhatsApp define o aplicativo de mesmo nome da seguinte forma: "WhatsApp Messenger é um aplicativo de mensagens multiplataforma que permite trocar mensagens pelo celular sem pagar por SMS. Está disponível para iPhone, BlackBerry, Android, Windows Phone, e Nokia e sim, esses telefones podem trocar mensagens entre si! Como o WhatsApp Messenger usa o mesmo plano de dados de internet que você usa para e-mails e navegação, não há custo para enviar mensagens e ficar em contato com seus amigos."

Outra forma de enxergar o WhatsApp é como um serviço de ligações por voz e mensagens de texto encriptadas, substituindo os serviços proporcionados pelas empresas telefônicas porém sem as mesmas obrigações legais e sem cooperação com a polícia ou justiça. Um dos argumentos utilizados pela empresa para não atender a requisições de informação e ordens judiciais é o de que o aplicativo foi

construído de forma a obscurecer, por meio de encriptação, a comunicação entre dois usuários de forma que nem a empresa possui as chaves de encriptação para a leitura da conversa ou escuta da chamada de voz.

A despeito da WhatsApp ter sido comprada pelo Facebook, as empresas alegam que funcionam independentemente, e assim o WhatsApp alega não ter sede ou representante no Brasil, a despeito de ter celebrado negócios com empresas de telefonia brasileiras.

Ante a não cooperação da empresa, recentemente condenada à suspensão de seus serviços no país por 48 horas por não cumprir determinação judicial em caso penal, as autoridades policiais tem as suas opções de obter textos de mensagens trocadas pelo WhatsApp somente quando o telefone é apreendido e essas mensagens podem ser extraídas por ferramentas de análise forense ou quando é utilizado programa de monitoramento inserido no telefone celular do alvo.

Todavia, não é possível dizer que a WhatsApp é uma empresa totalmente não cooperativa com organizações policiais. Em outro caso recente, em que terroristas executaram reféns em Paris, alguns veículos de imprensa mencionaram que o WhatsApp teria cooperado com o FBI e a polícia francesa para a identificação e localização de terroristas.

5.3. Hotmail, Live.com, Skype e demais serviços Microsoft:

A Microsoft, por ser a empresa que tem maior experiência no combate ao cyber crime, com décadas de experiência no robustecimento dos Sistemas Operacionais Windows e relações de longa data com entidades governamentais, é uma empresa entende o interesse público em cooperar com as Autoridades Policiais, respeita as leis brasileiras e tem equipe para o recebimento de requisições. Como com o resto do mercado, após a entrada em vigor do Marco Civil da Internet a empresa adotou uma abordagem cautelosa e exige a apresentação de ordem judicial para qualquer informação que vá além dos dados cadastrais, com a exceção dos casos em que a AP consiga demonstrar uma das situações de urgência mencionadas no item 02.

Para solicitar dados à Microsoft a Autoridade Policial necessita de enviar um ofício em que discrimine o sujeito passivo da requisição e quais são os dados requisitados, ofício esse em que AP precisa fornecer dados funcionais como o nome, endereço eletrônico funcional, matrícula, telefone do trabalho, lotação e número do caso. Os dados que podem ser fornecidos pela Microsoft vão dos IPs usados para a criação do usuário aos últimos acessos aos vários serviços da empresa.

Com relação ao Skype, é interessante que a AP leve em consideração as possíveis informações que a empresa possa deter sobre o usuário, e não deixar de solicitar as que possam ser no interesse da investigação. Algumas informações que a empresa pode deter são o endereço de IP utilizado para o registro no serviço e nos acessos mais recentes, os meios de pagamento utilizados em

transações financeiras conduzidas com o Skype, como a compra de créditos e números de telefone reais para os quais foram efetuadas chamadas (fixos e celulares).

A Microsoft explica que tipos de dados fornece a Autoridades Policiais na seguinte página:
https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/pppfaq/

Trecho relevante: "If a government wants customer data, it needs to follow applicable legal process - meaning, it must serve us with a warrant or court order for content or a subpoena for subscriber information or other non-content data. We require that any requests be targeted at specific accounts and identifiers. Microsoft's compliance team reviews government demands for user data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order."

Tradução livre: "Se um governo deseja dados relativos a um consumidor, é necessário que sejam seguidas as normas legais exigíveis - no sentido de que será necessário enviar um mandado ou uma ordem judicial para conteúdo ou uma requisição para dados cadastrais ou para outros dados que não contenham conteúdo. Nós exigimos que solicitações sejam relativas a contas e identificadores específicos. O serviço de verificação da Microsoft revisa solicitações governamentais para assegurar que tais solicitações sejam válidas, rejeitas as que não são válidas e só provê os dados especificados no pedido."

Outro trecho que é relevante por especificar as informações fornecidas e definir o que seriam dados cadastrais e dados de conteúdo: "Non-content data includes basic subscriber information, such as e-mail address, name, state, country, zip code, and IP address at time of registration. Other non-content data may include IP connection history, an Xbox Gamertag, and credit card or other billing information. We require a valid legal demand, such as a subpoena or court order, before we will consider disclosing non-content data to law enforcement.

Content is what our customers create, communicate, and store on or through our services, such as the words in an e-mail exchanged between friends or business colleagues or the photographs and documents stored on OneDrive (formerly called SkyDrive) or other cloud offerings such as Office 365 and Azure. We require a court order or warrant before we will consider disclosing content to law enforcement.".

Tradução livre: "Dados que não são de conteúdo, incluem informação básica do usuário, como endereço de e-mail, nome, estado, país, código postal e endereço IP no momento do registro. Outros dados, que não são de conteúdo, podem incluir o históricos de endereço de IP usados para conexão, um "Gamertag" de Xbox e número de cartão de crédito ou outros dados de pagamento. Nós exigimos uma demanda legal válida, como uma requisição ou

ordem judicial, antes que seja considerado o fornecimento de dados não relativos a conteúdo para autoridades policiais.

Conteúdo é o que nossos consumidores criam, comunicam e guardam dentro e através de nossos serviços, como nas palavras em um e-mail trocado entre amigos ou colegas de trabalho e as fotografias e documentos armazenados no OneDrive (previamente chamado de SkyDrive) ou outros serviços de nuvem como o Office 365 e Azure. Nós exigimos uma ordem judicial ou mandado antes de considerar sobre o fornecimento de conteúdo para autoridades policiais."

5.4. Twitter:

O Twitter, neste momento, não é uma empresa que pode ser vista como entusiasta em assistir ao trabalho policial de investigação de crimes cibernéticos. A empresa sustenta que, por não exigir verificação de e-mail ou de autenticidade de identidade para a inscrição de contas, não tem como afirmar que o endereço de e-mail que fornecerá sejam de fato o do usuário. O Twitter tem como política fornecer informações que contenham conteúdo somente mediante ordem jucial.

Há que se ressaltar, que o Twitter tem como política notificar os usuários acerca das informações que fornecerá em razão de requisições policiais, ou mandados judiciais, e assim recomenda-se que o pedido contenha a determinação que o Twitter deva ser expressamente proibido de notificar o usuário acerca da requisição de informações.

O Twitter tem uma página de "Diretrizes para autoridades policiais" no seguinte endereço:

https://support.twitter.com/articles/297661

Reproduzo[134] algumas informações relevantes contidas na página supracitada:

> "Informações sobre retenção de dados
>
> O Twitter retém diferentes tipos de informação para diferentes períodos de tempo e de acordo com nossos Termos de Serviço e Política de Privacidade. Considerando a natureza instantânea do Twitter, algumas informações (p. ex.: logs de IP) só podem ser armazenadas por um curto período de tempo."
>
> "Solicitações de preservação
>
> Aceitamos pedidos de autoridades policiais para preservar registros, que constituem evidência potencialmente relevante em processos judiciais. Preservaremos, mas não divulgaremos, um instantâneo temporário dos registros relevantes da conta por 90 dias, aguardando decisão de processo judicial válido."

[134] De acordo com a versão da página de janeiro de 2016.

"O Twitter notificará os usuários a respeito de solicitações de divulgação de informações da conta?

Sim. O Twitter tem como política notificar os usuários acerca de solicitações de divulgação de informações de conta, o que inclui uma cópia da solicitação, antes da divulgação, a menos que esta seja proibida (p. ex: uma solicitação com base em 18 U.S.C. § 2705(b)). Exceções ao aviso prévio podem incluir situações de emergência ou contraproducentes (p. ex.: emergências; comprometimento da conta). Quando o aviso prévio é proibido, nós podemos fornecer um aviso posterior aos usuários envolvidos."

Página para solicitar informações em casos emergenciais:
https://support.twitter.com/forms/lawenforcement

A despeito da página acima, o Twitter não aceita receber ordens judiciais por e-mail, ou aceita receber qualquer tipo de requisição ou ordem judicial que não seja de emergência.

O que diz o Twitter sobre solicitações de emergência:

"O Twitter avalia as solicitações de divulgação de emergência caso a caso, de acordo com a legislação pertinente (p. ex.: 18 U.S.C. § 2702(b)(8) e Seção 8 da Lei Irlandesa de Proteção de Dados de 1988 e 2003). Se recebermos informações que nos deem, de boa fé, a certeza de que há uma emergência envolvendo perigo de morte ou de sérios danos físicos à pessoa, nós poderemos fornecer as informações necessárias para evitar o dano se as tivermos."

Dados que devem constar de uma requisição de emergência:

- A clara identificação que o remetente é uma autoridade policial enviando uma "Solicitação de Divulgação de Emergência";
- A identificação clara de que a possível vítima corre risco de morte ou de sofrer sérios danos físicos;
- A natureza da emergência (mensagem de suicídio, ameaça de bomba, divulgação de pornografia infantil);
- O @nomedeusuário e o URL do Twitter das contas relacionadas ao pedido;
- Reprodução e/ou endereço dos Tweets que comprovam a emergência;
- A informação específica solicitada e por que essa informação é necessária para evitar a situação de emergência;
- A assinatura da autoridade policial
- Demais detalhes ou contexto da circunstância em particular.

Endereço para a remessa de requisições de informação ou ordens judiciais:

Twitter Brasil Rede de Informação Ltda.
Avenida Bernardino de Campos 98
3º andar, Sala 4
São Paulo - SP - CEP: 04004-040

O pedido de informações de usuários deve incluir o nome do usuário e a URL do perfil do Twitter em questão (exemplo: @safety e https://twitter.com/safety), detalhes específicos sobre as informações solicitadas. Um endereço de e-mail válido deve ser incluído para que o Twitter entre em contato com o solicitante após o recebimento do seu processo.

Como já dito a respeito do facebook, o Twitter fornece a algumas empresas, mediante pagamento, o seu fluxo completo de dados para que possa ser feita análise dos dados publicados no serviço, usualmente a serviço de grandes empresas para saber a reação do público a seus produtos, produtos de concorrentes e analisar tendências de mercado. Nada impede que esses dados sejam utilizados para finalidades como o mapeamento de ocorrência de doenças/fatos relevantes (já vi demonstração de empresa brasileira nesse sentido) ou para estudar a dinâmica de um protesto social, quais serão as próximas ações e locais de reunião.

5. REFERÊNCIAS

BRASIL. Presidência da República. Lei nº 12.830, de 20 de junho de 2013. Dispõe sobre a investigação criminal conduzida pelo Delegado de Polícia. Disponível em:
<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12830.htm>. Acesso em: 8 de janeiro de 2016.

BRASIL. Presidência da República. Lei nº 12.850, de 02 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei no 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>. Acesso em: 8 de janeiro de 2016.

BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. Manual de Cooperação Jurídica Internacional e Recuperação de Ativos: Cooperação em Matéria Penal / Secretaria Nacional de Justiça, Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI). - 2. ed. Brasília : Ministério da Justiça, 2012.

MALHEIRO, Emerson Penha. Cooperação Jurídica Internacional em Matéria Penal. Artigo publicado na internet, acessado em 27/12/2015, disponível em:
https://www.metodista.br/revistas/revistas-ims/index.php/RFD/article/viewFile/460/456

CABRAL, Bruno Fontenele. Considerações sobre cooperação policial internacional e poder requisitório do delegado de Polícia Federal. Artigo publicado na internet, acessado em 29/12/2015, disponível em: https://jus.com.br/artigos/36976/consideracoes-sobre-cooperacao-policial-internacional-e-poder-requisitorio-do-delegado-de-policia-federal

ANSELMO, Márcio Adriano. A criminalidade não tem fronteiras, e a polícia judiciária também não pode ter. Artigo publicado na internet, acessado em 28/12/2015, disponível em:
http://www.conjur.com.br/2015-dez-15/academia-policia-criminalidade-nao-fronteiras-policia-tambem-nao

SANNINI NETO, Francisco; CABETTE, Eduardo Luiz Santos. Poder requisitório do Delegado de Polícia. Artigo publicado na internet, acessado em 05/01/2016, disponível em: http://jus.com.br/artigos/32089

CAPÍTULO XI

Breves apontamentos sobre o uso da prova digital

Clayton Bezerra[135] *e Giovani Celso Agnoletto*[136]

1 - INTRODUÇÃO

A Internet trouxe inegáveis melhorias para nossas vidas, tanto profissional quanto pessoal. Facilidade na obtenção de informações, diversão, rapidez e eficácia nas ações são frutos inegáveis desse novo mundo, o mundo virtual, trouxe também um nova modalidade de crime, além de uma nova ferramenta para o cometimento de crimes antigos. O Criminoso agora é o mais rápido e com a capacidade de transpor fronteiras de idiomas, culturais e geo-físicas até mesmos de Países soberanos. O cibercriminoso é uma realidade que temos de enfrentar.

Concordamos com alguns autores que defendem o Direito Informático como ramo autônomo do Direito, considerando suas características próprias e específicas e defendemos que este novo direito englobe mudanças no Direito Processual Penal, visto que esta nova modalidade de crime necessita de uma nova sistemática de persecução penal e de polícia judiciária mais ágil e eficiente:

---

[135] O autor é Doutorando em Ciências Jurídica e Sociais pela Universidad Del Museo Social Argentino - UMSA, **Especialista em Direito e Processo Penal – AVM-Universidade Cândido Mendes – 2008,** Especialista em Direito Processual Civil – AVM Universidade Cândido Mendes - 2004, MBA em Gestão – Fundação Getúlio Vargas - 2003, Tutor da Academia Nacional de Polícia - ANP, É Delegado de Polícia Federal.

[136] O autor é aluno especial no Programa de Ciências da Comunicação do curso de Doutorado da Escola de Comunicação e Artes da Universidade de São Paulo – USP, mestre pelo Instituto Mauá de Tecnologia (área de meio-ambiente), pós graduado em Investigação Criminal pela Academia Nacional de Polícia – ANP-DF, pós graduado em Administração de Empresas pela Escola Superior de Propaganda e Marketing - ESPM-SP, graduado em Direito pela Universidade Bandeirante - Uniban-SP e também, graduado em Comunicação Social pela Escola Superior de Propaganda e Marketing - ESPM-SP.

> "Como conclusión, considerando su particular objeto, sus categorías próprias y la existencia de fuentes dedicadas, asi como la importância que revisten los bienes de la sociedad de la información y su específico sustrato físico o ámbito em la cual se producen los hechos, es decir, el sustrato tecnológico, podemos determinar que el derecho informático há devenido em una rama independiente del derecho, la cual, sin lugar a dudas, irá creciendo em importância proporcionalmente a la injerencia de la tecnología em el quehacer humano" (Anzit Guerrero, Ramiro El derecho informático y sus aspectos fundamentales: Buenos Aires: Catedra 2010)

Tal discussão é bastante atual e polêmica, e vai aio encontro do preconizado pela Convenção de Budapeste, também conhecida como convenção contra o cibercrime, que dispõe em seu preambulo de parte específica sobre a prova no Direito Processual em se tratando de crimes cibernéticos:

> "Preocupados com o risco de que as redes informáticas e as informações eletrônicas sejam igualmente utilizadas para cometer crimes e de que as provas dessas infrações sejam armazenadas e transmitidas através dessas redes".

Veremos mais adiante que tal fato já demonstra a importância que devemos dar a este objeto jurídico processual neste novo mundo que se apresenta que é o mundo virtual, em especial no tocante ao cibercrime, senão vejamos o mesmo dispositivo:

> Secção 2 – Direito Processual
> Título 1 – Disposições Comuns
> Art 14 – âmbito das Disposições Processuais
> 1 – Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para instruir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou procedimento penal.
> 2 – Salvo disposição em contrário constante do art. 21, cada Parte aplicará os poderes e procedimentos referidos no número 1:
> a) …
> b) …
> c) À recolha de prova de suporte eletrônico provas eletrônicas de qualquer infração penal.

A Convenção de Budapeste prossegue ainda com o Título 2 – Conservação expedita de dados informáticos armazenados (art 16 e 17) , com o Título 4 – Busca e Apreensão de dados informáticos armazenados (art 19) e com o título 5 – Recolha em tempo real de dados informáticos (art 20 e 21),os quais serão analisados ao longo do trabalho.

Necessitamos de um Processo Penal Digital específico para o combate ao

cibercrime, um processo penal mais rápido e eficiente, adaptado a nova realidade e que vai ao encontro do preconizado com o princípio constitucional da Eficiência na Administração Pública brasileira. Um bom exemplo é destacado no livro El Derecho Informático[137]. Sendo:

> "... em las postrimerías del siglo XIX la aparición de la fotografía instantánea y el avance de la tecnologia que permitió multiplicar las ediciones de los medios masivos de comunicación, trajeron como consecuencia la difusión con una qamplitud hasta el momento desconecida de hechos y eventos, los cuales afectaban la intimidad de las personas. Lhevando a que la doctrina y luego la jurisprudencia tuvieran que forzosamente redefinir el concepto de ïntimidad".

Uma coisa é certa, quanto mais demorarmos em nos proteger com medidas legais para o combate a este tipo de delito, mais ele crescerá. E como possui uma característica de auto renovação e desenvolvimento de tecnologias, mais difícil será acabar com a impunidade dos crimes cibernéticos que já possui uma geração econômica no patamar do tráfico internacional de entorpecentes, mas que não possui o mesmo viés de violência nem o esteriótipo dos guetos e favelas.

2 - DIREITO PROCESSUAL PENAL .

2.1) Definição de Direito Processual Penal

Para Baños[138] o direito processual penal é a passagem do Direito Penal em sua realidade abstrata (momento legislativo) para poder chegar a um aplicação concreta da lei. Passando assim por um rito ou processo. "en resumen, el derecho procesal es indispensable para traducir la norma penal abstracta em realidad concreta." e ainda "El derecho procesal es la rama del ordenamiento que regulamenta el sistema de normas constitucionales y supralehgales tendientes a dar vida práctica al drecho pena"[139]

Vemos que nos códigos de Processo são determinadas as formas pela qual vai se proceder a ação penal. Nele estão descritos os requisitos para a ação, os conceitos de local de crime, como se dá a competência para julgamento, os atores do processo (Réu, Juiz, Promotor, testemunhas etc.) as formas como são arrecadas as provas e quais são admitidas, os prazos, os recursos etc.

---

137 Anzit Guerrero, Ramiro El derecho informático y sus aspectos fundamentales: Buenos Aires: Catedra 2010

138 - Baños Javier Ignacio Sistema de Garantias Constitucionales em el Derecho Procesal Penal com Prólogo de Eugenio Raúl Zaffaroni, Buenos Aires: Lajouane 2009 pag 20

139 Baños Javier Ignacio Sistema de Garantias Constitucionales em el Derecho Procesal Penal com Prólogo de Eugenio Raúl Zaffaroni, Buenos Aires: Lajouane 2009 pag. 29

Para Reis, Processo Penal[140] é "o conjunto de princípios e normas que disciplinam a composição das lides penais, por maio da aplicação do Direito Penal.

A necessidade de um processo penal mais ágil para combater o cybercrime encontra guarita nas palavras de Sueiro[141] "La posibilidad de cometer este tipo de afectaciones a la distancia sin presencia material, desde conceptos fisicalistas de causa-efecto fáciles de apreciar, no solo será un problema para el titular del bien jurídico a la hora de prever el ataque y repelerlo, sino también, para el órgano jurisdiccional encargado de dirigir la investigación o imponer una condena."

2.2) Princípios e fundamentos do Direito Processual Penal

Dentre os diversos Princípios norteadores do Direito Processual Penal, como o da Inocência, da Defesa em Juízo, Juiz Natural, Do Devido Processo Legal, atentaremos ao que diz respeito ao objetivo do nosso trabalho que é o Princípio da Vedação de provas Ilícitas.

Tal Princípio está inscrito na Constituição da República Federativa do Brasil[142] e torna inadmissíveis em processo penal as provas por meio ilícito. No Brasil há também a inadmissibilidade da prova ilícita por derivação (Teoria dos frutos da árvore envenenada). Reis define "Constata-se, pois, que o Código de Processo Penal, a partir da edição da referida lei, perfilhou-se à teoria dos frutos da arvore envenenada (fruits of poisonous tree), segundo a qual a prova em si mesmo lícita, mas que foi obtida por intermédio da ação ilícita, deve também ser considerada ilícita."[143]

3 - PROVA

Ao escrever sobre provas em sua obra o professor Nucci[144] destaca: "Vale registrar que, quando cuidamos de provas, voltamos os nossos olhos para a busca da verdade, que, no processo penal, é denominada material, real ou substancial, justamente oara fazer contraste com a verdade formal ou instrumental do processo civil."

Uma das características do cibercrime é a de poder cometê-lo a distância, quer seja em outro estado ou província ou até mesmo em outro país (transnacionalidade). Pode-se até estar em um país (A), acessar o provedor que encontra-se no país "B" e fraudar uma conta em um País "C", ou até utilizar um

140 Reis Alexandre Cebrian Araújo Processo Penal Parte Geral São Paulo: Saraiva 14 edição pag. 1
141 Sueiro, obra citada pag 129
142 Art. 5o, LVI, da Constituição Federal do Brasil
143 Reis, obra citada, pag. 125
144 Nucci, Guilherme de Souza , Manual de processo penal e execução penal, 4 ed. Rev. Atual. e ampl – São Paulo: Editora Revista dos Tribunais 2008. pag 375

computador "escravizado" remotamente em um país "D" para cometer o crime descrito acima.

Pelo exposto vemos a importância crucial de uma investigação ágil, com cooperação entre os estados ou províncias de um Pais e até mesmo de uma cooperação internacional eficiente. Nesse contexto, o instituto jurídico da prova ganha destaque. "Frente a estas nuevas categorías de delitos de última generación, aparece una herramienta que permite demostralos ante la justicia: la prueba electrónica."[145]

Por tratar-se de trabalho próprio de Provas no Crime cibernético trataremos somente de alguns institutos específicos em matéria de Prova, contudo, no código de Processo Penal Brasileiro, de 1941, a Prova possui em Título próprio o de número sete (VII) e está dividido em:

- Capítulo 1 – Disposições Gerais (art. 155 a 157);
- Capítulo 2 - Do exame de corpo de delito, e das perícias em geral (art. 158 a 184);
- Capítulo 3 – Do interrogatório do acusado (art. 185 a 196);
- Capítulo 4 – Da confissão (art. 197 a 200);
- Capítulo 5 – Das perguntas ao ofendido (art. 201);
- Capítulo 6 – Das testemunhas (art. 202 a 225);
- Capítulo 7 – Do reconhecimento de pessoas e coisas (art. 226 a 228);
- Capítulo 8 – Da acareação (art. 229 e 230);
- Capítulo 9 - Dos documentos (art. 231 a 238);
- Capítulo 10 – Dos indícios (art. 239);
- capítulo 11 – Da busca e apreensão (art. 240 a 250).

3.1) Conceito de prova;

Para Reis[146], provar significa "demonstrar, no processo, a existência ou inexistência de um fato, a falsidade ou verdade de uma afirmação."

Capez[147] define assim este instituto "é o conjunto de atos praticados pelas partes, pelo juiz e por terceiros destinado a levar ao magistrado a convicção acerca da existência ou não de um fato, da falsidade ou veracidade de uma afirmação."

3.2) Meios de prova

Apesar do código de Processo Penal Brasileiro conter um rol de meios de prova (Testemunha, documentos, perícia etc.), o mesmo não é taxativo , ou seja, pode-se utilizar qualquer meio de prova adquirido de forma lícita. Vigora o Princípio

145 F. Lazaro, C. Y García (2008), Pruebas electrónicas ante los tribunales em la lucha contra ;a cibercriminalidad. Un proyecto Europeo, Enl@ce: Revista Venezolanoa de Información, Tecnología y Conocimiento, 5 (2), 139-152

146 Reis, obra citada. Pag 123

147 Capez, Fernando Curso de Processo Penal , São Paulo: Saraiva 2007 14a Edição Rev. E atual. pag 285

da Verdade Real "... de tal sorte que não há o que se cogitar qualquer espécie de limitação à prova, sob pena de se frustrar o interesse estatal na justa aplicação da lei."[148]

3.3) Finalidade das provas;

Parece bastante óbvia a finalidade das provas. Fornecer ao julgador elementos para a sua decisão. "A meta da parte, no processo, portanto, é convencer o magistrado, através do raciocínio, de que a *sua* noção da realidade é a correta, isto é, de que os fatos se deram no plano real exatamente como está descrito na sua petição."[149]

3.4) Valoração de provas;

De acordo com o passado histórico temos os sistemas:

3.4.1) Sistema ordálio ou as ordálias, que entregava a decisão ao sobrenatural. Tal sistema ainda é utilizado em algumas tribos da Africa. EX. Mulher acusada de adultério tem de passar ferro em brasa na língua. Caso não fique com queimaduras estará provada a sua inocência.

3.4.2) Sistema da prova Legal ou da certeza moral do legislador. A lei atribui um valor para cada tipo de prova, ficando o julgador adstrito a tal escore.

3.4.3) Sistema de íntima convicção ou da certeza moral do Juiz – A lei concede ao juiz uma liberdade ilimitada para decidir com queira. Não existe regras ou valoração de prova.

3.4.4) Sistema da livre convicção do juiz ou da persuasão. Para Capez[150] este sistema equilibra os sistemas anteriores. "O juiz tem liberdade para formar sua convicção, não estando preso a qualquer critério legal de prefixação de valores probatórios. No entanto, essa liberdade não é absoluta, sendo necessária a devida fundamentação"

3.5) Prova pericial;

Para Capez[151] a prova pericial :

> "...é um meio de prova que consiste em um exame elaborado por pessoa, em regra profissional, dotada de formação e conhecimentos técnicos específicos, acerca de fatos necessário ao deslinde da causa. Trata-se de um juízo de valoração científico, artístico, contábil, avaliatório ou técnico,

148 Capez Fernando obra citada pag 310
149 Nucci,obra citada, pag 376
150 Capez, Fernando obra citada pag 314
151 Caspez, Fernando obra citada pag 319

exercido por especialista, com o propósito de prestar auxílio ao magistrado em questões fora de sua área de conhecimento profissional."

Em Guia de estudo de processo penal Torres Neuquen[152] define "Orueba pericial es, entonces, la que se lleva a cabo cuando para conecer sobre los hechos controvertidos se requiere un conecimiento especial sobre determinada ciencia, arte, indudtria, profesión o actividad técnica especializada."

Considerando as características do crime cibernético as provas periciais terão grande destaque e serão fundamentais para a identificação da autoria destes delitos esta será abordada em capítulo próprio.

3.6) Prova Ilícitas;

Como já mencionado, nos regimes democráticos é comum a vedação a provas obtidas por meios ilícitos. Na recente história da América Latina como um todo, os diversos períodos de ditaduras militares vividas neste continente, nos mostraram a dura realidade de se viver em tal regime.

A vedação de provas ilícitas no processo é inerente ao Estado Democrático de Direito. Tal instituto encontra-se insculpido inclusive na Constituição da República Federativa do Brasil no artigo 5º[153]. Que diz " são inadmissíveis, no processo, as provas obtidas por meios ilícitos." também teve guarida no código de Processo Penal Brasileiro com o art 157[154].

> Art.157 São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais.(Redação dada pela Lei nº 11.690, de 2008)
> §1o São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008)
> §2o Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova. (Incluído pela Lei nº 11.690, de 2008)
> § 3o Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente. (Incluído pela Lei nº 11.690, de 2008)

[152] Neuquém, Torres, Guia de estúdio de processo penal:programa desarrolladode la matéria, 2ª edição, Buenos Aires: Editorial Estudio 2008

153 Art. 5o, LVI, da Constituição Federal do Brasil

154 Art. 157 – Código Penal Brasileiro.

3.7) Busca e Apreensão;

Tem especial atenção esta modalidade de medida cautelar tendo em vista que a prova pode desaparecer do mundo real e do mundo jurídico. A Busca e Apreensão pode ocorrer tanto na fase de investigação quanto na fase da ação penal.

Em se tratando de cibercrimes este instituto mereceu inclusive um título próprio[155] (Título 4 – Busca e apreensão de dados informáticos armazenados) na Convenção de Budapeste, Convenção Contra o Cibercrime.

3.8) Prova digital no Cibercrime;

Não há no direito brasileiro nenhuma restrição a provas digitais. Em se tratando de crimes praticados na Internet ou através dela. A doutrina Policial adotada pela Academia Nacional de Polícia (ANP – Brasil) entende que "'A Internet é um local de crime real e, portanto, deixa vestígios como registros de conexão à Internet, registros de utilização de serviços na Internet (envio e recebimento de e-mails, registros de trocas de mensagens, download de arquivos entre outros), além, obviamente, dos próprios computadores utilizados para a prática criminosa".

Para Pinheiro (2010)[156] "..a prova em meios eletrônicos é mais facilmente

155 Artigo 19º - Busca e apreensão de dados informáticos armazenados

1. Cada Parte adotará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a procederem a buscas ou a acederem de modo similar:

a) A um sistema informático, ou a parte dele, bem como aos dados informáticos aí armazenados; e

b) A um suporte que permita armazenar dados informáticos, no seu território.

2. Cada Parte adotará as medidas legislativas e outras que se mostrem necessárias para assegurar que, sempre que as suas autoridades procedam a buscas ou acedam de modo similar a um sistema informático específico ou a parte dele, em conformidade com o disposto na al. a) do n.º 1 do presente artigo, e tenham razões para crer que os dados procurados se encontram armazenados noutro sistema informático ou em parte dele, situado no território da Parte, e que tais dados são legalmente acessíveis a partir do sistema inicial ou estão disponíveis através desse sistema inicial, as referidas autoridades estejam em condições de estender, de forma expedita, a busca ou o acesso de modo similar ao outro sistema.

3. Cada Parte adotará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a apreender ou a aceder de modo similar aos dados informáticos relativamente aos quais o acesso foi efetuado em aplicação do disposto nos n.ºs 1 ou 2 do presente artigo. Tais medidas incluem as seguintes prerrogativas:

a) Apreender ou obter de modo similar um sistema informático ou parte deste, ou um suporte de armazenamento de dados informáticos;

b) Efetuar e conservar uma cópia de tais dados informáticos;

c) Preservar a integridade dos dados informáticos pertinentes armazenados;

d) Tornar inacessíveis ou remover tais dados informáticos do sistema informático acedido.

4. Cada Parte adotará as medidas legislativas e outras que se mostrem necessárias para habilitar as suas autoridades competentes a ordenar a qualquer pessoa que conheça o funcionamento do sistema informático ou as medidas aplicadas para proteger os dados informáticos nele contidos , que forneça todas as informações razoavelmente necessárias para permitir a aplicação das medidas previstas nos n.ºs 1 e 2 do presente artigo.

5. Os poderes e procedimentos referidos no presente artigo deverão estar sujeitos ao disposto nos artigos 14º e 15º da presente Convenção.

156 Pinheiro, Patricia Peck Direito Digital, São Paulo: Saraiva 2010 pag 75

averiguada do que no mundo real, uma vez que há como rastrear quase tudo que acontece." e complementa "Além de não existir nenhum óbice jurídico, o documento eletrônico assinado digitalmente torna factível a visualização de qualquer tentativa de modificação do documento por meio da alteração da sequência binária." e finaliza:

> "Todavia, nunca alcançaremos a certeza inequívoca de confiabilidade, tanto no sistema eletrônico quanto no tradicional, ou em outro qualquer, mas, ainda assim, é possível imprimir uma confiabilidade necessária para a concretização de negócios jurídicos nesse meio.
>
> Podemos afirmar que a tecnologia trouxe mais ferramentas para a validação jurídica das provas, algo que se busca há muito, e hoje, por certo, já há força legal muito maior numa prova composta por um e-mail do que apenas no testemunho oral ou em um mero fax; o mesmo para uma assinatura digital ou biométrica do que apenas o número de um RG ou CPF anotados a mão sem conferência do documento ou cuja foto, normalmente está desatualizada. A final, para todos nós, o teste de DNA continua sendo considerado prova inequívoca de autoria, apesar de não ter lei e não ser 100% de certeza."[157]

Certo é que a pessoa encarregada de arrecadação e armazenamento da Prova Digital também é um fator primordial na aceitabilidade e confiabilidade da mesma. "El soporte técnico, por un lado, y las garantías de autenticidad, por outro, completan el cuadro de factores que más influyen em los órganos juzgadores europeos a la hora de conceder mayor o menor valor probatorio a una determinada prueba."[158]

Abaixo, mostraremos um resumo (páginas 148 e 149) da pesquisa realizada no artigo "pruenbas electronicas ante los tribunales em la lucha contra ;la cibercriminalidad. Un proyecto europeo"[159], no qual fica demonstrado a diversidade de opiniões dos diversos atores (Juízes, Promotores, Juristas e Técnicos em informática) sobre as vantagens e desvantagens do uso da Prova digital em matéria de Processo Penal:

---

157 Pinheiro, obra citada pag 214/215

158 F. Lazaro, C. Y García (2008), Pruebas electrónicas ante los tribunales em la lucha contra ;a cibercriminalidad. Un proyecto Europeo, Enl@ce: Revista Venezolanoa de Información, Tecnología y Conocimiento, 5 (2), 139-152

159 F. Lazaro, C. Y García (2008), Pruebas electrónicas ante los tribunales em la lucha contra ;a cibercriminalidad. Un proyecto Europeo, Enl@ce: Revista Venezolanoa de Información, Tecnología y Conocimiento, 5 (2), 139-152

Atores	Vantagens	Desvantagens
Juízes	- Confiabilidade (Objetividade e exatidão); - Facilidade e rapidez de obtenção e uso, assim como conservação e armazenamento; - Uso de documentos e firmas eletrônicas favorece o desenvolvimento do comércio eletrônico e diminui os custos.	Falta de conhecimento dos juízes para verificar a sua autenticidade; - Dificuldade de estabelecer um valor jurídico devido ao desconhecimento sobre os procedimentos de processamento de dados e a interpretação das leis processuais a respeito do tema; -Dificuldades na conservação e armazenamento - Medo da vulnerabilidade e facilidade como as provas podem ser manipuladas
Juristas	- Informação exata, completa, clara, precisa, veraz, objetiva e neutra; - Uso de documentos e firmas eletrônicas favorece o desenvolvimento do comércio eletrônico e diminui os custos.	- Dificuldade de estabelecer um valor jurídico devido ao desconhecimento sobre os procedimentos de processamento de dados e a interpretação das leis processuais a respeito do tema; - Medo da vulnerabilidade e facilidade como as provas podem ser manipuladas; - Dificuldades na conservação e armazenamento
Técnicos	- Informação exata, completa, clara, precisa, veraz, objetiva e neutra; - Uso de documentos e firmas eletrônicas favorece o desenvolvimento do comércio eletrônico e diminui os custos.	- Falta de suporte legal e modelos de certificação digital; - O processo de obtenção e interpretação da informação requer muito tempo e tem alto custo. (para poder transformá-la e informações compreensíveis aos juízes e promotores)
Outros Informantes	- Solidez, confiabilidade, Viabilidade; - Uso de documentos e firmas eletrônicas favorece o desenvolvimento do comércio eletrônico e diminui os custos.	

3.2) História da prova digital no Crime Cibernético

Veremos abaixo em tabela retirada da obra Direito Digita de Patrícia Peck Pinheiro um demonstrativo de como se deu a aceitação dos meios informáticos e suas ferramentas como prova no âmbito do processo penal e do processo civil no Direito Brasileiro.

Ano	Poder Judiciário	Sociedade Civil
2002 a 2003	Monitoramento de e-mail: Considerado como invasão de privacidade	Monitoramento de e-mail: Não era feito ou era feito de maneira manual e esporádica, o empregador se responsabilizava pelos atos do empregado e pelo mau uso da informação, não podendo exercer vigilância por causa das questões de definição dos limites de intimidade
	E-mail como prova: Era restrita. Não serve como prova única, mas pode servir para ajudar as demais provas	E-mail como prova: Empresa e colaborador possuem dúvidas quanto à admissibilidade do e-mail como prova e não as utilizam com frequência.
2004 a 2006	Monitoramento de e-mail: Passa a ser admitido, nos casos em que a empresa comprova que havia ciência prévia do empregado.	Monitoramento de e-mail: As empresas passam a adotar procedimentos mais rígidos para a proteção de seus ativos, realizando monitoramento e adquirindo ferramentas para tal, mesmo que sem a ciência prévia do empregado, ainda sem a existência política de segurança da informação, ou a previsão tímida em normas esparsas de e-mail e Internet (que não deixavam claro se podia usar para fim pessoal a ferramenta de trabalho).
	E-mail como prova:	E-mail como prova: Colaboradores questionavam a privacidade do uso, pela empresa, dos e-mails para a prova de demissão por justa causa.

	Monitoramento de e-mail: é aceito já que a ferramenta de trabalho é do empregador e o mesmo é responsável por seu uso indevido por parte dos empregados	Monitoramento de e-mail: A empresa possui política de uso dos recursos e política de segurança da informação, aplicando a seus funcionários sempre que necessário. No entanto, ainda há uma zona cinzenta em ambientes de mobilidade, home office e terceirizados, que também precisa estar previsto em normas, códigos de conduta e contratos.
2007 a 2009	E-mail como prova: Admissão de novas tecnologias (e-mail, Orkut, Youtube, fotografia digital, mensagens sms etc) como prova, desde que não haja comprovação de alteração dos dados do e-mail. Ou seja, deve ser preservado de forma íntegra e pode haver perícia no original eletrônico.	E-mail como prova: Tanto as empresas como os colaboradores se valem de provas eletrônicas para fundamentar suas alegações. Não apenas o e-mail, mas também outras evidências eletrônicas.

No Código de Processo Penal anotado do professor Damásio de Jesus vemos que o Ônus da prova no Direito Processual Penal cabe a que alegar[160], contudo, uma nova realidade está se apresentando nos crimes informáticos, pois a complexidade de questões técnicas pode inviabilizar as punições por parte do Estado ao cibercriminoso.

Para Demócrito Reinaldo Filho[161] o ônus da prova neste tipo de delito tem de ser transferido ao acusado, "sob pena de comprometer irremediavelmente a atividade de persecução criminal". E o mesmo autor prossegue "As novas leis que dispuserem sobre crimes informáticos, sobretudo a modalidade de acesso não autorizados a sistema computacional, têm de prever o ônus da prova do réu, sempre que este alegar ter sido vítima de um ataque de vírus "spywere"[162] ou

160 Jesus, Damásio Código de Processo penal anotado 19 edi. Atual. São Paulo : Saraiva. 2002 . Art 156 Código de Processo Penal Brasileiro.

161 Revista Jus Vigilantibus, Domingo, 30 de novembro de 2003

162 Spywere - consiste em um programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o seu conhecimento nem o seu consentimento. (Wikipedia brasil http://pt.wikipedia.org/wiki/Spyware 30 de setembro de 2011.

"Trojan"[163], ou qualquer outra defesa que represente um ônus de prova técnica exagerado para a acusação.

Nos Estados Unidos a alteração do ônus da prova em matéria de crime informático já ocorre com a edição do Protect act[164] quando o país se deparou com alegação da defesa dos acusados de que as imagens em casos de pornografia infantil eram na verdade montagens e edições com adultos.

Podemos ver que o assunto é amplo e rico em interpretações, contudo temos de ter a noção de que o crime cibernético requer uma estrutura investigativa, pericial e judicial ágil.

É fundamental a coleta, armazenamento, lapidação e análise das diversas condutas criminosas perpetradas, visto que vários são os crimes cometidos de forma conexa e acompanhada, restando nesta ferramenta a maneira mais eficiente de se buscar os elos de ligação para a captura de criminosos e quadrilhas especializadas no cibercrimes.

Muito tem sido discutido sobre conceitos e novas tipificações em matéria de Direito Penal Informático e se esta é ou não um novo ramo independente de Direito (assim como o Direito Penal, Civil, Comercial etc.), mas joga-se a segundo plano ou ao completo descaso as questões relativas ao Direito Processual (informático ou não) no que tange à materialidade, territorialidade, investigação e prova nestes tipos de delito, tal fato tem de mudar se quisermos enfrentar com eficiência o crime cibernético.

4 - A PROVA NO DIREITO COMPARADO E A CONVENÇÃO DE BUDAPESTE

Diversos países já possuem legislações específicas para tratar as demanda relacionadas a crimes cibernéticos. Entretanto, muito do que se vê é a busca por tipificação de delitos para fazer frente ao Princípio da Reserva Legal, contudo pouco se busca em matéria de processo Penal.

Podemos citar os seguintes países seguindo a obra de Eduardo E. Rosendo Derecho Penal e Informática 2007 pag 218 / 282:

163 Trojan - Um **cavalo de Troia** (em inglês *Trojan horse*) é um malware (programa malicioso) que age como a lenda do cavalo de Troia, entrando no computador e liberando uma porta para uma possível invasão e é fácil de ser enviado, é só clicar no ID do computador e enviar para qualquer outro computador. http://pt.wikipedia.org/wiki/Trojan em 30 de setembro de 2011.

164 Protect Act Lei americana de proteção a pornografia Infantil.

País	Ano	Assunto
Alemanha	1986	Pirataria informática, Dano , Alteração de dados, Sabotagem de computadores etc.
Espanha	1995	ataques que se produzem contra o Direito de intimidade
Áustria	1987	Destruição de dados pessoais
Chile	1993	Lei n. 19223 (Lei de delitos informáticos de 28 de maio de 1993)
França	1988	Lei n. 88-19 de 5 de janeiro de 1998
Estados Unidos	1986	Ata de Fraude e Abuso Computacional
Itália	1993	Art 615 código Penal Italiano
Venezuela	2001	Lei Especial contra Delitos Informáticos (Diário Oficial n. 37.313 de 30 de outubro de 2001)
México	1999	Reforma do Código Penal Mexicano Artigos 210 e 2011
Bolívia	1997	Reforma do código Penal Boliviano Artigo 363
Costa Rica		Lei 8148 que adicionou os artigops 196 bis, 217 bis e 229 bis ao código penal Costarriquenho.
Perú	2001	Capítulo especial sobre delitos informáticos no Codigo Penal Peruano art 207 e seguintes
Equador	2002	Lei de Comércio, Mensagens Eletrônicas e Mensagens Eletrônicas de Dados incorpora os artigos 184, 185, 186, 415 e 416 ao Código Penal Equatoriano
Grã Betanha	1991	Lei de Abusos Informáticos
Portugal	1991	Lei Especial 109/1991
Japão	1987	Artigos 161 bis e seguintes

A convenção de Budapeste foi firmada pelo Conselho da Europa em 23 de novembro de 2001 e entrou em vigor no ano de 2004. Tal convenção formaliza a intenção da Comunidade Europeia em unificar uma legislação visando combater o cibercrime ao uniformizar terminologias, definições e prever a cooperação internacional, fundamental em uma passibilidade de crimes que avançam por diversas fronteiras. O Brasil não aderiu ao tratado na esperança da aprovação de sua Lei contra os crimes cibernéticos.

Está dividida em quatro capítulos sendo:

- I – Utilização de terminologia;
- II – Medidas a empreender a nível nacional – direito substantivo e direito processual;
- III – Cooperação internacional;
- IV – Disposições Finais.

Dispõe em seu preambulo de parte específica sobre a prova no Direito Processual em se tratando de crimes cibernéticos:

> "Preocupados com o risco de que as redes informáticas e as informações eletrônicas sejam igualmente utilizadas para cometer crimes e de que **as provas dessas infrações sejam armazenadas e transmitidas através dessas redes**". (grifo nosso).

Neste novo cenário em que vivemos, apresentam-se várias novas formas de delito, quer seja, usando a internet como ferramenta ou sendo a própria finalidade do crime em si. Independentemente do modo, as discussões de novas legislações para combater o cibercrime passam ao largo da discussão da matéria processual.

Os meios de prova na Internet são diferentes dos modelos de prova pensados na elaboração dos antigos códigos de processo penal. Para citar como exemplo o código de Processo Penal Brasileiro data de 1941 ou seja, pensado e discutido na década de 30 do século XX par ser editado na década de 40 onde não se imaginava o uso de computadores nem de uma rede que ligaria o mundo inteiro.

Uma das características do cibercrime é a transnacionalidade e vemos aí a importância que devemos dar a este objeto jurídico processual neste novo mundo que se apresenta, tal instituto já foi discutido e aprovado no principal documento sobre o cibercrime que é a Convenção de Budapeste, se não vejamos[165]:

> Secção 2 – Direito Processual
> Título 1 – Disposições Comuns
> Art 14 – âmbito das Disposições Processuais
> 1 – Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para instruir os poderes e os procedimentos previstos na presente Secção, para fins de investigação ou procedimento penal.
> 2 – Salvo disposição em contrário constante do art. 21, cada Parte aplicará os poderes e procedimentos referidos no número 1:
> a) …
> b) …

165 Corrobora com este entendimento as palavras do professor Anzit Guerrero "La ONU considera que el problema de los delitos informáticos se eleva a la escena internacional, por cuanto éstos constituyen una nueva forma de crimen transnacional y su combate reueiere de una eficaz cooperación internacional concertada. Anzit Guerrero pag 150

c) **À recolha de prova de suporte eletrônico provas eletrônicas de qualquer infração penal. (grifo nosso)**

Outros institutos são abordados no mesmo documento, sendo:
– Título 2 – Conservação expedita de dados informáticos armazenados (art. 16 e 17) – Aplicam-se a dados armazenados que já foram recolhidos e armazenados "pretende-se assegurar que as autoridades competentes disponham das capacidades necessárias para emitir uma ordem, ou obter a preservação expedita de dados informatizados armazenados"[166].

- Título 4 – Busca e Apreensão de dados informáticos armazenados (art. 19) - "Visa a modernização e harmonização das legislações nacionais relativamente à busca e apreensão desses dados para a obtenção de provas."[167];

– Título 5 – Recolha em tempo real de dados informáticos (art. 20 e 21) – É o recolhimento em tempo real das transmissões, no Brasil é chamada interceptação telemática. Ë um expediente eficaz já que muitos desses criminosos utilizam a própria internet para se comunicar (e-mail, MSN, SKYPE etc.). Para Venancio "Dessa Forma a interceptação das comunicações informáticas é tão importante como a interceptação de telecomunicações."[168]

5 - CONCLUSÃO

Nossas vidas mudam, assim como nossos pensamentos inclusive repercutindo sobre nosso modo de falar e escrever. O que era usual hoje, já não o é amanhã.

No Brasil estamos presos ao pensamento do judiciário por falta de previsão legal para o julgamento dos crimes cibernéticos, esta analogia e remendos não trazem nenhuma segurança jurídica e prejudica a investigação policial pois esta fica amarrada aos pilares do princípio da legalidade e de outros como é o caso do Princípio da Obrigatoriedade. Tal princípio abarrotas as delegacias de polícia judiciária[169] e por consequência o Ministério Público e o Poder Judiciário a cada

166 Venancio, Pedro Dias. Breve introdução da questão da Investigação e meios de prova na criminalidade informática, Lisboa: Verbo jurídico, 2006

167 Venancio, Pedro Dias. Breve introdução da questão da Investigação e meios de prova na criminalidade informática, Lisboa: Verbo jurídico, 2006

168 Venancio, Pedro Dias. Breve introdução da questão da Investigação e meios de prova na criminalidade informática, Lisboa: Verbo jurídico, 2006

169 Anualmente são demandados exames periciais em mais de 6.000 discos rígidos e computadores apreendidos pela Polícia Federal. O Volume de dados contidos nesse material é da ordem de 720 terabytes, o que corresponde a aproximadamente 36 vezes o conteúdo da maior biblioteca do mundo. Informações de vital importância para a investigação e persecução penal fazem parte dessa imensa massa de dados." Costa,

fraude verificada em uma conta corrente via internet banking ou de Cartão de Crédito/Débito clonados.

Um novo mundo se apresentou para a humanidade e teremos que lidar com suas características, tanto benignas quanto as malignas. O mundo "virtual" é uma realidade e necessitamos interpretar e ajustar nossas legislações para aplicarmos a essa realidade, pois os conflitos neste novo cenário já se fazem presente e possuem características não pensadas em nossa realidade pretérita. Algumas dos paradigmas do nosso mundo "concreto" não são aplicáveis, ou o são de maneira ineficaz no caso concreto.

O Direito Penal e Processual Penal, precisam ser repensados visando adequar a legalidade das ações com a realidade mundial, integrando os objetivos de prevenção e repressão da criminalidade além da busca de uma maior eficiência por parte dos Estados, isso passa por uma cooperação internacional prática e ágil, uma uniformização de processos e tipos penais e um maior preparo técnico por parte dos operadores do direito, senda a capacitação de Juízes e Promotores de Justiça ponto fundamental da efetiva punição aos cibercriminosos.

A prova digital precisa ser bem arrecadada, bem armazenada, bem explicada e bem entendida (pelos juízes e promotores) para ter validade e eficácia e eficiência.

Levi Roberto "Um método para sistematização do processo investigatório de análise da informação digital. Sixth International Conference on Forensic Computer Science – IcoFCS – 2011, Brasília: ABEAT editora 2011, pag.16.

6 - REFERÊNCIAS

ANZIT GUERRERO, Ramiro, El derecho informático y sus aspectos fundamentales, Buenos Aires: Cathedra Jurídica 2010

BAÑOS, Javier Ignacio, Introdución al derecho procesal penal; Buenos Aires: Jajouane 2011

BAÑOS, Javier Ignacio, Sistema de Garantias Constitucionales em el Derecho Procesal Penal com Prólogo de Eugenio Raúl Zaffaroni, Buenos Aires: Lajouane 2009

CAPEZ, Fernando, Curso de processo pena, São Paulo: Saraiva 2007

INSA, F. Lazaro, C. Y García Pruebas electrónicas ante los tribunales em la lucha contra ;a cibercriminalidad. Un proyecto Europeo, Enl@ce: Revista Venezolanoa de Información, Tecnología y Conocimiento, 5 (2), 139-152 2008

LEMOS, Ronaldo, Direito tecnologia e Cultura, Rio de Janeiro: FGV 2005

NEUQUÉN, Torres, Guia de estudio de proceso penal: programa desarrollado de la matéria, 2a edição, Buenos Aires: Editorial Estudio 2008

NUCCI, Guilherme de Souza, Manual de Processo Penal e Execução Penal, Editora Revista dos Tribunais 2008

REIS, Alexandre Cebrian Araújo, Processo Penal Parte Geral São Paulo: Saraiva 14 edição 2009

PINHEIRO, Patricia Peck, Direito digilal, São Paulo: Saraiva 2010

ROSENDE, Eduardo E., Derecho penal e informática, Buenos Aires: Fabián J Di Placido Editor 2007

SUEIRO, Carlos, Analisis integrado de la criminalidade informática, Buenos Aires: Fabián J Di Placido Editor 2007

TOBARES CATALA, Gabriel H, Delitos informáticos, Cordoba: Advocatus 2010

VENÂNCIO, Pedro Dias, Breve introdução da questão da Investigação e meios de prova na criminalidade informática, Lisboa: Verbo jurídico 2006

Capítulo XII

Perícia computacional e investigação de delitos informáticos: importância e desafios contemporâneos

Emerson Wendt[170]
emersonwendt@gmail.com

Higor Vinícius Nogueira Jorge[171]
contato@higorjorge.com.br

A constante evolução tecnológica que acompanhamos na contemporaneidade, principalmente considerando a inserção de inúmeros dispositivos que acessam a rede mundial de computadores, proporciona uma exploração criminal mais acentuada relativa às vulnerabilidades decorrentes do uso massivo desses dispositivos e suas aplicações. Por isso, os denominados crimes cibernéticos - ou mais amplificadamente os delitos informáticos[172] - têm acompanhado esse ritmo de crescimento e, constantemente, têm-se observado o surgimento de novas ameaças tecnológico-digitais[173].

Essas "novas" formas de praticar delitos representam um grande desafio para os órgãos da persecução penal, que devem ser/estar instrumentalizados para o enfrentamento e investigação criminal, cuja estrutura nacional depende de melhorias[174]. A forense computacional tem, também, de acompanhar esses

[170] Mestrando em Direito e Sociedade (Unilasalle, Canoas-RS). Delegado de Polícia Civil no RS. Lattes: http://lattes.cnpq.br/9475388941521093.

[171] Especialista em Polícia Comunitária (Unisul, Palhoça-SC). Delegado de Polícia Civil em SP. Lattes: http://lattes.cnpq.br/7040686244829651.

[172] Conceito adotado pela Lei 12.737/12, conhecida por Lei Carolina Dieckmann.

[173] As empresas de antivírus Kaspersky (http://brazil.kaspersky.com/), McAfee (http://www.mcafee.com/br/mcafee-labs.aspx), TrendMicro (http://blog.trendmicro.com/ e http://www.trendmicro.com.br/) e Symantec (http://www.symantec.com/about/profile/researchlabs.jsp) têm divulgado, periodicamente, dados sobre as ameaças e vulnerabilidades correntes, bem como projeções para os anos vindouros.

[174] Vide estrutura atual de combate aos crimes praticados pelos meios tecnológico-digitais no Brasil na lista de órgãos policiais elaborada por Emerson Wendt: WENDT, Emerson. **Lista dos Estados que possuem Delegacias de Polícia de combate aos Crimes Cibernéticos**. 2014. Disponível em:

avanços e caminhar ao lado da investigação criminal, pois é, no caso dos delitos relacionados à informática e telemática, principalmente, fundamental para o esclarecimento pleno dos fatos.

Assim, a forense computacional, considerada um conjunto de técnicas para identificar, coletar e caracterizar os dados e informações registradas nos dispositivos informáticos e telemáticos relacionados com a prática de crimes, a cada dia tem tido um incremento na sua utilização em razão do aumento na incidência destes delitos, embora perceba-se a sua não estruturação, principalmente em âmbito dos Estados brasileiros, prejudicando o bom andamento das investigações criminal. Há que se afirmar, de pronto, a necessidade de fomento desse ramo pericial, cujo futuro é promissor e fundamental para os trabalhos policiais.

> A forense computacional é definida como
> um conjunto de técnicas, cientificamente comprovadas, utilizadas para coletar, reunir, identificar, examinar, correlacionar, analisar e documentar evidências digitais processadas, armazenadas ou transmitidas por computadores.[175]

Uma característica relevante dos delitos cibernéticos é que seus autores estão sempre procurando inovar e criar novos estratagemas para o êxito da empreitada ou para aumentar a possibilidade de impunidade. Sob esta perspectiva, o perito que realizará a análise nos dispositivos utilizados na prática desses delitos deve acompanhar essas inovações e estar preparado para enfrentar/analisar medidas de evasão realizadas pelos criminosos.

Por esses motivos, o objetivo deste texto é abordar os principais aspectos técnicos relativos à perícia, principalmente sob a ótica policial e pericial, enfocando sua sistematização e importância frente aos desafios impostos pela contemporaneidade, baseada na comunicação em rede[176].

A forense de computadores também é conhecida como *Forense Digital*, *Forense Computacional*, *Perícia Computacional*, *Computação Forense, Perícia Digital*, dentre outras nomenclaturas que poderão encontrar nas publicações da área[177]. Em suma, ela é utilizada para a realização de investigações digitais e tem como objetivo principal a compreensão dos eventos ocorridos, aplicando-se ao processo as etapas tradicionais de forense (identificação, coleta, exame, análise e resultados[178]).

<http://www.emersonwendt.com.br/2010/07/lista-dos-estados-com-possuem.html>. Acesso em: 24 mai. 15.

[175] PIRES, Paulo S. da Motta. Forense Computacional: uma Proposta de Ensino. Disponível em: <http://www.leca.ufrn.br/~pmotta/ensino-forense.pdf>. Acessado em: 20 mar. 2005.

[176] O texto foi inicialmente produzido para integrar a 2ª Edição do livro "Crimes Cibernéticos: Ameaças e Procedimentos de Investigação", lançado em 2013 pelos autores (WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: Ameaças e procedimentos de investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013.).

[177] Vide DELLA VECCHIA, Evandro. **Perícia Digital**: da investigação à análise forense. Campinas: Millenium Ed., 2014.

[178] O "Guia básico de investigação computacional para Windows", da Microsoft (disponível <https://technet.microsoft.com/pt-br/library/dd458998.aspx>, acesso em 16 mai. 2015), apresenta, de forma

A imagem infra, extraída do site Forense Computacional[179], aborda os principais aspectos da etapa tradicional da forense computacional:

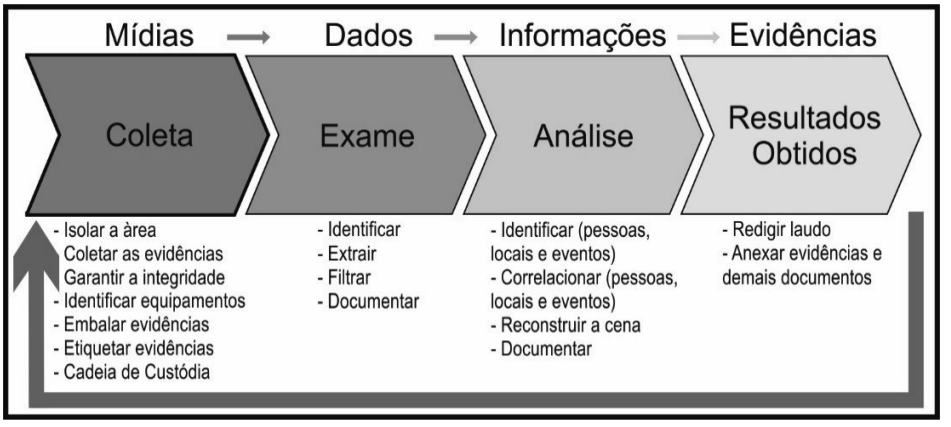


Figura 1 Fases da perícia forense (fonte: Forense Computacional)

A ideia, então, em relação a este tipo de perícia é a mesma de qualquer forense, pois leva em conta o princípio da "troca de Locard", pelo qual toda a pessoa que passa pela cena de um crime, deixa algo de si e leva algo consigo[180]. Assim, de forma similar, toda a pessoa que comete um delito cibernético, deixa rastros no sistema comprometido, seja ele um *pendrive* ou um computador, por exemplo. Em algumas situações, os rastros podem ser difíceis de serem seguidos, mas existem e bons profissionais são capazes de encontrá-los.

De acordo com Fernando de Pinho Barreira, a internet e outros meios de comunicação modernos,

---

resumida, as quatro fases da investigação e acompanhamento dos processos nas análises de evidências digitais. Segundo o referido Guia deve-se:

I - Avaliar a situação - Análise do escopo da investigação e ação a ser adotada.

II - Obter dados - Reunião, proteção e preservação das evidências originais.

III - Analisar os dados - Exame e correlação das evidências digitais com os eventos de interesse que irão auxiliá-lo na elaboração do caso.

IV - Relatar a investigação - Reunião e organização das informações coletadas que irão compor o relatório final.

[179] FORENSE COMPUTACIONAL. **Processo de Investigação**. Disponível em: <https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao>. Acesso em: 15 jun. 2015.

[180] Pelo princípio da troca de Locard, quem passa por uma cena de crime, real ou virtual, deixa e/ou leva vestígios consigo. O princípio é baseado nas concepções de Edmond Locard, considerado um dos principais expoentes da ciência forense. Esses vestígios, sob o aspecto comunicacional da Internet (*virtual*), são obtidos através dos registros (*logs*), onde o que fica registrado é, por exemplo: o arquivo produzido, acessado, modificado no computador, *tablet* ou *smartphone*; a conexão à Internet por meio de um provedor; o registro de acesso a uma determinada aplicação na *web*, como um *chat*, uma rede social, um correio eletrônico e as várias funcionalidades e aplicações existentes. Vide AZEREDO, Caroline Machado de Oliveira; CARLOS, Paula Pinhal de; WENDT, Emerson. **A Internet e a violência contra a mulher**: uma análise sobre a aplicação da Lei Maria da Penha aos casos de violência psicológica no contexto virtual. No prelo.

> apresentam tanta segurança quanto as formas de interação e comércio convencionais. Isto porque não existem dois mundos - um mundo virtual e outro real - e sim um mesmo mundo real virtualizado. Ou seja, as interações nos meios eletrônicos refletem as mesmas relações jurídicas já existentes, de modo que a maioria dos ilícitos igualmente podem ser praticados com o uso da Internet. Os ilícitos mais comuns nesse meio são os crimes contra a honra - calúnia, injúria e difamação - alguns crimes patrimoniais, como o furto mediante fraude (fraude Internet Banking), estelionatos; crimes de ódio - preconceitos contra etnias, credos, naturalidades, preferências sexuais, políticas, etc. - e de pornografia infantil. Importante é destacar que todas essas formas de crimes não ficam impunes, uma vez que é possível rastrear os criminosos e formar provas eletrônicas suficientes - e até com mais facilidade - que as produzidas contra os crimes convencionais. A perícia forense computacional é a ciência que se dedica a formar e analisar essas provas. Através de métodos, ferramentas e técnicas forenses, os peritos conseguem analisar as evidências e descobrir mesmo os criminosos mais dissimulados, gerando subsídios para a resposta penal às vítimas, ou seja: a condenação desses criminosos. Com a disseminação dos meios de prevenção que podem ser utilizados pelo Internauta e o aumento do conhecimento informático, bem como o constante empenho das forças de segurança, essa criminalidade tende a baixar a patamares pouco significativos, se comparados aos crimes praticados de modo convencional.[181]

A forense na área digital ou eletrônica, pode ter inúmeros usos: (a) perícia criminal, relacionada às atividades de polícias judiciárias, Civil e Federal, e dos Ministérios Públicos, Federal e Estadual; (b) Segurança da Informação e Protocolos e Termos de Uso relacionados; (c) perícia criminal, relacionadas às atividades judiciais e/ou jurídicas, do Poder Judiciário, em seus diversos campos além do criminal, como o Cível, Trabalhista, Fazendário etc.182; (d) auditorias, principalmente em ambientes coorporativos, públicos e/ou privados; (e) atividades de fiscalização fiscal/fazendária, tanto Federal quanto Estadual; (f) em sistemas antifraude e de defesa cibernética/lógica; (g) em compliance (monitoramento e desrespeito de regras de SI e TIC, formação de provas cíveis e

[181] BARREIRA, Fernando de Pinho. **Os Crimes Eletrônicos e A Perícia Criminal em Forense Computacional**. Disponível em: <http://fernandodepinhobarreira.wordpress.com/2013/06/20/os-crimes-eletronicos-e-a-pericia-criminal-em-forense-computacional>. Acesso em: 20 jun. 2013.

[182] São alguns dos exemplos de aplicações práticas da forense computacional no âmbito criminal: obtenção indevida de dados que possibilitem a movimentação financeira fraudulenta (fraudes financeiras); furto de informações sigilosas (espionagem comercial e industrial); destruição de propriedade (vírus, vandalismo, hacktivismo etc.); falsa identidade; chantagem, extorsão, ameaça, constrangimento ilegal; produção de imagem "pornográfica" envolvendo "menores"; distribuição de material pornográfico envolvendo menores; fornecimento de meios para a produção ou distribuição; aliciamento de crianças através da rede mundial de computadores, dentre outras tipificações.

trabalhistas); e, (h) em atividade de inteligência, principalmente cibernética e de segurança pública e de Estado.

São dois os principais tipos de forense computacional: online e o *post mortem* (ou *off line*). No primeiro, o sistema está ligado e é dinâmico, sendo que os dados mudam ou podem mudar durante a análise, sendo o principal objetivo a análise de conteúdos voláteis. Neste caso, importante que se diga, é indispensável a "fé pública" do profissional encarregado da atividade. Já no segundo, no método *off line*, o sistema está desligado e é estático, além de os dados originais poderem ser preservados, através do trabalho do perito sobre a imagem deles e não sobre o original. Neste caso, a análise é sobre as informações armazenadas e é totalmente auditável.[183]

A RFC (*Request for Comments*) 3227[184] estabelece que a ordem de coleta de evidências eletrônicas deve iniciar pelos dados mais voláteis até chegar aos dados menos voláteis e, inclusive, apresenta o seguinte exemplo de ordem de volatilidade de um sistema:

a) Registros e memória cache;
b) Tabela de roteamento e processos, cache ARP e estatísticas do kernel;
c) Memória;
d) Sistemas de arquivos temporários;
e) Disco;
f) Logs remotos que sejam relevantes ao sistema e monitoramento de dados relevantes para o sistema;
g) Configuração física e topologia da rede; e
h) Mídias.

Caso o dispositivo informático esteja *online*, os três primeiros itens possuem mais relevância. A RFC 3227 também sugere que se adotem cautelas relacionadas com a utilização dos programas do sistema e que se evite, a todo custo, a destruição de evidências, como, por exemplo, no caso de ocorrer o desligamento do dispositivo ou a retirada da rede de computadores que deflagre um processo capaz de eliminar informações que subsidiariam o trabalho pericial[185].

Outra abordagem sugerida pela RFC 3227 é relacionada com a necessidade de respeitar as regras de privacidade e as diretrizes da empresa ou órgão que possui o dispositivo analisado, sendo necessário sempre evitar coletar

[183] Vide DELLA VECCHIA, Evandro. **Perícia Digital**: da investigação à análise forense. Campinas: Millenium Ed., 2014.
[184] BREZINSKI, Dominique; KILLALEA, Tom. **Guidelines for Evidence Collection and Archiving**. Request for Comments: 3227, IETF, 2002.
[185] Exemplo claro dessa situação é o caso de o computador possuir sistema de criptografia instalado e que, ao desligá-lo, há automaticamente a criptografação de todo o seu conteúdo.

informações pessoais ou que não dizem respeito a investigação, dos usuários de computadores que trabalham com o referido dispositivo[186].

Estas diretrizes para coleta e arquivamento de evidências estabelecem que elas devem ser admissíveis perante o ordenamento jurídico, autênticas, evitando questionamentos quanto a sua veracidade, além de amplas, confiáveis e ser dotadas de credibilidade e simplicidade para ser aproveitada pelo órgão judicial, se for o caso.

Quanto às modalidades de forense, pode-se destacar também a *forense de redes* cabeadas e/ou sem fio, com reconstrução de sessões e geração de metadados. Finalmente, outra possibilidade é da *forense remota*, sobre conexões online e silenciosas, que tem a capacidade de obtenção de dados online e, também, a probabilidade/capacidade de remediar, por exemplo, incidentes.

Os tipos de evidência relativos à forense computacional são dois: *dados* e *equipamentos*. Em relação aos *dados*, temos, basicamente, aqueles armazenados em algum dispositivo ou mídia[187] e os coletados durante uma investigação, como ocorre no caso de uma interceptação telemática. Já em relação aos *equipamentos*, são em regra os *hardwares*, que podem ser gerais (computadores, servidores, roteadores etc.) ou específicos (com funções e finalidades específicas, além de configuração fechada e proprietária, ou seja, fogem do padrão dos equipamentos em geral).

Outro aspecto importante é que seja observada a denominada cadeia de custódia. A cadeia de custódia é o conjunto de processos direcionados a documentar toda a história cronológica da evidência eletrônica, garantindo a sua integridade, disponibilidade e idoneidade, em todas as etapas da forense computacional, de forma que possa ser utilizada como prova perante a Justiça.[188]

Há que se atentar para a necessidade de boas práticas que devem anteceder a coleta dos dados. Estes, assim, seriam os procedimentos que deveriam anteceder a investigação:

> 1. Esterilizar todas as mídias que serão utilizadas ou usar mídias novas a cada investigação; 2. certificar-se de que todas as ferramentas (softwares) que serão utilizadas estão devidamente licenciadas e prontas para utilização; 3. verificar se todos os equipamentos e materiais necessários (por exemplo, a estação forense, as mídias para coleta dos dados, etc.) estão a disposição; 4. quando chegar ao local da investigação, o perito

[186] Entende-se que essa diretriz dentro da RFC é relativa às forenses não oficiais, realizadas no âmbito das empresas e áreas de TI, para fins procedimentais da corporação. No caso de perícias oficiais, há dependência dos quesitos formulados pela autoridade requisitante.

[187] Exemplos: discos rígidos, mídias óticas, mídias magnéticas, memória flash e dispositivos móveis, como smartphones etc.

[188] Sobre cadeia de custódia, ver mais em WENDT, Valquiria Palmira Cirolini. **A prova penal e a cadeia de custódia**. In: Emerson Wendt; Fábio Motta Lopes. (Org.). Investigação Criminal: Provas. 1ed.Porto Alegre: Livraria do Advogado, 2015, v. 1, p. 51-64.

> deve providenciar para que nada seja tocado sem seu consentimento, com o objetivo de proteger e coletar todos os tipos de evidências; 5. os investigadores devem filmar ou fotografar o ambiente e registrar detalhes sobre os equipamentos como: marca, modelo, números de série, componentes internos, periféricos, etc. 6. manter a cadeia de custódia.[189]

Com relação a cadeia de custódia, de acordo com a RFC 3227[190], recomenda-se descrever claramente como a evidência foi localizada e todas as suas intercorrências, bem como indicar (a) "onde, quando e por quem a evidência foi descoberta e coletada", (b) "onde, quando e por quem foi a evidência tratada ou examinada", (c) "quem tinha a custódia das provas, durante o período e como realizou-se o armazenamento" e (d) "quando a prova mudou de custódia e como a transferência ocorreu".

A RFC 3227[191] sugere, ainda, algumas ferramentas consideradas imprescindíveis para a coleta de evidências eletrônicas. Nestes termos, de acordo com as referidas diretrizes, são necessários: (a) programa para examinar processos; (b) programa para análise do estado do sistema; (c) programa para realizar cópias bit-a-bit; (d) programa para a geração de *hashs*; (e) programa para geração e exame de imagens do núcleo, e; (f) *scripts* com a finalidade de automatizar a coleta de provas.

Como referido anteriormente, a forense segue uma metodologia. No caso, a sequência lógica e prática dessa metodologia é a seguinte:

> (a) Coleta de informações: o procedimento deve ser rápido, observando o necessário sigilo e registro da coleta de evidências. Ao par disto, o suspeito não deve ter chance de tentar ocultar ou destruir as provas, devendo ser feito o registro, formal e fotográfico do que foi coletado e do ambiente, caso necessário. Também, em regra, procede-se uma análise antes do acesso ao hardware para saber o procedimento adequado a tomar na forense. Para isso, é fundamental a preservação em que os equipamentos a serem periciados não devem ser acessados,

[189] PEREIRA, Evandro; FAGUNDES, Leonardo Lemes; NEUKAMP, Paulo; LUDWIG, Glauco e KONRATH, Marlom. Forense Computacional: fundamentos, tecnologias e desafios atuais. **VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Disponível em: <ceseg.inf.ufpr.br/anais/2007/minicursos/cap1-forense.pdf>. Acesso em: 16 jun. 2015. Nesse texto há citação da obra Perícia Forense Computacional – Teoria e Prática Aplicada, escrita por Dan Farmer e Wietse Venema, que primeiro mencionou sobre estes cuidados prévios à investigação. *Vide* também em BARREIRA, Fernando de Pinho. **Os Crimes Eletrônicos e A Perícia Criminal em Forense Computacional**. Disponível em: <http://fernandodepinhobarreira.wordpress.com/2013/06/20/os-crimes-eletronicos-e-a-pericia-criminal-em-forense-computacional>. Acesso em: 20 jun. 2013.

[190] BREZINSKI, Dominique; KILLALEA, Tom. Guidelines for Evidence Collection and Archiving. Request for Comments: 3227, IETF, 2002.

[191] BREZINSKI, Dominique; KILLALEA, Tom. Guidelines for Evidence Collection and Archiving. Request for Comments: 3227, IETF, 2002.

seja pelos agentes, seja pela autoridade policial, seja pelo oficial de justiça, além do que o desligamento deve ser rápido.

(b) Reconhecimento das evidências: além do trabalho prévio à forense, de seleção do que interessa à investigação em si, há a necessidade de reconhecimento e triagem das evidências. Por exemplo, de um computador, em regra, há necessidade de forense apenas de um HD (disco rígido).

(c) Restauração, documentação e preservação das evidências encontradas: neste processo, o trabalho da forense vai depender do contexto investigatório e do que for apresentado. Em regra, o perito vai trabalhar sobre a imagem dos dados, que é a imagem do disco ou cópia bit-a-bit, que inclui os espaços livres e os espaços não utilizados. Embora este processo exija mais espaço de armazenamento e consome mais tempo para realização, permite a recuperação de arquivos excluídos e dados não alocados pelo sistema de arquivos.

(d) Correlação das evidências: após a restauração, documentação e preservação das evidências, o perito trabalhará na análise e procurará correlacionar os dados, principalmente do ponto de vista do "problema" que lhe foi colocado. Desta forma, poderá compreender o que houve e tentar dar uma resposta à autoridade requisitante da forense.

(e) Reconstrução dos eventos: ao final do processo, poderá o perito reconstruir ou não os eventos com base nos dados analisados, respondendo aos quesitos formulados.

É importante mencionar que, em muitos casos, a forense computacional serve para auxiliar no levantamento de informações atinentes a diversos outros delitos, como o tráfico de drogas, homicídios, suicídios, sequestros, levantamento de dados contábeis (ex.: jogo do bicho), e, também, para verificação de hardwares, como ocorre nos crimes de defesa do consumidor (levantamento, identificação e confronto com a nota fiscal), capacidade ou funcionalidade de equipamentos, identificação de propriedade etc.

Assim, além das considerações já realizadas, sobre a importância da forense computacional e sua compreensão, optou-se por agregar aspectos fundamentais a respeito do que os peritos consideram importante para o bom encaminhamento da perícia, ou seja, o encaminhamento e formatação dos quesitos do caso investigado, que tem o viés de auxiliar no bom esclarecimento da investigação em curso.

Portanto, documentos sucintos e com quesitos genéricos não dão ideia ao perito do que se trata a investigação ou necessidade para uma eventual causa cível, penal, eleitoral, administrativa ou trabalhista. Exemplos disso são

questionamentos simples, como “qual o conteúdo do disco rígido?” ou “imprimir todo o conteúdo do disco rígido”, circunstâncias que são, logicamente, desproporcionais à investigação criminal.

Entretanto, o que deve conter no encaminhamento de solicitação de forense segue três regras básicas:

- Primeira regra: breve histórico do caso, com menção ao fato em si e os passos que a polícia adotou até a apreensão do equipamento e/ou dado a periciar;
- Segunda regra: envio de cópia de documentos coletados previamente, como por exemplo, testemunhos, xerox e boletim de ocorrência relacionados;
- Terceira regra: quesitos objetivos, sucintos e claros (na dúvida de elaboração, conversar previamente com o perito).

Desta forma o perito tem condições de filtrar melhor as informações e gerar um laudo com mais resultados úteis. Mas o que são quesitos objetivos? Eis a pergunta que todos agentes e autoridades policiais se fazem! Esclarece-se, em pormenores:

1º) Algumas “questões” estão sempre presentes no corpo dos laudos periciais, isto é, não são necessárias aparecer como quesitos. Exemplos:

“Qual o material que está sendo apresentado?”

“O material apresentado está em condição de uso?”

2º) No caso de delitos praticados por *hackers*, *crackers*, *bankers* etc., é (pode ser) importante questionar:

“O equipamento periciado apresenta condições de acesso a Internet?”

“Existem registros de acesso aos bancos X, Y e Z no período de ##/##/## a ##/##/##? Listar.”

“Existem bancos de dados configurados no equipamento analisado? Se sim, listar conteúdo que interesse ao delito investigado.”

3º) No caso de delitos relativos à imagens e vídeos de cenas de sexo explícito envolvendo crianças e adolescentes (pedofilia), previstos no Estatuto da Criança e do Adolescente, pode-se questionar:

“Existem imagens do acusado ou de “terceiros” abusando sexualmente de menores de idade?”

“Existem armazenadas fotografias de crianças e/ou adolescentes com imagens de pornografia ou cenas de sexo explícito?”

“Existem mensagens, conversas arquivadas ou outros arquivos relacionados à pornografia infantil?”

"Existe e-mails, enviados ou recebidos, com cenas de sexo explícito envolvendo crianças ou adolescentes?"

"Consta no histórico de navegação o acesso a sites, redes sociais ou fóruns de discussão que disponibilizam pornografia infantil ou facilita o contato entre pessoas que estejam em poder deste tipo de conteúdo ilícito?"

"Pelo material apresentado, pode-se afirmar que existia compartilhamento de imagens entre o proprietário do computador e a Internet?"

"Alguma das imagens encontradas já foi encontrada em outra perícia de crime similar? Se sim, informar os dados de identificação de autor e/ou vítimas."

4º) Nas perícias nos casos de crimes contra a honra, como calúnia, injúria e difamação[192], e, também, de racismo[193], é importante os quesitos:

"Existem imagens, diálogos ou similares com conteúdo racista (ofensivo à honra de fulano de tal)?" (genérico)

"Existem alguma mensagem de e-mail entre os dias ## e ## de agosto de 2015 contendo algum tipo de calúnia, injúria ou difamação direcionada ao Sr. fulano de tal? Se sim, é possível identificar o autor da mensagem?" (específico)

5º) Nas perícias dos crimes de violação dos direitos autorais e/ou de software[194] é importante:

"O material apresentado destina-se à gravação de CDs e DVDs?"

"O disco rígido possui produtos (software) de "tal fabricante" instalados?"

"Quais são os números de identificação (PRODUCT KEY, CD-KEY, ProductID) destes softwares?"

"Existe indicação no nome do usuário / empresa para quem o software está licenciado?"

"O equipamento possibilita a reprodução de áudio, vídeo, jogos e softwares?"

"O equipamento apresenta instalado algum tipo de programa que possibilita a reprodução de áudios, vídeos, jogos e softwares?"

6º) Em relação aos casos de falsificação de documentos[195], falsidade ideológica[196] e/ou estelionato[197] são importantes os seguintes questionamentos:

"Existem imagens de documentos públicos ou privados no disco rígido (pen drive, HD etc.) em questão? Quais?"

[192] Arts. 138 a 140 do Código Penal Brasileiro.
[193] Art. 20 da Lei 7.716/1989.
[194] Lei 9.609/1990.
[195] Arts. 297 e 298 do Código Penal.
[196] Art. 299 do Código Penal.
[197] Art. 171 do Código Penal.

"O conjunto de equipamentos em questão tem condições de produzir um documento similar ao apreendido com fulano de tal, cuja cópia segue anexa?"

"O documento em questão foi produzido pelo conjunto de equipamentos em perícia?"

"O documento questionado é autêntico?"

7º) Nos casos de investigação de crimes cometidos com a utilização de serviços de e-mails, a sugestão é quanto ao seguinte quesito:

"Verificar a origem (IP, cidade, empresa, etc.) do e-mail recebido dia ##/##/## com assunto "Descrever o assunto"."[198]

8º) Em relação à necessidade de identificação de propriedade do material questionado, sugere-se:

"É possível identificar o proprietário do equipamento questionado?"

"Existem arquivos com informações que possam identificar o proprietário (currículo, e-mails, etc.), mesmo que estejam excluídos? Quais?"

9º) Nos casos de investigação de organizações criminosas ou terrorismo pode-se indagar:

"Existem imagens do investigado ou de outros integrantes da organização praticando crimes, em poder de armas, drogas ou instrumentos ilícitos relacionados com a investigação?"

"Existem e-mails enviados ou recebidos, mensagens, conversas arquivadas ou outros arquivos relacionados com a atividade sob investigação?"

"Consta no histórico de navegação o acesso a redes sociais, sites ou fóruns de discussão ligados a organização criminosa em investigação?"

"Existem arquivos contendo informações sobre os investigados, seus comparsas, contatos, endereços, movimentações financeiras ou planejamento de ações criminosas?"

10º) No caso de imagens digitais, pode ser fundamental para a investigação as informações dos metadados (exif). Assim, pode ser quesitado:

"As imagens armazenadas possuem metadados? Se sim, relacionar as que possuem geolocalização."

11º) Finalmente, em relação a todos os tipos de perícia, sugere-se a adoção do seguinte quesito genérico, que permite ao perito a complementação de dados eventualmente não solicitados nos quesitos formulados:

"Outros dados julgados úteis?"

De outra parte, sistematizadas as possibilidades de forense computacional no que se refere à quesitação em relação aos principais delitos informáticos, existem, por assim dizer, desafios na realização da perícia digital, alavancados

[198] Neste caso, deve ser encaminhado junto o código fonte do e-mail.

pelos avanços tecnológicos. Dentre eles, podemos citar:

(a) *Cloud Computing*: a *cloud computing* ou computação em nuvem permite ao usuário ter acesso a todas as funcionalidades de um computador pessoal, mas pela Internet/Intranet, sendo necessária apenas a disponibilização de um computador/dispositivo com acesso à rede mundial ou local de computadores.

Todo o conteúdo que for produzido ficará disponibilizado "na nuvem", ou seja, em servidores hospedados no Brasil e/ou em outros países. Um usuário normal sequer sabe fazer a avaliação sobre se os seus dados estão na nuvem ou não, principalmente os que utilizam serviços gratuitos disponibilizados na web.

O tema merece a adequada atenção e apresenta algumas dificuldades por parte dos órgãos que realizam a investigação de eventuais crimes que tenha relação com esse tipo de serviço.

A apreensão de um computador cujos dados sobre o crime encontram-se em um servidor localizado em outro país é uma realidade que precisa ser enfrentada. Muitas vezes o referido computador não possui elementos capazes de auxiliar a investigação e pode existir grande dificuldade para obter a cooperação internacional do país onde o servidor esteja localizado. Geralmente há uma grande demora, ou até mesmo há a impossibilidade do servidor localizado no exterior fornecer as informações necessárias para a investigação criminal, principalmente se considerarmos que o Brasil não assinou a Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime. Esta convenção tem o intuito de incrementar a cooperação internacional entre os órgãos responsáveis pela investigação criminal; a previsão de novas condutas criminais que, pela internet, causem prejuízo ou transtorno para a vítima; a pressão para aprovação de legislação específica sobre o tema etc.[199]

Também existe dificuldade para garantir o respeito à cadeia de custódia e determinar que o provedor de outro país retire a publicação criminosa do site e/ou preste as informações prévias devidas.

(b) Capacitação de peritos computacionais, policiais e outros atores da persecução penal: a falta de capacitação dos atores da persecução penal representa um grande desafio, na medida que pode impedir a punição dos cibercriminosos, e, por consequência, causar impunidade.

A capacitação deve ser realizada continuamente, por profissionais especializados, de modo que os órgãos da persecução possam reprimir e acompanhar a evolução desses crimes. Os integrantes desses órgãos devem ser estimulados por políticas internas a participarem destas capacitações. Ademais, políticas públicas nacionais, voltadas aos órgãos de segurança pública, são bem-vindas e motivarão os estados a investirem na qualificação de seus quadros.

[199] Há que se registrar que o Brasil não foi firmatário de tal Convenção por haver conflito com as normas constitucionais brasileiras.

Em outros termos, excelentes profissionais, treinados adequadamente, trazem como retorno também o processo preventivo aos crimes cibernéticos, fator que é fundamental em virtude da falta de educação digital do usuário da internet.

(c) Criptografia e estenografia: a utilização da criptografia e da estenografia entre criminosos, para que não sejam identificados, representa outra tendência preocupante. Observam-se, inclusive, envolvendo criminosos com outras "frentes de atuação" no Brasil, delitos não necessariamente vinculados à área tecnológica.

Para esclarecer melhor estes dois recursos cabe considerar, que criptografia é um processo utilizado para misturar ou codificar dados/informações para garantir que apenas o destinatário possa ter acesso ao conteúdo produzido. De modo diferente, a estenografia permite esconder as informações de interesse no interior de uma mensagem. Geralmente são inseridos vídeos, textos ou áudios em imagens, sem que a pessoa que tiver contato com ela consiga perceber o seu conteúdo oculto.

A solução para estes casos viria de uma regulamentação do uso de softwares com criptografia, os quais só poderiam ser utilizados se devidamente registrados junto ao órgão competente e com depósito da chave correspondente. Quanto à estenografia, cujo processo diferenciado exige tratamento diverso, há que proceder ao treinamento de detecção e perícia forense computacional.

Pelo exposto, pode-se concluir em relação ao que foi exposto que, apesar de todos os desafios que envolvem o tema, para que a atuação do perito digital seja mais eficaz e, por consequência, o enfrentamento aos delitos informáticos, é imprescindível, além de se promover a capacitação constante de todos os envolvidos, também a adoção de procedimentos padrão com o intuito de sistematizar a perícia computacional, nos moldes do que se vislumbra em outros países. As experiências e boas práticas externas e internas ao Brasil são a alavanca necessária para firmar e consolidar os mecanismos e procedimentos de forense computacional no Brasil.

Destarte, o fomento da forense computacional no Brasil deve ser realizado, seja no âmbito federal ou nos Estados, em virtude da carência de profissionais e recursos qualificados para o incremento das investigações criminais e para uma maior eficácia da referida atividade.

REFERÊNCIAS

BARREIRA, Fernando de Pinho. **Os Crimes Eletrônicos e A Perícia Criminal em Forense Computacional**. Disponível em: <http://fernandodepinhobarreira.wordpress.com/2013/06/20/os-crimes-eletronicos-e-a-pericia-criminal-em-forense-computacional>. Acesso em: 20 jun. 2013.

BREZINSKI, Dominique; KILLALEA, Tom. **Guidelines for Evidence Collection and Archiving**. Request for Comments: 3227, IETF, 2002.

DELLA VECCHIA, Evandro. **Perícia Digital**: da investigação à análise forense. Campinas: Millenium Ed., 2014.

FORENSE COMPUTACIONAL. **Processo de Investigação**. Extraído do site: <https://sites.google.com/a/cristiantm.com.br/forense/forense-computacional/processo-de-investigacao>. Acesso em: 15 jun. 2015.

PEREIRA, Evandro; FAGUNDES, Leonardo Lemes; NEUKAMP, Paulo; LUDWIG, Glauco e KONRATH, Marlom. Forense Computacional: fundamentos, tecnologias e desafios atuais. **VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Disponível em: <ceseg.inf.ufpr.br/anais/2007/minicursos/cap1-forense.pdf>. Acesso em: 16 jun. 2015.

PIRES, Paulo S. da Motta. Forense Computacional: uma Proposta de Ensino. Disponível em: <http://www.leca.ufrn.br/~pmotta/ensino-forense.pdf>. Acessado em: 20 mar. 2005.

WENDT, Emerson. **Inteligência cibernética**: da ciberguerra ao cibercrime. A (in)segurança virtual no Brasil. São Paulo: Delfos, 2011.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: Ameaças e procedimentos de investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013.

WENDT, Emerson. **Lista dos Estados que possuem Delegacias de Polícia de combate aos Crimes Cibernéticos**. 2014. Disponível em: <http://www.emersonwendt.com.br/2010/07/lista-dos-estados-com-possuem.html>. Acesso em: 24 mai. 15.

WENDT, Valquiria Palmira Cirolini. **A prova penal e a cadeia de custódia**. In: Emerson Wendt; Fábio Motta Lopes. (Org.). Investigação Criminal: Provas. 1ed.Porto Alegre: Livraria do Advogado, 2015, v. 1, p. 51-64.

Capítulo XIII

Limites constitucionais e efetividade da investigação criminal de delitos cibernéticos

David Farias de Aragão[200]

INTRODUÇÃO

O presente estudo tem como área de concentração o Direito Constitucional e Processual Penal. Segue a linha de pesquisa Direito e Instituições do Sistema de Justiça, com foco no Sistema de Justiça Criminal e apresenta como tema limites constitucionais e efetividade na investigação criminal de delitos cibernéticos.

A formulação do problema passa pelo seguinte questionamento: os meios de coleta de elementos probatórios utilizados durante a investigação criminal permitem demonstrar a ocorrência e a autoria de ato ilícito praticado no espaço cibernético e estão em consonância com os ditames constitucionais brasileiros de proteção e promoção dos direitos fundamentais?

Trabalha-se a hipótese de que as técnicas de investigação existentes são eficazes para apontar a autoria e materialidade de infrações penais, mesmo que praticadas no espaço cibernético, mas que é preciso cautela no seu emprego para compatibilizar o exercício da atividade investigativa estatal com o modelo constitucional vigente. A observância dos direitos e garantias fundamentais, bem como das regras processuais, durante a coleta das evidências de um crime é imprescindível para que o resultado das apurações tenha serventia durante o processo criminal.

O objetivo deste estudo é analisar a investigação criminal de ilícitos praticados no espaço cibernético, destacando algumas das práticas de apuração

[200] Mestre em Direito e Instituições do Sistema de Justiça pela Universidade Federal do Maranhão - UFMA. Especialista em Gestão da Investigação Criminal pela Escola Superior de Polícia da Academia Nacional da Polícia Federal - ANP, Especialista em Ciências Penais pela UNISUL, Especialista em Direito Tributário pela UNAMA. Atualmente é Delegado de Polícia Federal, chefe da Delegacia de Repressão a Crimes Fazendários e Coordenador do Grupo de Repressão a Crimes Cibernéticos no Maranhão.

que estão sendo aplicadas pela Polícia Judiciária e sua adequação ao paradigma constitucional/garantista do Estado Democrático de Direito, em face da demanda por eficiência na segurança social equilibrada com a imprescindibilidade do resguardo do indivíduo que é submetido à persecução penal em relação aos seus direitos fundamentais.

Para acompanhar a evolução da criminalidade no campo tecnológico, é preciso que os órgãos que trabalham na persecução criminal busquem medidas inovadoras para atuar com eficiência na proteção de bens jurídicos não só no espaço físico, mas também no espaço cibernético, onde as pessoas passam a se relacionar cada vez mais.

Contudo, alguns julgamentos no âmbito do Superior Tribunal de Justiça invalidaram investigações policiais que duraram anos por considerar que houve violação a direito fundamental dos investigados[201]. Em que pese a casuística de algumas dessas decisões, a visão garantista do exercício da pretensão punitiva deve ser princípio orientador de todos os entes envolvidos na persecução penal, desde as instituições policiais até as mais altas cortes. A relevância da presente pesquisa se fundamenta na necessidade de se verificar a adequação jurídica da condução da fase investigativa aos paradigmas constitucionais de proteção e promoção dos direitos fundamentais.

O trabalho se inicia pelo estabelecimento do paradigma constitucional para o desenvolvimento válido da atividade de investigação criminal, que deve ter em mente o prisma garantista do exercício da pretensão punitiva, limitando a atuação estatal em relação aos direitos dos investigados, sem olvidar do direito da coletividade à segurança pública e quando será possível a relativização dos direitos fundamentais do investigado. É feita, ainda, uma breve análise dos limites da investigação criminal em face do direito à privacidade no direito norte-americano. Por fim, são expostas as questões processuais relativas a algumas das principais técnicas investigativas empregadas.

1. MODELO GARANTISTA PENAL E OS LIMITES AO PODER DE INVESTIGAR

A investigação criminal no Estado Democrático de Direito está informada pelo princípio democrático, baseado na defesa dos direitos fundamentais e na legalidade democrática da persecução criminal. As ações estatais, mormente as investigativas em geral, devem ser pautadas pela dignidade da pessoa humana,

[201] Cite-se como exemplo o julgamento do Habeas Corpus nº 137.349/SP e 159.159/SP referentes à Operação Castelo de Areia onde ficou estabelecido que denúncias anônimas não podem servir de base exclusiva para que a Justiça autorize a quebra de sigilo de dados de qualquer espécie, bem como do Habeas Corpus nº 191.378/DF referente à Operação Boi Barrica, posteriormente denominada de Operação Faktor, quando se entendeu que o Relatório de Informações Fiscais (RIF) emanado do Conselho de Controle de Atividades Financeiras (COAF) não é documento hábil para lastrear quebra de sigilo bancário e fiscal. Todos disponíveis em <www.stj.jus.br>. Acesso em 07 mar 2015.

por fundamento éticos e morais e, principalmente, pela transparência nos procedimentos investigativos (VALENTE, 2012, p.188).

Apesar do conceito de dignidade ser considerado vago e impreciso, na verdade, deve-se considerar que sua definição está em constante processo de construção de acordo com a evolução da sociedade e que se trata de um conceito aberto, que muitas vezes depende da análise do caso concreto, da diversidade histórico-cultural de um determinado povo, para permitir saber se o preceito foi respeitado ou não (GRECO, 2013, p. 10).

Conforme destaca Sarlet (2001, p.55),

> até que ponto a dignidade não está acima das especificidades culturais, que, muitas vezes, justificam atos que, para a maior parte da humanidade são considerados atentatórios à dignidade da pessoa humana, mas que, em certos quadrantes, são tidos por legítimos, encontrando-se profundamente enraizados na prática social e jurídica de determinadas comunidades. Em verdade, ainda que se pudesse ter o conceito de dignidade como universal, isto é, comum a todas as pessoas em todos os lugares, não haveria como evitar uma disparidade e até mesmo conflituosidade sempre que se tivesse que avaliar se uma determinada conduta é, ou não, ofensiva à dignidade.

Ainda que seja preciso muitas vezes a verificação da situação concreta para determinar o seu alcance, a dignidade da pessoa integra a própria condição humana e é um valor irrenunciável e inalienável, que não pode ser negado nem ao pior inimigo do Estado. Cada ser humano é merecedor de respeito e consideração por parte do Estado e da comunidade, *"implicando um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável"* (SARLET, 2001, p.60).

Ferrajoli (2014, p. 790) constrói sua teoria baseado na legalidade democrática e defende um modelo de Estado de Direito que prestigia a dignidade da pessoa humana, que entende como sinônimo de garantismo, nascido com as modernas Constituições e caracterizado no plano substancial como funcionalização de todos os poderes do Estado à garantia dos direitos fundamentais dos cidadãos, por meio da incorporação limitadora em sua Constituição dos deveres públicos correspondentes, isto é, das vedações legais de lesão aos direitos de liberdade e das obrigações de satisfação dos direitos sociais.

Para Ferrajoli (2006, p. 44) o paradigma constitucional ou garantista:

> equivale, en el plano teórico, al sistema de límites y vínculos sustanciales, cualesquiera que éstos sean, impuestos a la totalidad de los poderes públicos por normas de grado jerárquicamente superior a las producidas por su ejercicio. Es precisamente en su carácter formal, y por tanto en el

> reconocimiento del carácter «contingente» en el plano teórico-jurídico de sus contenidos, donde reside, a mi entender, la innegable y no opinable fuerza vinculante del paradigma constitucional; mientras la teses de la conexión con (esto es, conuna) moral debilita su valor teórico, reduciendo el constitucionalismo a una ideología más o menos compartida que sublima como código moral la constitución existente.

O garantismo figura como a outra face do constitucionalismo, ou seja, aponta para a necessidade de instrumentos de garantia à concretização das cartas constitucionais. E o jurista italiano acredita no direito e na democracia, mas em um direito que serve de instrumento para limitação e vinculação de qualquer que seja o poder, fundando essa perspectiva nos direitos fundamentais, e em uma democracia lastreada no conceito jurídico, constitucional (COPETTI NETO, 2013).

Trata-se de um parâmetro de racionalidade, de justiça e de legitimidade da intervenção punitiva a ser observado por todas as esferas do sistema de justiça criminal, desde a fase policial até a execução penal. É um modelo de verificação da normatividade constitucional nas práticas legislativas ordinárias, administrativas, policias e judiciais, de análise das prescrições constitucionais e seu efetivo funcionamento dentro do sistema. Quanto maior o grau de adequação ao modelo constitucional, maior o grau de garantismo.

> Uma Constituição pode ser muito avançada em vista dos princípios e direitos sancionados e não passar de um pedaço de papel, caso haja defeitos de técnicas coercitivas – ou seja, de garantias – que propiciem o controle e a neutralização do poder e do direito ilegítimo (FERRAJOLI, 2014, p. 786).

A teoria sistematizada por Ferrajoli do garantismo penal limita a atuação do poder de repressão penal do Estado e propõe mecanismos de efetivação dos direitos e garantias previstos constitucionalmente. Conforme esclarecem Bueno e Carvalho (2001, p.17):

> A teoria do garantismo penal, antes de mais nada, se propõe a estabelecer critérios de racionalidade e civilidade à intervenção penal, deslegitimando qualquer modelo de controle social maniqueísta que coloca a "defesa social" acima dos direitos e garantias individuais. Percebido dessa forma, o modelo garantista permite a criação de um instrumental prático-teórico idôneo a tutela dos direitos contra a irracionalidade dos poderes, sejam públicos ou privados.

Ferrajoli (2011, p. 686-687) conceitua direitos fundamentais como aqueles direitos em que todos são titulares enquanto pessoas naturais e aponta que os direitos fundamentais são direitos subjetivos, são interesses juridicamente

protegidos, como expectativas positivas ou negativas e também são direitos universais, que pertencem a todos em condições de igualdade. Os direitos fundamentais revelam não só uma forma de legitimação e de justificação das cartas constitucionais, como também são fonte de deslegitimação e invalidação das regras que não lhe são consentâneas (FERRAJOLI, 2011, p. 775).

A proposta de modelo constitucional elaborada por Ferrajoli funda-se na imposição de limites e vínculos à atuação dos poderes públicos e privados, por meio de um constitucionalismo forte, centrado nos direitos fundamentais, que conforma não apenas o ser, mas também o dever ser do Direito. E os direitos fundamentais, nesse modelo, assumem destacada função, uma vez que figuram como instrumentos indispensáveis na atuação jurídica em qualquer esfera, tanto naquilo sobre o que não se pode decidir como em relação ao que não se pode deixar de decidir (COPETTI NETO e FISHER, 2013, p. 420).

O modelo garantista proposto por Ferrajoli, não obstante sua ancoragem no Direito Penal Material, abrange discussões muito mais amplas. Aborda – como não poderia deixar de ser – por exemplo, o modelo político de Estado, fazendo um contraponto entre o discurso (dever ser) e realidade (ser). Obviamente, o garantismo alcança também as "regras do jogo" no processo penal e na investigação criminal, uma vez que estas são (devem ser) instrumentos de garantias de direitos (MENDES, 2010, p.63).

Ferrajoli apresenta dez axiomas, que seriam condições indispensáveis para a afirmação da responsabilidade penal e aplicação da pena, tratando-se de um modelo-limite, apenas tendencialmente e jamais perfeitamente satisfazível, conforme ressaltado pelo próprio autor, a saber:

> (i) princípio da retributividade da pena em relação ao delito; (ii) princípio da legalidade; (iii) princípio da necessidade ou da economia do Direito Penal; (iv) princípio da lesividade do evento; (v) princípio da materialidade da ação; (vi) princípio da culpabilidade ou da responsabilidade pessoal; (vii) princípio da jurisdicionariedade; (viii) princípio acusatório ou da separação entre Juiz e acusação; (ix) princípio do ônus da prova; (x) princípio do contraditório ou da defesa (FERRAJOLI, 2014, p. 74/75).

Para Coppeti (2000, p. 108), o âmago do garantismo é apontar o paradoxo que existe entre o Estado real e aquele que se apresenta como ideal. É uma antítese entre um arquétipo normativo tendencialmente garantista e as práxis operacionais tendencialmente antigarantistas, aparecendo, dessa maneira, como uma teoria da divergência entre normatividade e realidade.

Ao analisar a teoria do garantismo, Lopes Júnior e Gloeckner (2014, p. 49) consideram que o termo pode ser tratado como um neologismo para designar *uma técnica de tutela de direitos fundamentais*, pouco importando se tais direitos são negativos (direitos de liberdade) ou positivos (direitos sociais). Em outra passagem de sua obra, esses autores esclarecem essa afirmação, dizendo que

> o *garantismo* não tem nenhuma relação com o mero legalismo, formalismo ou processualismo. E, muito menos, com defesa da impunidade, como querem fazer crer alguns manipuladores. Consiste na tutela dos direitos fundamentais, os quais – da vida à liberdade pessoal, das liberdades civis e políticas às expectativas sociais de subsistência, dos direitos individuais aos coletivos – representam valores, os bens e os interesses, materiais e pré-políticos, que fundam e justificam a existência daqueles artifícios – como chamou *Hobbes* – que são o Direito e o Estado, cujo desfrute por parte de todos constitui a base substancial da democracia. Dessa afirmação de Ferrajoli é possível extrair um imperativo básico: o Direito existe para tutelar os direitos fundamentais (LOPES JÚNIOR e GLOECKNER, 2014, p. 45).

Além de prescrever a maximização dos direitos sociais e a mínima intervenção jurídico-política nos direitos liberais, a teoria do garantismo também prega a separação entre vigência e validade, uma divisão entre forma e substância. Para que uma norma exista, esteja em vigor, é suficiente que satisfaça as condições de validade formal relativas ao procedimento e competência para elaboração do ato normativo, mas para que seja válida, é necessário que satisfaça, ainda, as condições de validade substancial, relativas ao seu conteúdo e significado em relação às normas superiores, em especial as constitucionais, habitualmente se relacionando a valores como igualdade, liberdade e garantias dos direitos dos cidadãos (FERRAJOLI, 2014, p. 806). Sem o respeito a esses valores, não se pode falar no exercício válido da atividade investigativa.

O garantismo penal é um esquema tipológico baseado no máximo grau de tutela dos direitos e na fiabilidade do juízo e da legislação, limitando o poder punitivo e garantindo as pessoas contra qualquer tipo de violência arbitrária pública ou privada (BUENO e CARVALHO, 2001, p. 19). Não propõe, como já foi mal-interpretado, um sistema de garantias apenas ao acusado, mas busca a proteção do cidadão contra as ofensas dos delitos, bem como os autores dos fatos delituosos contra a vingança ilimitada, seja do Estado, seja do particular (MENDES, 2010, p. 62).

Segundo Fernandes (2010, p. 40), o garantismo se liga umbilicalmente à ideia do devido processo legal em seus aspectos subjetivos (garantias das partes, essencialmente do investigado/indiciado/acusado) e objetivos (garantias de justo processo). A investigação criminal cuida especialmente da reconstrução de fatos, em proximidade com as investigações científicas e a busca pela verdade, tendo limitações de ordem jurídica, tanto no que tange ao direcionamento da apuração, mas também no seu alcance e limites. Neste particular, o devido processo legal se caracteriza como sendo o balizamento jurídico, o limite negativo, por meio do qual a investigação criminal deve se ater para que não ofenda direitos fundamentais do homem de maneira proibida (FANTINI, 2010, p. 33).

Assim, o exercício do poder punitivo estatal, além de estar subordinado a

uma forma de agir, prevista em lei, também não pode contrariar determinados conteúdos que a sociedade elegeu como invioláveis, os direitos fundamentais (CADEMARTORI, 1999, p. 32). Mas esse discurso em defesa da Constituição, núcleo da teoria garantista, impede que o texto fundamental seja reduzido a um mero *status* formal, sem qualquer possibilidade de real efetividade ou inserção no mundo da vida, tornando-se verdadeiro mecanismo de cognição constitucional necessário e indispensável para o controle estatal (VALLE, 2012, p. 25).

Para finalizar a análise do tema, Lopes Júnior e Gloeckner (2014, p. 48) apresentam um resumo do que se pode entender como garantismo penal na obra "Direito e Razão", de Luigi Ferrajoli, em três aspectos:

> a) maximização dos direitos sociais e mínima intervenção jurídico-política nos direitos liberais;
> b) separação entre vigência e validade, como uma teoria crítica do paleopositivismo, que confunde ambos os níveis normativos. Essa cisão entre a forma e a substância, por outro lado, desemboca numa revisão da própria teoria da democracia (substancial), a fim de se estabelecer aquilo que não pode ser tocado pelo legislador bem como aquilo que deve ser tocado pelo legislador (problema da omissão, em especial quanto aos direitos sociais prestacionais);
> c) a necessidade de uma legitimação externa do Direito, que ultrapasse a justificação baseada em um modelo superado de regras sobre regras (modelo piramidal kelseniano), com as vertentes de Hart (das regras de reconhecimento – *rule of recognition*) e Raz (da cadeia de validade – *chain of validity*). A justificação externa estará centrada na valorização dos direitos do homem, hoje especialmente regulados por um Direito supranacional, assentada na promessa de oferecer autonomia e emancipação, eternas promessas da modernidade.

Pode-se concluir, portanto, que o modelo penal garantista é aquele que tem como parâmetro os ditames constitucionais que servem como limites ao exercício do poder punitivo do Estado e paradigma para análise da sua validade substancial e não apenas formal. Um modelo de racionalidade e contenção da intervenção estatal na seara criminal, baseada nos direitos fundamentais.

2. A EFICIÊNCIA DA INVESTIGAÇÃO CRIMINAL COMO MEIO DE PROMOÇÃO DE SEGURANÇA PÚBLICA

O Estado Democrático de Direito só se consagra por meio da defesa irrestrita dos direitos e garantias fundamentais de seus cidadãos. Não basta apenas prevê-los em textos legais, ainda que no mais elevado na escala hierárquica das leis, a

Constituição, mas é preciso que atuação do poder público ofereça os meios necessários para o seu livre exercício.

Se por um lado o Estado deve estabelecer políticas de desenvolvimento desses direitos, por outro, deve observá-los como limitadores de suas atividades, como ficou claro no tópico anterior. Assim, ao desempenhar a atividade de segurança pública, o Estado tem como limites à sua atuação os direitos fundamentais do investigado.

Mas também deve-se destacar que o dever do Estado de promover a segurança pública, seja preventivamente, pela ação ostensiva, ou repressivamente, por meio da persecução penal é, na verdade, uma forma de assegurar a proteção do direito da vítima do ato ilícito que teve seu direito violado pela prática do fato tipificado na lei penal, ou seja, que teve um de seus bens jurídicos mais importantes atingidos. Em última análise, de assegurar à coletividade a plena liberdade para o exercício de seus direitos.

De acordo com Parejo (2008, p.31),

> precisamente porque a segurança jurídica é um bem e um princípio geral de matriz constitucional, a segurança em sentido material (entendida como normalidade mínima necessária para a efetividade da ordem jurídica) é um direito subjetivo, e um direito subjetivo fundamental, que, como a liberdade pessoal a que está intimamente ligada, remete à exigência da correspondente prestação por parte do Poder Público em forma de ação administrativa policial preventiva e, quando for o caso, repressiva.

O sistema de justiça criminal pode ter diversos atores e configurações de acordo com as opções adotadas pelos legisladores de cada país. No Brasil, é composto por três subsistemas, quais sejam, o policial, o judicial e o prisional. No subsistema policial são desenvolvidas as atividades de prevenção em sentido estrito ao crime por meio do policiamento ostensivo, bem como a primeira fase da sua repressão através da atuação da polícia investigativa na busca de elementos de autoria e materialidade que justifiquem a deflagração da fase judicial, quando será formulada uma acusação que pode ou não gerar uma condenação. O subsistema prisional fica encarregado da execução e acompanhamento das penas determinadas pela condenação.

Assim, em âmbito processual, temos duas fases, uma pré-processual, por meio de inquérito policial ou termo circunstanciado de ocorrência, durante a qual são buscados elementos acerca da autoria e da materialidade de um fato possivelmente típico, atividade esta a cargo da Polícia Judiciária, chefiada por delegado de polícia[202], materializada pelo inquérito policial, e outra processual,

[202] Além das disposições contidas no Código de Processo Penal brasileiro sobre a condução do inquérito policial, a investigação criminal presidida pelo delegado de polícia está regulamentada hoje pela Lei nº 12.830/2013, com previsão de poder requisição e regramento sobre o

por meio da ação penal, durante a qual o Ministério Público ou a vítima, conforme o caso, promoverá em juízo a acusação.

No que se refere apenas ao campo da investigação criminal, que possui natureza jurídica complexa, podendo ser composta por atos administrativos e/ou jurisdicionais, existem três grandes modelos no mundo moderno de acordo com o órgão encarregado pela apuração do delito, o Estado-investigação: o juizado de instrução, o inquérito ministerial e o inquérito policial. Mas antes da análise de cada um desses modelos, é importante destacar o entendimento de Pitombo (1987, p. 21-22), segundo o qual como a finalidade da investigação estatal é a *persecutio criminis extra juditio*, com vistas ao esclarecimento de fatos e circunstâncias acerca de uma possível prática delituosa, pela qual até mesmo o inquérito policial pode e deve ser visto como um procedimento judicial[203].

No juizado de instrução, a presidência da investigação criminal é titularizada por um magistrado, denominado juiz de instrução, juiz-instrutor ou juiz-investigador. A Polícia Judiciária se afigura, neste caso, como mero órgão auxiliar, diretamente subordinada ao magistrado no plano funcional. Dentre as atribuições do juiz instrutor encontram-se, por exemplo, proceder ao formal interrogatório do suspeito, determinar medidas cautelares pessoais ou reais, colher todos os elementos de convicção necessários ao esclarecimento do fato noticiado e requisitar perícias (PERAZZONI, 2011, p. 86).

A iniciativa e os poderes instrutórios encontram-se inteiramente concentrados na figura do juiz instrutor. A participação da defesa e do órgão acusador limita-se a simples solicitação da realização de diligências, as quais poderão ser deferidas ou não, a seu talante (LOPES JÚNIOR, 2001, p. 72). É o sistema adotado atualmente pela França e Espanha. Tem como principal fator negativo a grande concentração de poder nas mãos do juiz-instrutor que inclusive autoriza eventuais medidas cautelares necessárias no curso das apurações.

No modelo de inquérito ministerial, o órgão acusador é que preside as investigações. Foi a escolha feita por Itália e Alemanha. Essa forma de investigar acaba por concentrar muito poder nas mãos de um único órgão, o Ministério Público, que fica responsável por investigar, acusar e, ainda, caso verifique a inocência de algum investigado, produzir prova a seu favor, prejudicando, sem sombras de dúvidas a imparcialidade das investigações, já que na Alemanha[204],

---

indiciamento do investigado.

[203] A Lei nº 13.047/2014 consagrou esse entendimento ao estabelecer a natureza híbrida das funções desempenhadas pela autoridade policial, nos seguintes termos: *"Os ocupantes do cargo de Delegado de Polícia Federal, autoridades policiais no âmbito da polícia judiciária da União, são responsáveis pela direção das atividades do órgão e exercem função de natureza jurídica e policial, essencial e exclusiva de Estado".*

[204] "*O processo penal alemão com a reforma de 1975 teve a estrutura correspondente ao 'inquérito' sensivelmente modificada, assumindo o Ministério Público (Staatsanwajtshaft) uma posição de supremacia na condução das investigações. No entanto, esta modificação contribui também para a emancipação do Ministério Público e para um novo equilíbrio de poder na investigação desfavorável ao suspeito, sendo que a investigação preliminar vem sendo alvo de profundas*

por exemplo, o *parquet* possui o monopólio inclusive da ação penal privada (FERREIRA, 2012, p. 97).

Nesse sentido, Lopes Júnior (2001, p. 97), alerta sobre os riscos da investigação pelo órgão acusador:

> Na prática, o promotor atua de forma parcial e não vê mais que uma direção.
> Ao se transformar a investigação preliminar numa via de mão única, está-se acentuando a desigualdade das futuras partes com graves prejuízos para o sujeito passivo. É convertê-la em uma simples e unilateral preparação para a acusação, uma atividade minimista e reprovável, com inequívocos prejuízos para a defesa.

Por fim, tem-se o modelo do inquérito policial adotado no Brasil e Inglaterra[205], que tem a grande vantagem de separar em órgãos distintos as funções de investigar, atribuída à Polícia, de acusar, atribuída ao Ministério Público, e de julgar, destinada ao Judiciário, minimizando a possibilidade de eventual parcialidade na condução das investigações. Como já ficou demonstrando no tópico anterior deste capítulo, o atendimento às "regras do jogo", em especial aquelas presentes no texto constitucional, fazem parte do parâmetro garantista de regular exercício de qualquer atividade estatal, em especial aquelas que podem ter reflexos sobre diretos fundamentais, como a investigação criminal.

Com bem pontua Valente (2009, p.317):

A investigação criminal compõe-se de actos juridicamente préordenados que são praticados por grupos de pessoas legal e legitimamente autorizadas, que seguem um modelo padronizado e sistemático, e que irão dizer se existiu ou não um crime, determinar os autores e reunir as provas necessárias a uma decisão.

Não se concebe a existência de um procedimento de investigação criminal ou com finalidade criminal, realizado à revelia do direito e da lei. No caso, tais instrumentos de investigação não podem embasar, sem ofensa ao devido processo legal, ação penal cujo propósito final é a condenação do indivíduo a penas que poderão lhe restringir a vida, liberdade ou propriedade. Na consecução do Direito Processual Penal não há espaço para subterfúgios, pois as possíveis

---

críticas e de um movimento reformista no sentido de reforço aos direitos de defesa". (CHOUKR, 2006, p. 39).

[205] *"No Sistema Inglês inexiste a figura do Juízo de Instrução, recaindo exclusivamente sobre a polícia o dever na consecução das investigações criminais, podendo avaliar os resultados dos procedimentos investigatórios e iniciar a persecução criminal, com a acusação do suspeito e remetendo o caso ao 'Crown Prosecution Service' (Serviço da Promotoria da Coroa), que deverá notificar o acusado e preparar o procedimento para julgamento".* (FERREIRA, 2012, p.99).

consequências poderão ofender aos bens mais preciosos do ser humano, mormente a liberdade. Ora, quaisquer procedimentos, distintos daqueles previstos por lei, cuja finalidade precípua não envolve a apuração de delitos, não podem ser usados em processo criminal, uma vez que afrontam o devido processo legal, bem como ao princípio da legalidade (FANTINI, 2010, p.34).

No artigo 144, §1º, incisos I e II, da Constituição Federal brasileira estão definidas as atribuições investigativas da Polícia Federal, nos seguintes termos:

> I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei.
>
> II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência.

Já o inciso IV do mesmo dispositivo constitucional prevê as atribuições das Polícias Civis, a quem compete *"as funções de polícia judiciária e a apuração de infrações penais, exceto as militares".* Por sua vez, o artigo 4º do Código de Processo Penal dispõe que 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".* Os artigos seguintes do mencionado código regulamentam o instrumento legal adequado onde se formaliza a investigação criminal, o inquérito policial.

Para os crimes previstos no Código Penal Militar, a sua apuração deve obedecer ao Título III do Código de Processo Penal Militar e ser formalizada por meio de inquérito policial militar.

Também em caráter excepcional, existem alguns instrumentos normativos que preveem a possibilidade de outras autoridades promovam investigação criminal, sem que seja estabelecido o procedimento formal a ser aplicado:

a) as Comissões Parlamentares de Inquérito – CPIs, conforme previsão do art. 58, §3º, da Constituição da República de 1988;
b) as Procuradorias Gerais de Justiça, que deverão apurar o envolvimento de membros do Ministério Público em eventual ilícito penal , de acordo com a Lei n.º 8.625/93 - Lei Orgânica Nacional do Ministério Público;
c) os Tribunais de Justiça, Regionais Federais ou Superiores, que deverão promover a investigação criminal quando houver possível cometimento de ilícito penal por magistrado, conforme prevê a Lei Complementar n.º 35/79 – Lei Orgânica da Magistratura Nacional.

Há, ainda, duas hipóteses de atribuição de poder investigatório com base em regimento interno, ambas de questionável legalidade:

a) o Presidente ou Ministro do Tribunal deverá presidir inquérito ou delegar esta função a outra autoridade quando ocorrer um crime no interior da sede do respectivo Tribunal, nos termos do artigo 43 do Regimento Interno do Supremo Tribunal Federal e artigo 58 do Regimento Interno do Superior Tribunal de Justiça;
b) as polícias do Senado Federal e da Câmara dos Deputados também serão responsáveis por apurar ilícitos praticados no interior das casas legislativas, conforme a Resolução nº 59/2002 do Senado Federal e Resolução nº 018/2003 da Câmara dos Deputados.

O estabelecimento de procedimentos de investigação criminal ou a atribuição desse poder para outras autoridades por meio de normas regimentais ou resoluções afronta o artigo 22, inciso I, da Constituição Federal que estabelece como competência privativa da União legislar sobre Direito Penal e Processual. Para que o Estado possa exercer de forma legítima seu poder de persecução penal, é preciso observar os limites exigidos pelo devido processo legal e pelo princípio da legalidade também na fase de investigação criminal.

Apesar da ausência de previsão legal expressa, o Ministério Público vem conduzindo diretamente investigações criminais no Brasil. Trata-se de tema polêmico, que não se pretende aprofundar neste estudo[206], mas que não poderia deixar de ser mencionado. São apresentados como argumentos favoráveis a esse posicionamento a teoria dos poderes implícitos[207], a regra interpretativa segundo a qual quem pode o mais (acusar) pode o menos (investigar) [208], de que no direito comparado assim se procede, que o Supremo Tribunal Federal permite[209], bem

[206] Para aprofundamento do tem, conferir Silva (2011), Bitencourt (2012) e Nucci (2012).

[207] *"Poderes implícitos só podem existir quando a Constituição for omissa, isto é, quando não conferir os meios expressamente em favor do titular ou em favor de outra autoridade, órgão ou instituição. Se, no entanto, expressamente outorgar a quem quer que seja o que se tem como meio para atingir o fim pretendido, não se pode falar em poderes implícitos. Não há poder implícito onde este foi explicitado, expressamente estabelecido, mesmo que tenha sido em favor de outra instituição. Enfim, o poder implícito somente pode ser reconhecido quando a Constituição não disciplina a matéria: a competência que atribuída a um órgão, não pode ser invocada por outro, sob nenhum pretexto, como acremente sentencia Canotilho: 'Mas são claros os limites dos poderes implícitos: eles não podem subverter a separação e a interdependência dos órgãos de soberania constitucionalmente estabelecida, estando em especial excluída a possibilidade de eles afetarem poderes especificamente atribuídos a outros órgão'"* (BITENCOURT, 2012, p.133).

[208] Investigar não é um menos em relação a acusar, assim como acusar não é um menos em relação a sentenciar. São funções distintas. "*As competências são outorgadas expressamente aos diversos poderes, instituições e órgãos constitucionais. Nenhuma é mais, nenhuma é menos. São o que são, porque as regras de competência são regras de procedimento ou regras técnicas, havendo eventualmente regras subentendidas (não poderes implícitos) às regras enumeradas, porque submetidas a essas e, por conseguinte, pertinente ao mesmo titular. Não é o caso em exame, porque as regras enumeradas, explicitadas, sobre investigação na esfera penal conferem esta à Polícia Judiciária, e são regras de eficácia plena, como costumam ser as regras técnicas"* (SILVA, 2011, p.1155).

[209] Existe entendimento do próprio Supremo Tribunal Federal contrário à investigação criminal pelo Ministério Público, como o RHC 81326/DF. Contudo, existe uma tendência atual de possibilitar um poder investigatório supletivo à Polícia Judiciária para apurar crimes cometido por policiais, por

como que a corrupção policial[210] e a sua falta de estrutura impedem a apuração eficiente de crimes[211].

Como objeção à investigação direta pelo Ministério Público, apresenta-se a ofensa ao princípio da legalidade (artigo 37 da Constituição Federal), em face da ausência da previsão legal, a ofensa ao princípio do devido processo legal (artigo 5º, LIV, da Constituição Federal), em razão do não atendimento às prescrições do Código de Processo Penal sobre quem deve conduzir e como o procedimento investigativo deve se desenrolar. A ausência de forma, objeto, procedimento, prazo, maneiras de conclusão, e não submissão ao controle judicial, leva, também, à violação dos princípios da privacidade e da publicidade. Além disso, como o Ministério Público é a parte responsável pela acusação no processo penal, há desrespeito ao princípio da isonomia processual e paridade de armas em relação ao réu, que não poderá promover investigação privada, sob pena de usurpar função pública[212]. Sobre a questão do direito comparado, já se abordou acima os três modelos de investigação e houve uma clara opção do constituinte brasileiro de 1988 pelo sistema inglês do inquérito policial. Por fim, em relação às investigações realizadas por outros órgãos em âmbito administrativo como IBAMA, Receita Federal e o próprio Ministério Público através do inquérito civil, cabe esclarecer que essas investigações não têm finalidade criminal, mas seu resultado já pode oferecer elementos suficientes para a formação da opinião sobre o delito e possibilitar a apresentação da ação penal em juízo. Contudo, no caso de insuficiência, o trabalho a ser conduzido pela Polícia Judiciária é imprescindível, em especial quando se trata de organização criminosa que para identificação de sua amplitude e extensão com frequência é necessária a utilização de técnicas especiais de investigação criminal que só podem ser efetivadas pelo órgão constitucionalmente detentor dessa atribuição.

---

membros do *parquet* e crimes contra a administração pública, ainda pendente de decisão final referente ao RE 593.727 e HC 84.548.

[210] *"Uma das características do crime organizado está no envolvimento de autoridades públicas como um dos modos de sua ação e de sua impunidade. Não falta quem diga que o fato de a polícia estar na linha de frente da investigação criminal contribui para a contaminação de alguns de seus elementos, e não é garantido que, se o Ministério Público assumisse tal condição, ficaria imune aos mesmos riscos"* (SILVA, 2011, p.1156).

[211] A questão da falta de estrutura das polícias se resolve dando esse estrutura, não usurpando suas funções. O Ministério Público também não possui tal estrutura, pois já é responsável por uma série de atribuições relevantíssimas, além de não dispor de corpo técnico nem de expertise para desenvolver a investigação criminal.

[212] A profissão de detetive particular ainda não é regulamentada no Brasil, mas já existe projeto lei nº 1.211/2011 aprovado na Câmera dos Deputados e ainda pendente de análise no Senado Federal, tendo sido considerado inconstitucional a atribuição de natureza criminal aos detetives particulares, por ser a atividade de apuração de infrações penais atribuída constitucionalmente às Polícias Civil e Federal, ficando permitida apenas a coleta de dados e informações de natureza não criminal. O § 1º do artigo 4º do mencionado projeto de lei ficou com a seguinte redação: *"É vedado ao detetive particular prosseguir na coleta de dados e informações de interesse privado se vislumbrar indício de cometimento de infração penal, cabendo-lhe comunicar ao delegado de polícia".* Disponível em www.camera.gov.br. Acesso em 11 mar 2015.

Voltando aos demais aspectos da investigação criminal, em estudo desenvolvido em atendimento a demanda da Organização das Nações Unidas para elaboração de um manual de formação em direitos humanos para força policiais, Lasso (2001, p. 80) ressaltou que

> a investigação do crime constitui a primeira etapa fundamental da administração da justiça. Trata-se do meio pelo qual aqueles que são acusados de um crime podem ser levados a comparecer perante a justiça a fim de determinar a sua culpabilidade ou inocência. É também essencial para o bem-estar da sociedade, pois o crime causa sofrimento entre a população e compromete o desenvolvimento econômico e social. Por estas razões, a condução das investigações criminais de forma eficaz e em conformidade com a lei e com os princípios éticos é um aspecto extremamente importante da atividade policial.

Ao analisar os sistemas de investigação preliminar, Lopes Júnior (2001, p. 40), estabelece como fundamento de existência desta fase da persecução penal a sua *"instrumentalidade garantista"*. De um lado ela é necessária para fundamentar a decisão de abertura ou não do juízo oral (fase processual). De outro lado, assim como o processo não é um fim em si mesmo, a face garantista da investigação criminal tem como finalidade evitar acusações e processos infundados. Para Carnelutti (1997, p.338), a investigação preliminar não se faz para a comprovação de um delito, mas para excluir uma acusação aventurada. Além disso, serve para evitar equívocos, um verdadeiro obstáculo judicial a superar antes de poder abrir o processo judicial (1997, p. 346).

O processo é o caminho necessário para a pena, mas antes de chegar a ela é preciso percorrer todo esse caminho. A investigação preliminar é o primeiro degrau da escada e, através dela, se chegará a uma gradual conceituação de sujeito passivo. Com base nos elementos fornecidos na investigação preliminar, serão realizados esses diferentes juízos, de valor imprescindível para chegar ao processo ou ao não processo (LOPES JÚNIOR, 2001, p.45).

Além de servir de filtro processual, a investigação também esclarece um fato oculto, pois aquele que rompe com as regras de convivência social para ofender ou ameaçar os bens jurídicos tutelados pela última esfera de controle precisa ocultar sua ação e os instrumentos que utilizou para praticá-la de forma a ter sucesso em seu intento criminoso, além de não desejar sofrer a consequência jurídica da sua conduta que é a pena. Assim, na maioria dos casos, é necessário que a vítima informe ao Estado a ocorrência do fato criminoso por meio da formulação de uma *notitia criminis* para gerar a reação estatal que, conforme apontado por Dias e Andrade (1992, p. 135), deve levar em consideração quatro elementos:

a) Índole secreta do crime: pela própria expressão material e fática da conduta, pode evitar por completo a observação. Também os delitos sem vítima concreta, como nos delitos contra a saúde ou a fé pública, ou naqueles em que a vítima não tem consciência da ilicitude da conduta, o que frequentemente ocorre nos crimes econômicos, pode prejudicar a reação estatal;
b) Razões da vítima: a vítima é considerada a mais decisiva instância não formal de seleção, pois cerca de 90% (noventa por cento) da delinquência oficial é introduzida no sistema penal por meio dela. Assim, podem existir razões específicas que a impeçam de noticiar o fato, como a falta de confiança nas instâncias formais de controle do Estado e o desejo de evitar os incômodos resultados aleatórios da atuação dessas instâncias, o medo de represálias ou mesmo de evitar uma exposição pública da sua condição de vítima e das circunstâncias em que se deu o fato criminoso;
c) Tolerância social: a capacidade da sociedade de absorver determinadas taxas de criminalidade e certas modalidades de delitos. Tanto maior será a tolerância da sociedade quanto menor seja a correspondência entre as normas penais e as representações axiológicas da coletividade;
d) Reações privadas: existe uma tendência crescente de utilizar formas privadas de resposta ao delito, revelando a falta de confiança nos instrumentos formais de controle da criminalidade. Essas reações vão desde as manifestações mais simples de autotutela até as reações para-institucionais aplicadas por empresas, supermercados e grandes centros comerciais.

A investigação criminal preliminar ainda tem uma outra finalidade de salvaguardar a sociedade em razão de atender ao anseio da sociedade de que as condutas que possam configurar ilícitos penais venham a ser objetos de apuração pelo Estado, evitando a impunidade e proporcionando a deflagração do processo penal que pode culminar como uma justa punição àquele que descumpriu as normas de conduta social. Após pontuar que a investigação preliminar protege a sociedade pelo afastamento da certeza de impunidade, pelo seu caráter oficial, pelo estímulo negativo para prática de novas infrações e possível impedimento da consumação de um delito, Lopes Júnior (2001, p. 45) ressalta também a sua função cautelar nesse contexto, afirmando que

> podem ser adotadas medidas que tenham natureza pessoal, patrimonial ou probatória. A produção antecipada de provas pertence à classe das medidas de proteção da prova, pois visa assegurar provas técnicas ou testemunhais. Sem embargo, não é esta a única manifestação da função cautelar. As medidas cautelares patrimoniais têm como objeto garantir o pagamento das custas do processo e/ou o ressarcimento dos prejuízos causados pelo delito, ou seja, basicamente assegurar a eficácia da sentença condenatória com

> relação às responsabilidades civis. Isso também contribui para manter a tranquilidade social e a confiança no funcionamento da justiça.
> Mas, sem dúvida, são as medidas cautelares de caráter pessoal que exteriorizam com mais clareza a proteção da sociedade e o restabelecimento da paz social afetada pelo delito.

Assim, resta claro que a investigação criminal é uma proteção ao cidadão no sentido de que não será submetido a um processo abusivamente, mas também uma defesa conferida à sociedade de que os atos ilícitos serão efetivamente reprimidos, ainda que aquele que os praticou tente se furtar da responsabilização penal por meio da ocultação do fato criminoso ou de seus instrumentos e proveitos.

A atividade da Polícia Judiciária é, portanto, de suma importância para o sucesso da segunda fase da persecução penal. Não só porque nela devem ser observados também os limites à atuação estatal, mas também em razão da atividade de investigação ser o meio mais legítimo para apurar a conduta de indivíduos que ofendem os valores penal penalmente tutelados e, portanto, mais caros de uma sociedade, e depois levar ao seu processamento, julgamento e punição, assegurando a liberdade daqueles que foram ofendidos. Sem segurança, não há liberdade.

Canotilho (1993, p. 407), destaca que a função de direitos de defesa dos cidadãos se cumpre sob uma dupla perspectiva: jurídico-objetiva – com *"normas de competência negativa para os poderes públicos, proibindo fundamentalmente as ingerências destes na esfera jurídica individual"* e jurídico-subjetiva – por meio do *"poder de exercer positivamente direitos fundamentais (liberdade positiva) e de exigir omissões dos poderes públicos de forma a evitar agressões lesivas por parte dos mesmos (liberdade negativa)"*.

Contudo, não se pode esquecer que o Estado também tem deveres de proteção, que para Sarlet (2007, p. 165), devem ser exercidos

> no sentido de que a este incumbe zelar, inclusive preventivamente, pela proteção dos direitos fundamentais dos indivíduos não somente contra os poderes públicos, mas também contra agressões provindas de particulares e até mesmo de outros Estados. Esta incumbência, por sua vez, desemboca na obrigação de o Estado adotar medidas positivas da mais diversa natureza (por exemplo, por meio de proibições, autorizações, medidas legislativas de natureza penal etc.), com o objetivo precípuo de proteger de forma efetiva o exercício dos direitos fundamentais.

Como toda atividade da administração pública, a atividade de investigação criminal, parte da política de segurança pública do Estado, deve atender ao princípio da eficiência, consagrado no texto constitucional brasileiro a partir da emenda constitucional número 19 de 1998 que o incluiu expressamente no *caput* do artigo 37.

O princípio da eficiência é dotado de normatividade suficiente para, na condição de princípio jurídico-político, vincular as atividades da administração pública, impondo-lhe, como corolário do princípio da prossecução do interesse público e decorrente da própria ideia de dignidade da pessoa humana, um verdadeiro dever de otimização das relações meio-fim e de orientação para o bem comum (BATISTA JÚNIOR, 2004, p. 130).

Bulos (2007, p. 644) define esse princípio como aquele que prescreve que o aparelho estatal deve se revelar apto a gerar benefícios, prestando serviços à sociedade e respeitando o cidadão contribuinte. Advoga que a eficiência traduz a ideia de presteza, rendimento funcional, responsabilidade no cumprimento de deveres impostos a todo e qualquer agente público, com o objetivo de obter resultados positivos no exercício dos serviços públicos, satisfazendo as necessidades básicas dos administrados. Seria um reclamo contra a burocracia estatal, avessa à resolução imediata e rápida de problemas, e contra a conduta tecnocrática, que se volta contra a qualidade final dos serviços que podem ser prestados para satisfação do usuário.

É importante ressaltar que, embora as raízes do conceito de eficiência estejam no campo da ciência da administração, na seara jurídica, não se confunde com mera economicidade. Conforme destaca Almeida Neto (2013, p.143):

> É por não se limitar a uma mera análise quantitativa que a eficiência, no campo jurídico, apresenta singularidades. Muitas vezes, um determinado ato conquanto tenha causado prejuízos para a administração, não pode ser rotulado de ineficiente se, nas circunstâncias fáticas em que foi praticado, assegurou concretamente a dignidade da pessoa humana ou satisfez necessidades coletivas. É por estar orientado também para o bem comum e permeado pelo valor fundamental da dignidade da pessoa humana que o princípio, quando inserido no sistema de valores constitucionais, ganha conteúdo próprio, para além de uma abordagem meramente econômica.

Nesse sentido, Modesto (2000, p. 65) aponta que para atendimento ao princípio além da exigência da racionalização e otimização no uso dos meios, também é preciso que os resultados tenham qualidade e satisfatoriedade. Em outras palavras, não basta simplesmente atender à noção de economicidade do ato praticado pela administração, mas se deve buscar também o resguardo da dignidade da pessoa humana e o atendimento das necessidades coletivas.

A análise da efetividade implica, portanto, na verificação do resultado positivo do ato realizado. Trazendo essa noção para o processo penal, significa que um ato investigação ou processual gerou o efeito que dele se espera. Assim, a obtenção de elementos sobre a prática de um ato ilícito deve ser célere, sob pena de não se prestar mais ao fim pretendido, por não ser mais encontrado. Por outro

lado, um elemento probatório colhido durante uma investigação tem como objetivo a instrução processual e para tanto, é preciso obedecer ao devido processo legal em sua coleta, sob pena de não se atingir o fim almejado, pois provas ilícitas não podem ser utilizadas no processo.

O Instituto de Pesquisa Econômica Aplicada – IPEA, elaborou estudo sobre a eficiência do sistema de justiça criminal no Brasil, coordenado por Ferreira e Fontoura (2008, p. 39), e propõe como medida para verificação do desempenho da apuração de crimes pela polícia a verificação da proporção de crimes registrados que chegam até a denúncia (ou queixa-crime) nos procedimentos ordinários ou sumários da Justiça criminal relativos aos casos de crimes comuns, ou até a audiência preliminar de procedimento sumaríssimo nos casos de infração de menor potencial ofensivo. Quanto maior a proporção, mais eficaz seria a ação da polícia.

Contudo, esse parâmetro de análise pode trazer falsos resultados, pois é preciso relembrar que a finalidade da atividade de investigação criminal não é apenas possibilitar a denúncia de um crime, mas também levantar elementos mínimos que justifiquem a deflagração ou não de uma ação penal, podendo se chegar à conclusão que esses elementos não existem ou mesmo de que o fato investigado sequer configurou uma ação penalmente relevante. Não se esqueça, ainda, da função cautelar de produção antecipada de provas comentada acima.

Por outro lado, como o próprio estudo reconhece, a eficácia do trabalho policial depende da ajuda da população e de órgãos públicos ou privados. *As informações disponibilizadas por vítimas, testemunhas e organizações são fundamentais no registro e apuração de crimes e na detenção de infratores* (Fereira e Fontoura, 2008, p.41).

Em síntese, o binômio eficiência e garantismo, no processo penal, traduz-se na necessidade de se balancear adequadamente os direitos fundamentais à liberdade e à segurança. Desse modo, a persecução penal será eficiente e garantista, se atingir, em prazo razoável, um resultado justo, consistente na atuação do direito punitivo, com a observância dos meios essenciais para a defesa da liberdade do acusado (FERNANDES, 2005, p. 40).

A sociedade contemporânea não pode prescindir dos mecanismos hoje existentes para o efetivo combate à macrocriminalidade que instrumentalizem o processo penal, como a interceptação telefônica e telemática, as buscas domiciliares e acesso a dados dos investigados, institutos, aliás, utilizados por todos os países responsáveis e civilizados (SANCTIS, 2009, p. 91). Mas é preciso compatibilizar o emprego dessas técnicas com os direitos fundamentais dos investigados, aplicando-as apenas quando realmente necessárias e apenas para os casos mais importantes.

A história do processo penal é marcada por movimentos pendulares, ora prevalecendo ideais de segurança social, de eficiência repressiva, ora predominando pensamentos de proteção ao acusado, de afirmação e preservação

de suas garantias. De acordo com Fernandes (2010, p.19), essa diversidade de encaminhamentos é manifestação natural da eterna busca de equilíbrio entre o ideal de segurança social e a imprescindibilidade de se resguardar o indivíduo em seus direitos fundamentais, uma dicotomia representada pelo confronto entre eficiência e garantismo no processo penal, mas "em uma visão moderna, esses dois vetores não se opõem, pois não se concebe um processo eficiente sem garantismo".

3. A POSSIBILIDADE DE RELATIVIZAÇÃO DOS DIREITOS FUNDAMENTAIS DO INVESTIGADO

As Constituições dos Estados surgiram como instrumento de limitação do poder político e como forma de assegurar direitos e garantias individuais aos seus cidadãos. Com o decorrer do tempo e a evolução da vida em sociedade, passaram a abarcar outros temas e a ter maior protagonismo na regulação das relações sociais e no estímulo a determinados valores. Diversas conceituações doutrinárias de Constituição podem ser encontradas, classificáveis em sociológicas, políticas ou jurídicas, de acordo com o enfoque que se pretende dar.

Expoente da concepção sociológica, Lassale (1988, p.37) defendeu que a Constituição escrita é mera folha de papel e que a Constituição real seria, na verdade, resultado da soma dos fatores reais de poder de uma nação. Schmitt (1982, p. 46-47) via a Constituição como decisão política fundamental da unidade política, distinguindo a Constituição propriamente dita, que se refere àquelas normas de grande relevância jurídica, sobre organização do Estado, princípios democráticos e direitos fundamentais, dos demais dispositivos que tratam de outros assuntos, mas também estão contidos na Constituição, denominando-os apenas de leis constitucionais.

A visão jurídica de Constituição foi elaborada de forma mais científica por Kelsen (2006, p. 222), segundo o qual haveria uma norma fundamental hipotética, de caráter lógico-jurídico, que dá fundamento à criação da Constituição em sentido jurídico-positivo e a todo o direito positivo. Preocupado com a compreensão material de Constituição e em oposição ao conceito meramente formal de Kelsen, Smend (1985, p.132) definiu Constituição como a ordenação jurídica da dinâmica vital do processo de integração do Estado, cuja finalidade é a perpétua reimplantação da realidade total do Estado.

Apesar do esforço de se encontrar um conceito que retrate a importância da Constituição tanto no plano formal quanto no plano material, ou que englobe as suas dimensões sociológica, política e jurídica, isso ainda não foi possível. Como constatou Bonavides (2004, p.93), "*a palavra Constituição não basta, hoje, no campo do Direito Constitucional, para exprimir toda a realidade pertinente à organização e funcionamento das estruturas básicas da sociedade política*".

Para superar esse problema, passou-se a utilizar a expressão sistema constitucional[213], que é mais abrangente e leva em consideração a complexidade do fenômeno jurídico que não se restringe à norma, mas também inclui fatos e valores sociais. Mesmo não sendo o conceito de sistema unívoco, a expressão dá ideia de limite, contornos do ordenamento jurídico, permitindo estabelecer o que faz parte dele ou não.

Tem-se, assim, a Constituição como marco inaugural do sistema jurídico, que tem por finalidade regular racionalmente a conduta humana e ao mesmo tempo assegurar os valores da pessoa humana, em especial sua dignidade. Além de específico em relação aos demais, o sistema jurídico é aberto, pois

> tem uma estrutura dialógica, traduzida na disponibilidade e capacidade de aprendizagem das normas constitucionais para captarem a mudança da realidade e estarem abertas às concepções cambiantes da verdade e da justiça (CANOTILHO, 1993, p. 165).

Sob outro prisma, e em decorrência de sua abertura, o sistema jurídico também é dinâmico, não só pela possibilidade de criação e revogação de normas jurídicas como apontado por Kelsen, mas principalmente em razão da mutação das significações normativas manifestada através da interpretação e aplicação das normas jurídicas (NEVES, 1988, p. 31-32).

A Constituição, portanto, deve ser analisada como um dinâmico sistema aberto de regras e princípios. Neste trabalho, não se discutirá a fundo a polêmica distinção entre princípios e regras[214], mas é preciso pontuar que enquanto as regras seguem a lógica do tudo ou nada, os princípios constitucionais permitem o balanceamento de interesses, de acordo com seu peso e a ponderação de outros princípios eventualmente conflitantes (CANOTILHO, 1993, p. 168).

De acordo com Alexy (2008, p.103), os princípios seriam mandamentos de otimização que exigem que algo seja realizado dentro das possibilidades jurídicas e fáticas existentes, conforme cada caso concreto. Defende, ainda, o autor alemão a aplicação da teoria dos princípios à teoria dos direitos fundamentais, ensinamento este seguido no presente estudo para análise do direito à privacidade e seus consectários, objeto de nossa pesquisa.

A teoria de Alexy teria como fundamento a elucidação e a clarificação do discurso ético, pois como indivíduos resolvem conflitos e coordenam ações pelo uso da linguagem, falando uns com os outros, isso implica que o discurso, e não a propaganda ou a violência, é a mais básica forma de ação humana (MENÉDEZ,

---

[213] Para Carvalho (2008, p. 23), a expressão sistema constitucional *"traduz o sentido tomado pelo texto constitucional, em face da ambiência social, a cujas pretensões está sujeito em escala crescente, retratando a globalidade do fenômeno de ordenação jurídica fundamental do Estado e da sociedade"*.

[214] Para aprofundar o tema, conferir Ávila (2005).

2004, p. 2). Em razão da abertura do texto legal que possibilita a existência de *hard cases*, nos quais o magistrado não pode se limitar a dizer a lei, simplesmente porque sua redação não oferece uma solução incontroversa para o caso concreto, é preciso buscar soluções racionais para esse problema[215].

A Constituição prevê diversos direitos e deveres que eventualmente entram em conflito em determinados casos concretos e que, por isso, podem ser limitados, de sorte que não há direito fundamental absoluto. A Declaração de Direitos proclamada na França em 1789 já previa em seu artigo 4º, como limites das liberdades de cada, um o gozo dessas mesmas liberdades pelos outros membros da sociedade (COLLIARD, 1972, p.109).

Contudo, os direitos fundamentais não encontram limites apenas em outros direitos da mesma natureza, mas também no interesse público específico com base em outros valores e normas desde que igualmente constitucionais. Nessa segunda situação estão em jogo direitos fundamentais e bens da coletividade ou do Estado constitucionalmente protegidos.

Alexy (2008, p. 94-95) traz um interessante exemplo de choque entre direitos fundamentais e interesses do Estado julgado pelo Tribunal Constitucional alemão. Um acusado em um processo penal estaria impossibilitado de participar de uma audiência em razão do risco de sofrer um derrame cerebral ou um infarto. Nesse caso haveria uma colisão entre o direito estatal de garantir uma aplicação adequada do Direito Penal e o interesse do acusado de manter incólume sua vida e sua integridade física.

Para solucionar o problema, o doutrinador alemão constata que abstratamente ambos os interesses estão no mesmo plano e propõe que seja feito um sopesamento[216] entre os interesses conflitantes no caso concreto para decidir qual deles deve prevalecer, aplicando-se o princípio da proporcionalidade para se chegar à solução adequada.

De acordo com esse princípio, três máximas parciais devem ser observadas. A primeira, da adequação, impõe que o meio empregado deve ter idoneidade para alcançar o resultado pretendido. É um critério negativo que elimina meios não

---

[215] Na obra A Teoria da Argumentação Legal, Alexy busca responder a questão de como argumentar de forma legal os *hard cases, "where and to what extent value-judgments are required, how the relationship between these value-judgments and the methods of legal interpretation as well as the propositions and concepts of legal dogmatics are to be determined, and how these value-judgments can be rationally grounded or justified"*. Conferir Alexy (1989, p. 7).

[216] *"A lei de colisões significa, em primeira linha, àquilo que resulta das colisões. Porém, ela não trás nenhuma evidencia de como tais embates devam ser resolvidos. É aí que entram em cena as chamadas ponderações de princípios. A técnica de ponderação é que trará a medida mais efetiva para a resolução das colisões como ocorre com a vida e a dignidade na anencefalia fetal; através dela, afasta-se o princípio que, diante das condições fáticas e jurídicas observadas no caso concreto, tenha um peso menor. Para tanto, a ponderação estrutura-se por três fases gradativas: a primeira defini o grau de limitação a um princípio; na segunda, se verifica a importância de se efetivar outro comando principiológico e na terceira, pondera-se se a efetivação de um princípio justifica a limitação do primeiro"* (XAVIER, 2012, p.228).

adequados. Além disso, se existir mais de um caminho a ser trilhado, aquele menos gravoso deve ser escolhido. Por fim, deve ser realizada a ponderação propriamente dita (ALEXY, 2008, p. 116-117).

As máximas parciais da adequação e da necessidade expressam mandamento a ser otimizado em relação às possibilidades fáticas e não tratam de ponderação, mas do modo de evitar intervenções em direitos fundamentais que sem custos para outros princípios são evitáveis. A máxima parcial da proporcionalidade em sentido restrito se refere às possibilidades jurídicas, que são os princípios ou normas de direitos fundamentais em jogo na colisão. É o campo onde se efetiva a ponderação.

A técnica da ponderação desenvolvida por Alexy é objeto de críticas especialmente apresentadas por Habermas[217], que propõe o modelo do discurso de aplicação proposto por Klaus Günther, segundo o qual o debate jurídico comporta dois níveis discursivos: discursos de justificação e de aplicação. A teoria criada por Günther é que a justificação de normas e a aplicação de normas, sejam elas regras ou princípios, têm objetivos diferentes e são guiadas por princípios norteadores específicos. Somente a fundamentação de normas é orientada pelo principio da universalidade, idealizado por Habermas – assim representado por Günther: (U) – ao passo que a aplicação de normas já fundamentadas aos casos concretos exige uma perspectiva distinta. Logo, Günther visa exonerar o instante da fundamentação do excesso de tarefas que fariam corretas as críticas que apontam à inviabilidade prática de (U). O próprio Habermas aceitou a necessidade de reformulação do princípio (U) nos termos em que Klaus Günther sugere. (HABERMAS, 1997, p.215-216).

A técnica da ponderação não significa uma simples solução silogística, mas um processo explícito e transparente de argumentação legal. O objetivo é

[217] Oliveira (2004, p. 535) considera a resposta obtida por meio da ponderação como inadequada ao paradigma procedimental do Estado democrático de direito, apontando os seguintes problemas que sintetizam as críticas de Habermas:

a) ao se admitir uma compreensão dos princípios jurídicos como mandamentos de otimização, aplicáveis de maneira gradual, Alexy emprega uma operacionalização própria dos valores: isso faria, então, com que os princípios perdessem a sua natureza deontológica, transformando o código binário do Direito em um código gradual;
b) como consequência desse raciocínio, o Direito passaria a indicar o que é preferível, em vez de o que é devido;
c) o Direito – como pretensão de universalidade sobre a correção de uma ação – então, não mais pode ser considerado como um "trunfo", como quer Dworkin, nas discussões políticas que envolvam o bem-estar de uma parcela da sociedade; desnatura-se, portanto, a tese sobre a prevalência do justo sobre o bem, como preceitua Rawls;
d) a tese de Alexy nega a diferenciação entre discursos de justificação e discursos de aplicação, transformando a atividade judiciária em um poder constituinte permanente;
e) olvida-se da racionalidade comunicativa, uma vez que todo o raciocínio é pautado por uma racionalidade instrumental, deixando a aplicação jurídica a cargo de um raciocínio de adequação de meios a fins, ficando em segundo plano a questão da legitimidade da decisão jurídica; exatamente por isso o raciocínio sobre a ponderação acaba por cair em um decisionismo de cunho irracionalista, isto é, ausência de uma racionalidade comunicativa.

estabelecer um critério que permita a replicação do julgamento para avaliar sua precisão. Apesar disso, devido à limitações cognitivas humanas, a argumentação legal nunca vai ter a precisão de um cálculo matemático, mas pelo menos inclui o elemento da racionalidade na atividade (MENÉDEZ, 2004, p.10).

Nas investigações criminais que versam sobre crimes cibernéticos, a busca dos vestígios de autoria e materialidade frequentemente deve ser realizada por meio de técnicas de investigação que podem se chocar com os direitos fundamentais previstos nos incisos X, XI e XII do artigo 5º da Constituição Federal Brasileira, quais sejam, direito à privacidade, inviolabilidade do domicílio e das comunicações, que serão analisados mais adiante neste estudo.

Fernandes (2009, p. 10-12), após reforçar que não há antagonismo entre eficiência e garantismo, ressalta que a utilização de meios especiais e investigação e de produção de prova, em especial referente à criminalidade organizada, podem representar limitações a direitos ou garantias constitucionais e, portanto, para serem aceitos devem atender ao princípio da proporcionalidade, com lei prévia que as regulamente, com as seguintes especificações:

a) pessoas legitimadas a solicitar o uso desses meios especiais de investigação, as autorizadas a empregá-los em suas atividades e as encarregadas de fiscalizar a sua utilização;

b) condicionamento do uso do meio em causa a prévia, circunstanciada e fundamentada decisão judicial, com exceções somente para situações em que, em virtude de urgência, isso seja impossível ou desaconselhado;

c) enunciação dos requisitos para sua concessão.

Interessa saber até onde a atividade de investigação criminal pode ir sem que ofenda esses direitos do investigado e quando, mesmo que possa haver ofensa a esses direitos, será razoável relativizá-los, em sede legal ou judicial, em prol do direito da coletividade à segurança pública e do dever do Estado de promovê-la.

As técnicas investigativas serão objeto do terceiro capítulo deste estudo, mas antes de iniciá-lo, serão abordados o direito à privacidade, o sigilo de dados e a inviolabilidade do domicílio e das comunicações em face da necessidade de promoção da investigação criminal.

3.1 Direito à privacidade

Para que o indivíduo possa se autodeterminar e desenvolver sua personalidade, precisa ter liberdade de ação para agir e decidir longe da perturbação de terceiros. Sem sigilo, o desenvolvimento intelectual pode ficar prejudicado. Por isso, o constituinte brasileiro de 1988 declarou o direito fundamental à privacidade no inciso X do seu artigo 5º ao considerar como invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas. No entanto, especialmente após o advento dos avanços tecnológicos, está cada vez mais fácil o acesso a informações pessoais privadas[218].

[218] Segundo Silva (2006, p.209), o amplo sistema de informações computadorizadas gera um

O termo privacidade é utilizado em uma acepção ampla, para incluir as manifestações da esfera íntima da pessoa física, tais como sua forma de vida, as relações familiares e afetivas, seus hábitos, sua particularidade, seus pensamentos, seus segredos, seus planos futuros. É o direito de estar só, ou *right of an individual to live a life of reclusion and anonimity*, como decorrência do direito à privacidade[219], consagrado na doutrina e jurisprudência americana desde 1873 por meio do Juiz Cooly (BULOS, 2007, p.147).

A privacidade, como direito subjetivo fundamental, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem só respeito a ele, deseja manter para si, ao abrigo de sua única e discricionária decisão. O objeto desse direito, ou seja, o bem a ser protegido, que pode ser uma coisa, não necessariamente física, é a integridade moral do sujeito (FERRAZ JÚNIOR, 1993, p. 440).

Rodatá (2008, p.93) destaca dois aspectos em torno do conceito de privacidade determinados pelas mudanças decorrentes das tecnologias da informação. De um lado, ocorreu

> uma redefinição do conceito de privacidade que, além do tradicional poder de exclusão, atribui relevância cada vez mais ampla e clara ao poder de controle. Por outro lado, o objeto do direito à privacidade amplia-se, como efeito do enriquecimento da noção técnica da esfera privada, a qual compreende um número sempre crescente de situações juridicamente relevantes.
> ...
> hoje a sequência quantitativamente mais relevante é "pessoa-informação-circulação-controle", e não mais apenas "pessoa-informação-sigilo", em torno da qual foi construída a noção básica de privacidade. O titular do direito à privacidade pode exigir formas de "circulação controlada", e não somente interromper o fluxo das informações que lhe digam respeito.
> Nesse contexto, é importante ressaltar que a vida privada[220] protegida

processo de esquadrinhamento das pessoas, que ficam com sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados, que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento.

[219] O Tribunal de Justiça da União Europeia (TJUE) reconheceu em 13 de maio de 2014 o direito dos cidadãos de serem "esquecidos" na *internet*, ou seja, de poderem pedir ao Google e a outros buscadores que retirem os *links* a informações que os prejudicam ou já não são pertinentes. Somente em um dia (30/05/2014), a empresa Google recebeu 12 mil pedidos de internautas europeus para que seus nomes desaparecem do seu motor de buscas, ao que a imprensa chamou de um novo "direito ao esquecimento", que nada mais é que uma decorrência do direito à privacidade. (Disponível em <http://www1.folha.uol.com.br/tec/2014/06/1463681-google-recebeu-12-mil-pedidos-de-direito-ao-esquecimento-em-um-dia.shtml> Acesso em 04 jun 2014).

[220] Vida privada e intimidade são conceitos que carregam consigo uma grande controvérsia no campo do direito, razão pela qual trataremos os dois termos como sinônimos nesse estudo. De

constitucionalmente é aquela íntima, abrangendo inclusive as informações armazenadas em meios digitais, como computadores pessoais e *smartphones*. Contudo, a proteção constitucional não inclui a vida exterior, divulgada para um número irrestrito de pessoas, mormente na atual sociedade informatizada, onde as pessoas estão a todo tempo expondo suas vidas em redes sociais.

Conforme constatado por Rodatá (2008, p. 105), o reconhecimento do direito à privacidade como direito fundamental vem acompanhado de um sistema de exceções que tende a determinar sua aceitação social e sua compatibilidade com interesses coletivos.

> As formas de limitação mais difundidas, que chegam a sacrificar a tutela da privacidade em prol de outros interesses, considerados temporariamente ou não como prevalecentes, são bem conhecidas e em muitos casos estão previstas na própria legislação sobre bancos de dados. Dizem respeito sobretudo a interesses do Estado (segurança interna ou internacional, polícia, justiça) ou a relevantes direitos individuais e coletivos (tradicionalmente, o direito à informação, sobretudo como liberdade de imprensa; e cada vez mais intensamente o direito à saúde, principalmente em sua dimensão coletiva).

Considerando a crescente utilização dos meios digitais para a prática de crimes ou a presença de vestígios nessas plataformas que possam elucidar a autoria ou a materialidade delitiva, tem-se como razoável o afastamento do direito à privacidade para a investigação criminal, prevalecendo o dever do Estado de promover a persecução penal em face do direito individual do investigado de ter sua privacidade resguardada. Mas é preciso analisar o caso concreto para saber se é necessária autorização judicial para o desenvolvimento da técnica investigativa, bem como se não há outro meio disponível para a coleta da prova.

Nesse sentido, Tucci (1993, p. 419) assevera que os proclamados direitos do indivíduo integrante da comunidade põem-se como autênticas barreiras contra a atuação dos agentes estatais da persecução penal e dos órgãos do Poder Judiciário, limitando-a no interesse da privacidade, cuja asseguração constitui exigência inarredável do Estado de Direito. Mas o Estado, no exercício do poder-dever de punir, no curso da persecução penal, pode limitar a tutela da intimidade e da vida privada do indivíduo, nos termos da Lei Maior. A diminuição, porém, há que estar vinculada e ser proporcional ao fato perquirido. (PITOMBO,2012, p. 685)

---

acordo com Dotti (1980, p.137), a mobilidade e a extensão do bem jurídico protegido, ou seja, a liberdade através do isolamento, não permitem e nem recomendam a formulação de um conceito definitivo, mesmo porque não é possível estabelecer os limites físicos e espirituais dos ambientes de privacidade.

3.2 Sigilo de dados, inviolabilidade do domicílio e das comunicações

A intimidade, espécie de privacidade, mantém forte ligação com os direitos declarados nos incisos XI e XII do artigo 5º da Constituição Federal, quais sejam, a inviolabilidade de domicílio e o sigilo de correspondências e da comunicação de dados. Contudo, como esclareceu Carvalho (2007, p.137) ao tratar do sigilo bancário, o objeto de proteção do inciso XII é a comunicação de dados informáticos, ou seja, o ato de transmitir e receber dados eletronicamente para que a informação repassada não venha a ser conhecida por pessoa estranha à relação comunicativa, enquanto que o inciso X protegeria os dados informáticos de forma estanque, desde que o seu conhecimento por terceiros afete ou possa afetar a privacidade de alguém. Portanto, temos o sigilo de dados como decorrência do direito à privacidade[221].

A inviolabilidade do domicílio, por sua vez, está protegida pelo inciso XI da Constituição Federal, nos seguintes termos: *"a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial"*.

Quanto ao conceito de casa e domicílio, a doutrina consolidou, ao longo dos anos, interpretação bastante ampla, destacando que devem ser considerados domicílio, para fins de busca e apreensão, as casas e os apartamentos propriamente ditos, devidamente habitados, bem como as áreas contíguas, como quintais e garagens. Também será considerada casa o quarto de hotel, de pousada, de pensão ou qualquer outro lugar fechado utilizado como morada de alguém (por exemplo: edifício abandonado que esteja sendo utilizado como moradia de andarilhos). Igualmente serão considerados casa, para fins de busca domiciliar, o consultório médico, o escritório de advocacia ou outro lugar não aberto ao público em que alguém exerce profissão (BADARÓ, 2008, p. 272).

A inviolabilidade das comunicações, por fim é a garantia de cada indivíduo poder se relacionar com outras pessoas e, para tanto, utilizar os instrumentos de comunicação existentes, sem que o conteúdo de suas conversas seja disponibilizado a terceiros sem seu consentimento. Existem certas manifestações da pessoa que se destinam a permanecer inacessíveis ao conhecimento alheio, ou acessíveis a um grupo reduzido de pessoas, a quem o sujeito permita tal comunicação (FREGADOLLE, 1998, p. 87).

O inciso XII do artigo 5º da Constituição Federal prevê a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. Gomes Filho (1997, p. 121), ao tratar da questão do sigilo das comunicações, esclarece que

[221] Nesse sentido, conferir Ferraz Júnior, 1993, p. 439: *"a inviolabilidade do sigilo de dados é correlata ao direito fundamental à privacidade"*.

> tradicionalmente, até porque essa era a única forma de comunicação entre as pessoas que estavam em lugares diversos, o objeto da proteção estava limitado à correspondência epistolar, mais recentemente, com os avanços da tecnologia, problemas correlatos e delicados surgiram igualmente em relação às formas modernas de comunicação, e especialmente as telegráficas, de dados informatizados e telefônicas.

O preceito constitucional em tela, portanto, se destina a todo tipo de comunicação e protege o particular contra ações infundadas do Estado, assim como os demais membros da coletividade. Sobre os progressos tecnológicos, especialmente na área de telefonia, Avolio (2003, p. 90) destaca que

> o emprego de meios eletrônicos para conhecer ou documentar o conteúdo de conversações telefônicas é, atualmente, bastante comum e difundido. Devido aos progressos da tecnologia, são, na prática, acessíveis não apenas às autoridades públicas, mas também ao homem comum.

Apesar disso, o sigilo das comunicações é um valor constitucional a ser protegido pelo Estado, apenas podendo ser afastado dentro das condições previstas constitucionalmente e na Lei nº 9.296/96, que inclusive criminaliza a interceptação clandestina de comunicação com pena de dois a quatro anos de reclusão[222].

Ao tratar das técnicas de investigação especiais que têm reflexos sobre esses direitos e garantias fundamentais, voltaremos ao assunto, mas antes, será feita uma breve análise do tratamento dado ao tema pelo direito norte-americano.

3.3 Privacidade e investigação criminal nos Estados Unidos da América

No direito norte-americano, o assunto está regulamentado pela quarta emenda à Constituição Federal dos Estados Unidos, que prevê que

> o direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas[223].

[222] Sobre o bem jurídico tutelado pela vedação à interceptação telefônica não autorizada, Medroni (2012, p. 132) cita duas teorias, originariamente alemãs, uma que afirma que deve ser protegida a *confidencialidade* da palavra, fundamentada pelo perigo de que as palavras desautorizadamente cheguem pelo seu prolator ao conhecimento de pessoas estranhas, e outra, majoritária, que considera o direito à palavra falada, embasada no direito que as pessoas têm de decidir quem pode gravar a sua voz e, uma vez gravada, quem e quando poderá ter acesso ao teor da gravação e à sua voz.

[223] Disponível em <http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-à-criação-da-Sociedade-das-Nações-até-1919/constituicao-dos-estados-unidos-da-america-1787.html>.

A jurisprudência da corte suprema norte-americana criou um conceito para a aplicação racional/proporcional de técnicas investigativas que relativizem a inviolabilidade das pessoas, casas, papéis e haveres, que é o seguinte: *reasonable expetation of privacy* (expectativa razoável de privacidade). Del Carmen e Hemmens (2010, cap.1), analisam o caso paradigma Katz vs. Estados Unidos e outros subsequentes, além de algumas leis do mencionando país para explorar o que chamam de vigilância eletrônica em uma investigação criminal e dar as bases necessárias para se entender o conceito de expectativa razoável de privacidade.

O precedente Katz vs. Estados Unidos de 1967[224] foi levado à corte suprema norte-americana para que fosse verificada a legalidade da condenação de Charles Katz com base na transmissão de informações sobre apostas por meio de aparelho de telefone utilizando linhas do Estado. A Polícia Federal Americana, o FBI, instalou dispositivos de escuta em um telefone público que era usado por Katz e gravou as ligações feitas por ele, no interior da cabine telefônica que era parcialmente feita de vidro, de forma que ele podia ser visto de fora enquanto realizava as ligações. A coleta dessa evidência havia sido considerada legal pela corte inferior, tendo em vista que os policiais não entraram fisicamente na cabine telefônica e, portanto, conforme precedentes Olmstead vs. Estados Unidos (1928)[225] e Goldman vs. Estados Unidos (1942)[226], não teriam violado a quarta emenda.

A questão a ser enfrentada pela corte suprema americana era se uma cabine de telefone público era um local constitucionalmente protegido, de forma que a utilização de um aparelho eletrônico de escuta pelo lado de fora seria uma violação ao direito de privacidade do usuário, pois até então, a escuta telefônica não violava a quarta emenda, desde que a área sob proteção constitucional, como o domicílio, por exemplo, não fosse violada.

Justice (ministro da corte suprema) Stewart, ao proferir sua decisão sobre o caso de Charles Katz, considerou que a questão de fundo sobre a quarta emenda era se um indivíduo demonstrou uma expectativa subjetiva de privacidade que a sociedade considera razoável[227] e que, portanto, a emenda protegia pessoas e não

---

Acesso em 26 nov 2014.

[224] Disponível em <https://supreme.justia.com/cases/federal/us/389/347/case.html>. Acesso em 27 nov 2014.

[225] Disponível em < https://supreme.justia.com/cases/federal/us/277/438/case.html>: *"Evidence of a conspiracy to violate the Prohibition Act was obtained by government officers by secretly tapping the lines of a telephone company connected with the chief office and some of the residences of the conspirators, and thus clandestinely overhearing and recording their telephonic conversations concerning the conspiracy and in aid of its execution. The tapping connections were made in the basement of a large office building and on public streets, and no trespass was committed upon any property of the defendants. Held, that the obtaining of the evidence and its use at the trial did not violate the Fourth Amendment"*. Acesso em 27 nov 2014.

[226] Disponível em < https://supreme.justia.com/cases/federal/us/316/129/case.html>: "*The use by federal agents of a detectaphone, whereby conversations in the office of a defendant were overheard through contact on thewall of an adjoining room, did not violate the Fourth Amendment, and evidence thus obtained was admissible in a federal court"*. Acesso em 27 nov 2014.

[227] *Whether an individual has exhibited a subjective expectation of privacy that society considers reasonable".*

lugares, de forma que o que a pessoa conscientemente expõe ao público, mesmo em sua própria casa ou escritório não é objeto de proteção constitucional, mas aquilo que a pessoa pretende manter privado, mesmo em uma área acessível ao público, pode ser constitucionalmente protegida (DEL CARMEN e HEMMENS, 2010, p. 18).

Justice Harlan seguiu o mesmo entendimento de que a quarta emenda protege pessoas e não lugares e concluiu que a verdadeira questão era saber que tipo de proteção a norma constitucional confere, tendo definido o padrão de ponderação que é utilizado até hoje, segundo o qual são necessários dois requisitos para proteção constitucional à privacidade: primeiro, a demonstração de uma atual expectativa subjetiva de privacidade e segundo, que esta expectativa seja tal que a sociedade está preparada a reconhecer como razoável (DEL CARMEN e HEMMENS, 2010, p. 19). Assim, os cidadãos que demonstrem a razoável expectativa de privacidade podem usufruir da proteção prevista na quarta emenda em relação às suas atividades e conversas onde quer que estejam.

Após o caso Katz, algumas leis americanas passaram a dizer até onde a investigação policial pode ir na vigilância eletrônica independente da obtenção de ordem judicial, dentre elas o *Omnibus Crime Control and safe Streets Act of 1968 (Title III),* o *Eletronic communications an Privacy Act of 1986 (ECPA),* o *Communications Assistance for Law Enforcement Act de 1994 (CALEA)* e o *Patriot Act* de 2001, este último que flexibiliza algumas regras no caso de terrorismo e, por ser considerado uma regra de exceção, não será objeto deste estudo.

O CALEA[228] teve por objetivo tornar claro o dever de cooperação das empresas de telecomunicação com as agências estatais de persecução penal, estabelecendo que elas devem possibilitar as interceptações legalmente autorizadas e proteger a privacidade individual em face do grande poder das novas tecnologias. Em resumo, a norma pretende conferir proteção aos direitos individuais e simultaneamente conferir aos órgãos do Estado permissão para monitorar e acessar comunicações eletrônicas.

No caso Berger vs. Nova Iorque[229], foram estabelecidos os requisitos para obtenção válida de ordem judicial que autorize a vigilância eletrônica, devendo ser elaborado um requerimento que contenham as circunstâncias da *probable cause*[230] (causa provável), expressão contida na quarta emenda. Del Carmen e Hemmens (2010, p. 27) enumeram cinco condições para o atendimento do requisito da causa provável, decorrentes desse julgamento e posteriormente incorporados à legislação norte-americana: a) identificar qual crime está sendo cometido; b) descrever o local onde a interceptação será feita ou como será feita

[228] Disponível em < http://thomas.loc.gov/cgi-bin/bdquery/z?d103:HR04922:>. Acesso em 27 nov 2014.

[229] Disponível em < https://supreme.justia.com/cases/federal/us/388/41/case.html>. Acesso em 27 nov 2014.

[230] De acordo com Lehman e Phelps (2005, p. 118), causa provável é um nível razoável de crença baseado em fatos que podem ser articulados de que uma situação seja verdadeira para justificar uma intervenção policial em alguns casos com prévia e outros sem prévia autorização judicial.

ou usada; c) especificar o tipo de comunicação que se pretende interceptar; d) identificar a pessoa, se conhecida, que está praticando o ato ilícito e qual comunicação será interceptada; d) declarar que outros meios investigativos foram tentados e falharam ou que é improvável que outros meios tenham sucesso ou que sejam muito perigosos.

Em suma, da análise do direito americano podemos trazer os conceitos de causa provável e expectativa razoável de privacidade para auxiliar na ponderação do caso concreto entre direito à privacidade dos investigados e o dever do Estado de promover a segurança pública por meio da investigação criminal e em que casos será necessária autorização judicial para tanto. A título de ilustração, traz-se a colação alguns precedentes da suprema corte americana nos quais foi considerada dispensável a obtenção de ordem judicial para o emprego de técnicas de investigação que podem ter reflexo sobre o direito fundamental à privacidade do investigado.

No caso Estado Unidos vs. Knotts de 1983[231] ficou estabelecido que a polícia pode usar tecnologia comum como lanternas e binóculos para aumentar seus sentidos sem violar a quarta emenda. No caso Smith vs. Maryland de 1979[232] foi considerado que o uso de *pen registers*[233] para obtenção de registros telefônicos de um investigado independe de autorização judicial, pois quando o usuário do telefone voluntariamente digita um número de outro telefone e expõe à companhia a informação no curso normal do negócio de telefonia, assume o risco de que a operadora revele essa informação. Nesse caso, ficou decidido que não há expectativa de privacidade sobre informações que a pessoa repassa a terceiros. Por fim no caso Estados Unidos vs. Karo de 1984[234], foi considerada desnecessária a obtenção de ordem judicial para instalação de *beeper* e outros dispositivos de rastreamento, desde que o objeto monitorado esteja em uma área pública, mas quando estiver em área protegida pela inviolabilidade constitucional, a autorização judicial passa a ser exigida.

4. PRINCIPAIS TÉCNICAS INVESTIGATIVAS UTILIZADAS

Explorados os aspectos matérias relativos às fraudes bancarias eletrônicas, passa-se à análise das questões processuais penais relativas aos meios de investigação comumente empregados para apuração de sua autoria e materialidade.

---

[231] Disponível em < https://supreme.justia.com/cases/federal/us/460/276/case.html>. Acesso em 27 nov 2014.

[232] Disponível em < https://supreme.justia.com/cases/federal/us/442/735/case.html>. Acesso em 27 nov 2014.

[233] Dispositivos que capturam registros de ligações telefônicas sem interceptar seu conteúdo.

[234] Disponível em < https://supreme.justia.com/cases/federal/us/468/705/case.html>. Acesso em 27 nov 2014.

4.1 Acesso a dados cadastrais e pesquisas em fontes abertas

Dados cadastrais não se encontram protegidos constitucionalmente por qualquer tipo de sigilo, pois referidos dados contém apenas informações qualificativas, relativas ao nome, documentos e endereço de um determinado consumidor de um serviço. São dados que apenas identificam um indivíduo no meio social e que são utilizados em suas relações públicas com pessoas físicas e jurídicas.

Essas informações são muito utilizadas pelas empresas que as detém, por exemplo, ao ligarem indiscriminadamente para os terminais telefônicos de qualquer brasileiro oferecendo seus serviços. Não revelam, portanto, qualquer aspecto de intimidade ou vida privada, porque expostos a vários atos da vida social, não fazendo qualquer sentido a existência de sigilo sobre tais informações.

Como bem pontua Ferraz Júnior (1993, p. 450),

> a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles. Em consequência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos.

Diversos precedentes judiciais nas cortes nacionais consagram esse entendimento[235 e 236].

---

[235] HABEAS CORPUS. TRANCAMENTO AÇÃO PENAL. IMPOSSIBILIDADE. DADOS CADASTRAIS DE E-MAIL. REQUISIÇÃO AUTORIDADE POLICIAL. ORDEM JUDICIAL. DESNECESSIDADE. INEXISTÊNCIA DE OFENSA AO DIREITO FUNDAMENTAL À PRIVACIDADE.

I. O resguardo do sigilo de dados, genericamente considerado, possui, como garantia que é, função instrumental, no sentido de viabilizar a efetiva realização de direitos individuais relativos à incolumidade da intimidade e da vida privada. Isso significa dizer que a garantia, conceitualmente, por si só, não tem qualquer sentido satisfatório, sendo antes uma projeção do direito cuja tutela instrumentaliza (STF, MS 23452 / RJ - RIO DE JANEIRO, Rel. Min. Celso de Melo). Nesse contexto, o campo de manifestação da garantia informa-se exatamente pela latitude da necessidade de tutela do direito, a entendermos, conseguintemente, que não se cogitando de ameaça ou efetiva lesão ao direito à intimidade e vida privada, igualmente não se pode cogitar em garantia de sigilo de dados.

II. O conhecimento de dados meramente cadastrais, inclusive de e mail, quando disso não se extrapola para a dimensão de informações sobre o status ou modus vivendi da pessoa, não atinge a intimidade ou a vida privada de alguém, não estando submetido à cláusula de reserva de jurisdição. Licitude da prova produzida nesses termos.

... (HC 3265 DF 2007.01.00.003265-4, DESEMBARGADOR FEDERAL CÂNDIDO RIBEIRO, julgamento em 08/05/2007, TERCEIRA TURMA, publicado em 22/06/2007 DJ p.17).

[236] AÇÃO CIVIL PÚBLICA. LIMINAR. MINISTÉRIO PÚBLICO FEDERAL. INQUÉRITO. FORNECIMENTO DE DADOS CADASTRAIS. USUÁRIOS DE TELEFONIA MÓVEL E FIXA.

A mera identificação e obtenção do endereço dos usuários de telefones fixos e móveis não configura quebra de sigilo das comunicações telefônicas (interceptação), ou de "comunicação de dados"...

Dessa forma, como meros dados cadastrais não estão protegidos por sigilo, é desnecessária a obtenção de decisão judicial para acesso a esse tipo de informação. Esse entendimento da jurisprudência brasileira foi consagrado com a Lei nº 12.683 de 09 de julho de 2012, que acrescentou o art. 17-B na Lei de Lavagem de Dinheiro (9.613/1998) com a seguinte redação:

> A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de acesso à internet e pelas administradoras de cartão de crédito.

Apesar da mencionada Lei tratar especificamente de lavagem de dinheiro, entende-se que esse dispositivo, que se encontra posicionado nas disposições gerais, aplica-se à investigação de qualquer tipo de delito, pois a norma legal apenas consagra que meros dados cadastrais não merecem proteção para a investigação criminal conduzida pela autoridade policial, o delegado de polícia, e para a instrução da ação penal, conduzida pelo representante do Ministério Público.

A Associação Brasileira de Concessionárias de Serviço Telefônico Fixo Comutado – ABRAFIX ajuizou ação direta de inconstitucionalidade autuada sob o número 4906/2013-DF, questionando mencionado dispositivo legal, alegando que haveria ofensa ao artigo 5º, X, da Constituição Federal. Apesar de não ter havido ainda julgamento, a Procuradoria Geral da República já apresentou parecer pela improcedência da ação, sob o argumento de que dados cadastrais não são informações de cunho estritamente privadas e íntimas, de forma que é razoável e proporcional o acesso a tais dados independente de ordem judicial.[237]

Recentemente, outro instrumento legal, a Lei nº 12.850/2013, que conceitua organizações criminosas e relaciona meios de obtenção de prova em qualquer fase da persecução penal, confirmou, no seu artigo 15, a prescindibilidade da reserva de jurisdição para o acesso a dados cadastrais nos seguintes termos:

> O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão

(TRF4, AI 2006.04.00.031773-3/RS. Desembargador Federal Edgard Antônio Lippman Júnior, DE 05.03.2007).

[237] Disponível <http://noticias.pgr.mpf.mp.br/noticias/noticias-do-site/copy_of_constitucional/acesso-a-dados-pessoais-de-investigado-por-lavagem-de-dinheiro-e-constitucional> . Acesso em 13 nov 2014.

de crédito.

Por outro lado, a pesquisa em fontes abertas na *internet* também configura uma importante ferramenta à disposição da polícia para obter dados relevantes para a investigação criminal sem a necessidade de obtenção de autorização judicial para tanto, já que se trata de informação que está disponível para qualquer pessoa na rede, não havendo razoável expectativa de privacidade sobre ela.

Não existe uma regulamentação específica no Brasil para o recolhimento desse tipo de informação para fins de instrução criminal, mas ela é amplamente utilizada pelo mundo, inclusive em nível de inteligência policial, como se pode observar no item 4 do artigo 25 do regramento elaborado pelo Conselho da União Europeia que trata do tema em relação à sua polícia, a Europol[238].

Bravo (2014), estabelece os seguintes requisitos para que uma informação disponível na rede mundial de computadores seja considerada como fonte aberta:

a) se a conduta praticada não é expressamente proibida pelo Direito Processual Penal de um País;
b) se a conduta praticada é proporcional ao objetivo pretendido, ou seja, necessária, adequada e proporcional, e em simultâneo garantir o mínimo dano aos direitos, liberdades e garantias dos cidadãos;
c) se a conduta praticada não dependeu da ultrapassagem e ou da anulação de alguma forma de proteção de carácter técnico do serviço ou plataforma em causa, então, a informação proveniente dessa conduta pode ser considerada como extraída ou obtida a partir de fontes abertas e de forma lícita.

4.2 *Acesso a dados armazenados nas nuvens*

Com a difusão dos equipamentos informáticos, tornou-se comum iniciar a edição de um texto no trabalho e a sua conclusão em casa, por exemplo. Para tanto, no início, eram utilizados dispositivos móveis denominados disquetes, por meio dos quais um dado digital poderia ser levado de um computador para outro. Depois surgiram os *pen-drives*, que servem para o mesmo fim, mas com uma capacidade de armazenamento infinitamente superior.

Esse tipo de serviço de armazenamento remoto ficou conhecido como *cloud computing* ou, em tradução livre para nossa língua, computação nas nuvens. Gilman (2011, p.2) apontou que o termo se consagrou em razão da inclusão da

238 Disponível em < https://www.europol.europa.eu/sites/default/files/council_decision.pdf>. Acesso em 28 nov 2014: *"In addition to the processing of data from private parties in accordance with paragraph 3, Europol may directly retrieve and process data, including personal data, from publicly available sources, such as media and public data and commercial intelligence providers, in accordance with the data-protection provisions of this Decision. In accordance with Article 17, Europol shall forward all relevant information to the national units"*.

imagem de uma nuvem em apresentações feitas pelos responsáveis por esse tipo de serviço para empresários com o objetivo de facilitar o entendimento de que os dados ficam armazenados em um local diferente de onde se encontra a pessoa que os acessa, muitas vezes até em outros países.

Com a utilização desse serviço, o usuário pode então começar a escrever um texto no trabalho e terminá-lo em casa sem precisar portar consigo qualquer tipo de dispositivo. Pode, ainda, armazenar todas suas fotografias, planilhas e arquivos que contenham informações relativas à sua vida privada e sejam de interesse para uma investigação criminal[239]. No Brasil, os provedores de armazenamento de dados nas nuvens mais difundidos são *dropbox, skydrive* e *googledrive*, vinculados a empresas sediadas nos Estados Unidos.

É possível que criminosos utilizem o armazenamento de dados nas nuvens para guardar informações que podem servir como prova da ocorrência de um crime ou de sua autoria. Muitos assim o fazem com o objetivo de evitar a jurisdição das cortes dos países onde residem, preferencialmente armazenando seus arquivos em servidores situados em nações com pouca tradição em cooperação jurídica internacional.

Tratando-se de meros dados cadastrais, tais como nome de usuário e qualificação, a autoridade policial responsável pela investigação criminal, no Brasil, pode requisitar diretamente essas informações. No entanto, tratando-se de dados amparados pela inviolabilidade prevista no inciso X do art. 5º da Constituição Federal, decorrente do direito fundamental à privacidade, é necessária a obtenção de uma ordem judicial para seu acesso.

A questão que se põe é se empresas com sede no exterior estão submetidas às decisões das cortes brasileiras e às requisições das autoridades policiais, bem como se é válido que um juiz nacional determine a busca de dados que são acessíveis virtualmente do Brasil, mas que estão fisicamente armazenados em outro lugar do mundo, fora de sua jurisdição.

Vaciago (2011, p. 124-129) apresentou três possíveis soluções jurídicas para o problema levantado. Uma primeira, que denominou de abordagem tradicional, seria de que em razão do princípio da territorialidade, apenas a corte com jurisdição sobre o local onde o dado está fisicamente armazenado é que teria competência para ordenar o fornecimento dos dados. Critica essa posição asseverando que inviabilizaria a investigação criminal, pois muitas vezes nem mesmo o provedor de armazenamento de dados na nuvem sabe onde estes dados estão fisicamente com exatidão.

A segunda abordagem proposta tem como fundamento o princípio da nacionalidade, de forma que a corte competente seria aquela do país de origem do criminoso. A censura feita a essa tese se dá em razão do criminoso poder ser

[239] Mason e George (2011) destacam que a importância da admissão de evidência obtida das nuvens vai ser cada vez maior no futuro.

um estrangeiro praticando atos ilícitos em determinada nação, em especial porque o crime cibernético é geralmente transnacional e não necessita de proximidade física. Ademais, aduz o professor italiano que dados não têm nacionalidade, pois são atributos de um indivíduo.

A última solução se daria com base no princípio da bandeira, pela qual os crimes cometidos a bordo de navios, aeronaves e naves espaciais estariam submetidos à jurisdição do país da bandeira do meio de transporte, independente de sua localização física. Como o dado digital está constantemente mudando de localização assim como as embarcações, Vaciago defende que se aplique essa solução, apesar de enxergar o risco dos criminosos procurarem um provedor de serviço de armazenamento nas nuvens que atua sob uma "bandeira pirata".

O autor italiano destaca, ainda, outra solução apresentada pelo Conselho da Europa no contexto do Projeto Global em Crimes Cibernéticos, denominada "abordagem do poder de disposição", que superaria as questões legais enfrentada pelas demais e segundo a qual os agentes estatais poderiam acessar os dados do investigado armazenados nas nuvens desde que conseguissem obter legalmente seu nome de usuário e senha.

Como afirmado anteriormente, os provedores de armazenamento de dados nas nuvens mais difundidos no Brasil são *dropbox, skydrive* e *googledrive*, vinculados a empresas sediadas nos Estados Unidos. Presumindo-se que os computadores-servidores que armazenam os dados também estejam fisicamente situados nos Estados Unidos e aplicando-se a abordagem tradicional com base no princípio da territorialidade, a autoridade policial que entendesse necessário o acesso a dados armazenados em qualquer desses provedores deveria representar ao juiz competente para processar as medidas cautelares criminais relativas à investigação que conduz no Brasil para que fosse expedida uma carta rogatória para cumprimento por autoridade judiciária americana, seguindo os demorados e burocráticos canais diplomáticos, incompatíveis com a necessidade de rápido acesso à informação em uma investigação criminal.

Felizmente, o arcaico instituto da carta rogatória vem sendo substituído por mecanismos mais modernos, versáteis e compatíveis com a necessidade de célere acesso à informação, como, por exemplo, o pedido de auxílio direto baseado em acordos bilaterais, chamados *Mutual Legal Assistance Treaties* ou *MLATs*[240]. O Brasil celebrou um acordo dessa natureza com os Estados Unidos, promulgado em nosso país por meio do Decreto nº 3.810/ 2001. Apesar de menos demorado, o tempo médio para obtenção de uma resposta por meio desse mecanismo é de alguns meses, pois ainda é necessária a manifestação de uma autoridade central americana para que se consiga as informações desejadas.

Em caso recentemente julgado[241], o Superior Tribunal de Justiça, por meio da

[240] Para saber mais sobre os mecanismos de cooperação jurídica internacional no Brasil, conferir TOFOLLI e CESTARI (2008).

[241] Não foi possível acesso ao inteiro teor nem ementa do acórdão, pois o caso ainda está sob

sua Corte Especial, parece ter adotado a abordagem com base no princípio da bandeira quando determinou à Google Brasil Internet Ltda. que cumprisse ordem judicial de quebra de sigilo das comunicações de seu provedor de correio eletrônico, o Gmail. A ministra relatora pontuou que com a quebra do sigilo, haveria razoável expectativa de se obterem importantes elementos de prova e que o que se pretendia era a entrega de mensagens remetidas e recebidas por brasileiros em território nacional, envolvendo supostos crimes submetidos induvidosamente à jurisdição brasileira.

Não foi acatada a alegação da Google Brasil de que seria impossível cumprir a ordem de quebra de sigilo das comunicações porque os dados em questão estariam armazenados nos Estados Unidos e, por isso, sujeitos à legislação daquele país, que considera ilícita a divulgação. A empresa teria indicado a via diplomática para a obtenção dessas informações, fazendo menção ao acordo de assistência judiciária em matéria penal em vigor entre o Brasil e os Estados Unidos (Decreto 3.810/01).

Em seu voto, a ministra Laurita Vaz afirmou que o fato de estarem armazenados em qualquer outra parte do mundo não transforma esses dados em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para sua transferência. "*Nenhum obstáculo material há para que se viabilize o acesso remoto aos dados armazenados em servidor da empresa Google pela controlada no Brasil, atendidos, evidentemente, os limites da lei brasileira. A ordem pode ser perfeitamente cumprida, em território brasileiro, desde que haja boa vontade da empresa. Impossibilidade técnica, sabe-se, não há*" – disse a ministra.

A referida ministra destacou, ainda, que a Google Brasil foi constituída em conformidade com as leis brasileiras e, evidentemente, deve se submeter à legislação pátria, não podendo invocar leis americanas para se esquivar do cumprimento de requisição judicial. E acrescentou: "*Não se pode admitir que uma empresa se estabeleça no país, explore o lucrativo serviço de troca de mensagens por meio da internet – o que lhe é absolutamente lícito –, mas se esquive de cumprir as leis locais*."

Apesar de específico para o acesso a mensagens eletrônicas, o mesmo raciocínio pode ser aplicado para os demais dados armazenados nas nuvens. Podemos concluir, portanto, que para o Superior Tribunal de Justiça, caso a empresa responsável pelo provimento do serviço de armazenamento nas nuvens tenha filial no Brasil, ainda que os dados estejam armazenados em outro país, deve respeitar as leis locais e cumprir as ordens judiciais independente de cooperação internacional. Destarte, para os serviços de armazenamento

segredo de justiça, constando apenas notícia sobre o julgamento disponível no site do próprio Superior Tribunal de Justiça (www.stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=109906, Acesso em 30 mar 2014).

googledrive e *skydrive*, oferecidos pelas empresas Google e Microsoft, as quais têm sede no exterior, mas filiais no Brasil, basta a obtenção de uma decisão judicial local para acessar os dados de investigados mantidos por essas empresas, ainda que armazenados fisicamente no exterior. O que significa que o STJ adotou a abordagem com base no princípio da bandeira, pelo menos da bandeira da filial.

Por outro lado, essa mesma solução não poderia ser aplicada no caso do provedor de armazenamento nas nuvens *dropbox*. Com efeito, não se tem notícias de que exista filial desta empresa no Brasil, apesar de muitos brasileiros utilizarem esse serviço. Nesta situação, caso seja seguido o critério da bandeira, é preciso utilizar o MLAT.

Caso não seja oportuno para a investigação aguardar o trâmite do MLAT, considera-se possível, nesta hipótese, utilizar a abordagem do poder de disposição, desde que se observe as devidas cautelas legais. Assim, a autoridade policial poderia representar pela interceptação de dados telemáticos do investigado e obter o nome de usuário e senha para acesso ao armazenamento remoto, por exemplo, utilizando técnicas de engenharia social[242] ou de programas espiões. De posse do meio de acesso e autorizado judicialmente, poderia ser feito o espelhamento de todo o conteúdo armazenado remotamente para analise criminal e posterior utilização como evidência na fase judicial da persecução penal[243].

4.3 Busca domiciliar

A busca constitui diligência cautelar, normalmente operada na fase de investigação e, muitas vezes, no momento mesmo da prática delituosa ou logo após, em decorrência de perseguição ao autor do crime. Dada a sua natureza de providência cautelar, exigem-se para sua perfeita efetivação os requisitos do *periculum in mora* e do *fumus boni iuris.*

Normalmente, a busca na pessoa suspeita ou em residência é justificada pela urgência na sua perpetração, pois quase sempre existe o risco de se perderem vestígios do crime, importantes para a demonstração do corpo de delito ou outros elementos probatórios relevantes, os quais poderão desaparecer antes de serem apreendidos. O *fumus boni iuris* é exigido expressamente pelo Código. Dispõe o §1º do art. 240 do Código de Processo Penal que a busca domiciliar será efetivada quando "*fundadas razões a autorizarem*". O art. 244 repete a exigência para a busca pessoal.

[242]Expressão consagrada no livro a Arte de Enganar do cracker americano Kevin Mitnik, significando a utilização de técnicas sob-reptícias que levam a pessoa a entregar as informações que se deseja obter.

[243]No ordenamento jurídico brasileiro, não ~~nos~~ parece razoável na ponderação entre segurança pública/repressão a crimes e direito à privacidade/devido processo legal a utilização dessa técnica para acessar dados armazenados nas nuvens independente de ordem judicial, como aceito pela Corte Suprema italiana na decisão nº 16556, de 14 de outubro de 2009, a não ser que haja uma lei específica autorizando o acesso direto pelas agências de persecução penal, como entendeu a Suprema Corte alemã ao julgar a inconstitucional essa possibilidade em 20 de dezembro de 2006. Para maiores detalhes sobre os dois julgamentos, conferir Vaciago, 2011.

Assim, é pressuposto essencial da busca que a autoridade, com base em elementos concretos, possa fazer um juízo positivo, embora provisório, da existência de motivos que possibilitem a diligência. Deve dispor de elementos informativos que lhe façam acreditar estar presente a situação legal legitimadora da sua atuação. Mais dificultosa é a avaliação do *fumus boni iuris* nas hipóteses em que o agente ou a autoridade policial, por suspeita de flagrante, deva ingressar no domicílio sem mandado. Nessa situação, haverá necessidade de informes que façam surgir razoável convicção da prática delituosa. Deve-se supor, com assento em dados obtidos previamente que a coisa ou pessoa procurada se encontra naquela determinada residência. Não se exige, contudo, que a diligência seja cercada de êxito, com a consequente apreensão da pessoa ou coisa procurada. É suficiente ter a autoridade, antes do ingresso, razoáveis motivos para suspeitar da ocorrência de crime e forte convencimento de que irá prender determinadas coisas ou pessoas necessárias à demonstração da prática ilícita. (GRINOVER; FERNANDES e GOMES FILHO, 2001, p. 170-171).

> O §1º do art. 240 do CPP também elenca rol exemplificativo com as finalidades dessa técnica investigativa, quais sejam:
> a) prender criminosos;
> b) apreender coisas achadas ou obtidas por meios criminosos;
> c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;
> d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso;
> e) descobrir objetos necessários à prova de infração ou à defesa do réu;
> f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;
> g) apreender pessoas vítimas de crimes;
> h) colher qualquer elemento de convicção.

De acordo com Medroni (2012, p.177), "o cumprimento de mandado de busca e apreensão é atividade tipicamente policial. São eles treinados e preparados para agir, podendo antever eventuais problemas a serem encontrados no âmbito da operacionalização da diligência".

Tucci (2012, p.1231) define o instituto da busca e apreensão se trata de "meio de prova, de natureza acautelatória e coercitiva, consubstanciado no apossamento de elementos instrutórios, quer relacionados com objetos, quer com as pessoas do culpado e da vitima, quer, ainda, com a prática criminosa que tenha deixado vestígios".

Apesar do Código de Processo Penal tratar a busca e apreensão como instituto singular, ambos não se confundem. A busca tem como objetivo encontrar vestígios, coisas ou pessoas relacionadas a um fato que está sendo investigado, restringindo certos direitos fundamentais como a inviolabilidade de

domicílio e a privacidade. A apreensão, por sua vez, é meio cautelar de obtenção de provas e tem por objetivo assegurar elementos indispensáveis à comprovação do fato e convencimento do juiz. (COLLI, 2010, p.141). Tem como finalidade guardar e proteger pessoas e coisas que foram retiradas – com intento maior de constituir prova em juízo – do poder daqueles que as detinham ou retinham (PITOMBO, 2005, p.117).

Assim, um instituto é diferente e independente do outro, podendo haver busca sem apreensão, quando, por exemplo, a coisa procurada não é localizada. Por outro lado, também pode haver apreensão sem busca, como no caso de apresentação voluntária de material de interesse para a investigação.

Por se tratar de medida investigativa que limita o exercício de direitos fundamentais, a busca deve estar em perfeita consonância com as regras previstas na legislação processual penal, sob o risco de nulidade das provas eventualmente coletadas. Colli (2010, p.142) classifica as formalidades a serem observadas em dois grupos. O primeiro composto pelas regras relativas à expedição da ordem judicial previstas no artigo 243 do Código de Processo Penal[244] e o segundo grupo relativo à forma de sua execução, regulamentada pelo artigo 245 do mencionado instrumento legal[245].

É preciso esclarecer, ainda, para que tipo de local é necessária a obtenção de ordem judicial para se proceder à busca. O inciso XI do artigo 5º da Constituição Federal utiliza o termo "casa" e o Código de Processo Penal no artigo 240 e seguintes o termo "domicílio". A doutrina considera ambos como sinônimos e consolidou entendimento ampliativo à proteção. De acordo com Badaró (2008, p.

---

[244] Art. 243. O mandado de busca deverá:
I - indicar, o mais precisamente possível, a casa em que será realizada a diligência e o nome do respectivo proprietário ou morador; ou, no caso de busca pessoal, o nome da pessoa que terá de sofrê-la ou os sinais que a identifiquem;
II - mencionar o motivo e os fins da diligência;
III - ser subscrito pelo escrivão e assinado pela autoridade que o fizer expedir.
§ 1º Se houver ordem de prisão, constará do próprio texto do mandado de busca.
§ 2º Não será permitida a apreensão de documento em poder do defensor do acusado, salvo quando constituir elemento do corpo de delito.

[245] Art. 245. As buscas domiciliares serão executadas de dia, salvo se o morador consentir que se realizem à noite, e, antes de penetrarem na casa, os executores mostrarão e lerão o mandado ao morador, ou a quem o represente, intimando-o, em seguida, a abrir a porta.
§ 1º Se a própria autoridade der a busca, declarará previamente sua qualidade e o objeto da diligência.
§ 2º Em caso de desobediência, será arrombada a porta e forçada a entrada.
§ 3º Recalcitrando o morador, será permitido o emprego de força contra coisas existentes no interior da casa, para o descobrimento do que se procura.
§ 4º Observar-se-á o disposto nos §§ 2o e 3o, quando ausentes os moradores, devendo, neste caso, ser intimado a assistir à diligência qualquer vizinho, se houver e estiver presente.
§ 5º Se é determinada a pessoa ou coisa que se vai procurar, o morador será intimado a mostrá-la.
§ 6º Descoberta a pessoa ou coisa que se procura, será imediatamente apreendida e posta sob custódia da autoridade ou de seus agentes.
§ 7º Finda a diligência, os executores lavrarão auto circunstanciado, assinando-o com duas testemunhas presenciais, sem prejuízo do disposto no §4º.

272),

> devem ser considerados domicílio, para fins de busca e apreensão, as casas e os apartamentos propriamente ditos, devidamente habitados, bem como as áreas contíguas, como quintais e garagens. Também será considerada 'casa' o quarto de hotel, de pousada, de pensão ou qualquer outro lugar fechado utilizado como morada de alguém (por exemplo: edifício abandonado que esteja sendo utilizado como moradia de andarilhos). Igualmente serão considerados casa, para fins de busca domiciliar, o consultório médico, o escritório de advocacia ou outro lugar não aberto ao público em que alguém exerce profissão.

A jurisprudência brasileira acompanha esse entendimento, incluindo na proteção não apenas imóveis residenciais, mas também todos aqueles locais não abertos ao público em geral como escritórios de empresas, escritórios profissionais[246] e quartos de hotéis ocupados[247].

Antes de finalizar a análise da busca domiciliar, é preciso destacar o entendimento defendido por Costa e Lobo que classificam a medida investigativa de acesso a dados armazenados nas nuvens, tratada no item 3.3.2 deste estudo, como modalidade de busca e apreensão classificada como digital[248].

4.4 Interceptação telefônica e telemática

Uma das ferramentas mais eficazes na obtenção de elementos probatórios que demonstrem a atuação de organizações criminosas é a interceptação das suas comunicações, pois por meio dela é possível desvendar os papéis desempenhados por cada um de seus integrantes e acompanhar em tempo real as suas atividades ilícitas. Ao tratar da interceptação telefônica, Medroni (2012, p.132) considera a

---

[246] *"Para os fins da proteção jurídica a que se refere o art. 5º, XI, da Constituição da República, o conceito normativo de "casa" revela-se abrangente e, por estender-se a qualquer compartimento privado não aberto ao público, onde alguém exerce profissão ou atividade (CP, art. 150, § 4º, III), compreende, observada essa específica limitação espacial (área interna não acessível ao público), os escritórios profissionais, inclusive os de contabilidade, "embora sem conexão com a casa de moradia propriamente dita"* (HC 82788/RJ, Relator Ministro Celso de Mello, julgado em 14/04/2005, DJ de 02/06/2006, p. 43).

[247] *"Para os fins da proteção jurídica a que se refere o art. 5º, XI, da Constituição da República, o conceito normativo de 'casa' revela-se abrangente e, por estender-se a qualquer aposento de habitação coletiva, desde que ocupado (CP, art. 150, § 4º, II), compreende, observada essa específica limitação espacial, os quartos de hotel. Doutrina. Precedentes. - Sem que ocorra qualquer das situações excepcionais taxativamente previstas no texto constitucional (art. 5º, XI), nenhum agente público poderá, contra a vontade de quem de direito ('invito domino'), ingressar, durante o dia, sem mandado judicial, em aposento ocupado de habitação coletiva, sob pena de a prova resultante dessa diligência de busca e apreensão reputar-se inadmissível."* (RHC 90376/ RJ, Relator Ministro Celso de Mello, julgado em 03/04/2007, DJ de 18/05/2007, p.113).

[248] *"A busca e apreensão de dados armazenados em servidores remotos pode ser realizada se o mandado judicial respectivo indicar, expressamente, que as informações devem ser buscadas e apreendidas em servidor de acesso remoto e se esse mesmo mandado judicial impuser, também, que o administrador do sistema forneça nome de usuário e senha para a execução dessa ordem"* (COSTA e LOBO, 2011, p.203).

técnica como de

> Considerável grau de importância como meio de produção de prova, já que planejamento, ordens e execuções de crimes invariavelmente passam por necessidade de comunicação entre os agentes, principalmente tratando-se de organização criminosa.

Conforme definição de Castro (2003, p.21), interceptar é interromper o curso originário, impedir a passagem, ter contato com o teor da comunicação, mas sem impedir que ela chegue ao seu destinatário. Ferraioli e Dalia (2001, p. 657) conceituam interceptação como a captação, mediante instrumento mecânico ou eletrônico, de comunicações ou conversações que ocorrem à distância, por meio de telefone ou outros meios de telecomunicações, ou entre pessoas presentes em um mesmo contexto ambiental por pessoa que não participa da conversa e não é destinatário da comunicação interceptada. No primeiro caso temos a interceptação de telecomunicações e, no segundo, a interceptação ambiental.

Grinover, Fernandes e Gomes Filho (2001, p. 175), exemplificam as várias modalidades de "captação eletrônica da prova":

a) interceptação da conversa telefônica por terceiro, sem o conhecimento dos dois interlocutores;
b) a interceptação da conversa telefônica por terceiro, com o conhecimento de um dos interlocutores;
c) a interceptação da conversa entre presentes, por terceiro, sem o conhecimento de nenhum dos interlocutores;
d) a interceptação da conversa entre presentes por terceiro, com o conhecimento de um ou algum dos interlocutores;
e) gravação clandestina da conversa telefônica por um dos sujeitos, sem o conhecimento do outro;
f) gravação clandestina da conversa pessoal e direta, entre presentes, por um dos interlocutores, sem o conhecimento dos outros.

A finalidade inicial da interceptação, quando começou a ser desenvolvida nos Estados Unidos ainda na década de 60, era de caráter militar, de forma a possibilitar o monitoramento e espionagem das atividades do inimigo e estar preparado para possíveis ataques, porém, com o fim da Guerra Fria, os projetos de interceptação foram voltados ao combate da criminalidade (ASSUMPÇÃO, 2009, p. 172), apesar da recente volta de seu uso para o combate ao terrorismo.

Como se trata de uma medida de produção antecipada de prova no processo penal, com reflexos sobre os direitos fundamentais ao sigilo das comunicações e à privacidade, é necessária a obtenção de autorização judicial para sua execução. A própria Constituição Federal já prevê a possibilidade de utilização dessa técnica no inciso XII do artigo 5º, mas apenas para produção de prova em investigação criminal e em instrução processual penal.

Quando realizada dentro dos parâmetros previstos no ordenamento jurídico, precedida de autorização judicial fundamentada que avalia a presença dos requisitos que justificam as medidas cautelares, o *fumus boni juris* e *o periculum in mora,* o resultado da interceptação é considerado fonte de prova e o meio de prova a ser introduzido no processo é a gravação e sua transcrição (GRINOVER; FERNANDES e GOMES FILHO, 2001, p. 176).

No Brasil, o estatuto legal que regulamenta a interceptação de comunicações é a Lei nº 9.296 de 24 de julho de 1996. No parágrafo único do seu artigo 1º, prevê que a norma não se aplica somente às interceptações telefônicas, mas também às interceptações do fluxo de comunicações em sistemas de informação e telemática. A literatura diverge quanto à constitucionalidade da interceptação telemática. Para Pitombo (2005, p.123) e Greco Filho (1996, p.10), a medida seria vedada constitucionalmente em razão do inciso XII do artigo 5º da Constituição Federal não permitir expressamente a medida.

Prado (1997, p.13) defende a necessidade de adaptação da sociedade às novas formas de cometimento de delitos, afastando eventual inconstitucionalidade do delito. Oliveira (2006, p. 297), no mesmo sentido, aponta

> A possibilidade de autorização judicial também para a interceptação do fluxo de comunicações em sistema de informática e telemática, como ali previsto, é perfeitamente constitucional, e vem completar o rol de proteção do inc. XII do art. 5º CF, estabelecendo que em todas as hipóteses ali mencionadas a quebra do sigilo exigirá autorização judicial fundamentada.

Concorda-se com o entendimento pela constitucionalidade da interceptação telemática, em especial pelo fato que esse meio vem sendo amplamente utilizado para tratativas relativas a atos ilícitos, não sendo razoável uma mera interpretação literal restritiva do texto constitucional, que na verdade tem por finalidade é estabelecer a reserva de jurisdição para o afastamento do sigilo das comunicações em geral. A título de ilustração, veja-se algumas das principais ações criminosas tipificadas e classificadas como crimes cibernéticos em que se registra a viabilidade no manejo da interceptação telemática:

a) No capítulo dos crimes contra a administração pública, especialmente no que e refere aos artigos 313-A e 313-B do Código Penal;
b) Divulgar, sem justa causa, informações sigilosas ou reservadas, contidas ou não nos sistemas de informações ou banco de dados da administração pública, encontra adequação penal no artigo 153, §1.º, do Código Penal;
c) A violação do sigilo funcional prevista no artigo 325 do Código Penal;
d) As práticas de crimes de pornografia infanto-juvenil por meio da internet, alcançada pelo disposto no artigo 241 do Estatuto da Criança e do Adolescente, com atenção especial para a atual redação determinada pela Lei n.º 11.829/08;
e) A prática ou incitação de racismo via rede mundial, que encontra

reprimenda penal no artigo 20, caput e §2.º, da Lei n.º 7.716/89;

f) O furto mediante fraude bancária eletrônica, tipificado no artigo 155, §4º, inciso IV, do Código Penal, como visto acima.

A execução da interceptação será conduzida pela autoridade policial, nos termos do artigo 6º da Lei nº 9.296/1996[249]. São considerados pressupostos legais para adoção da medida: a) estar em curso investigação policial ou instrução processual penal; b) existirem indícios razoáveis de autoria; c) inexistir a possibilidade de utilização de outro meio de prova; d) estar prevista a pena de reclusão para o delito investigado.

Recentemente, a República Federativa do Brasil foi condenada pela Corte Interamericana de Direitos Humanos pela promoção de atos de investigação conduzidos em procedimentos irregulares. No caso Escher e Outros vs. Brasil, julgado em julho de 2009, estava ausente instrumento formal de investigação a dar supedâneo a medidas cautelares, conforme se observa nos trechos do julgamento abaixo transcritos[250]:

> De acordo com o artigo 1º da Lei n. 9.296/96, a interceptação telefônica deve ter o propósito de investigar criminalmente ou de instruir um processo penal. No presente caso, apesar de indicar a necessidade de investigar supostas práticas delitivas, quais sejam, o homicídio de Eduardo Aghinoni e o desvio de recursos públicos, a solicitação do major Neves não foi apresentada no marco de um procedimento investigativo que tivesse por objeto a verificação dos fatos. O pedido de interceptação sequer mencionou os autos da investigação do homicídio que se encontrava a cargo da polícia civil de Querência do Norte, cujo delegado de polícia não teria sido notificado a respeito. Outrossim, tampouco consta que na época dos fatos existisse uma investigação pelo suposto desvio de recursos públicos por parte dos dirigentes da COANA e da ADECON. Quanto ao pedido do sargento Silva, este não apontou o propósito das interceptações pretendidas nem sua vinculação com uma investigação ou processo penal. Desse modo, em detrimento do artigo 8º da Lei Nº 9.296/96, o Pedido de Censura foi uma diligência isolada e não tramitou em autos anexos a um procedimento de investigação ou processo criminal iniciados anteriormente. Portanto, ambas as solicitações descumpriram com o disposto nos artigos supracitados.
>
> A Corte conclui que as interceptações e gravações das conversas telefônicas objeto deste caso não observaram os artigos 1º, 2º, 3º, 4º, 5º, 6º e 8º da Lei nº 9.296/96 e, por isso, não estavam fundadas em lei. Em

[249] "Deferido o pedido, a autoridade policial conduzirá os procedimentos de interceptação, dando ciência ao Ministério Público, que poderá acompanhar a sua realização".

[250] Disponível em <http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf>, p. 41 e 45. Acesso em 04 fev 2015.

consequência, ao descumprir o requisito de legalidade, não resulta necessário continuar com a análise quanto à finalidade e à necessidade da interceptação.

Outra questão polêmica se refere à obtenção dos extratos de ligações telefônicas. Assim como os dados cadastrais dos usuários de linhas telefônicas e de protocolos de *internet* fornecidos pelas provedoras de acesso, não se encontram protegidos por reserva de jurisdição, por não configuram ofensa ao sigilo das comunicações, entende-se também que os extratos telefônicos podem ser requisitados diretamente pela autoridade policial no âmbito da investigação criminal e pelo representante do Ministério Público no curso do processo penal.

Apesar de literatura contrária a esse posicionamento, como se observa em Gomes e Cervini (1997, p.103), para quem os registros ou dados telefônicos só poderão ser obtidos através de ordem judicial, que deve se ater na avaliação do principio da proporcionalidade, já existem julgados que afastam a reserva de jurisdição, como o a seguir colacionado:

> Investigação criminal – Requisição para que seja apresentado o número de chamadas entre aparelhos telefônicos – Violação do art. 5º, XII, da CF – Inocorrência – Inteligência art. 5º, XII, da CF – Inocorre violação ao princípio constitucional do sigilo das comunicações telefônicas, caso para fins de investigação criminal se pretenda somente a obtenção dos números de chamadas entre aparelhos telefônicos, não sendo pretendida a escuta ou a conversação telefônica entre pessoas, vez que, nessa hipótese, inocorre invasão da privacidade. (MS nº 238.416/4, julgado em 6.5.1993, 1ª Câmara, relator Pires Neto, Voto Vencedor: Silva Rico, RJDTACrim 18/167).

Como esse entendimento ainda é minoritário em âmbito jurisprudencial, na prática, ainda se representa em juízo para acesso aos registros de ligações telefônicas.

CONCLUSÕES

Os órgãos que compõem o sistema de justiça criminal devem agir de maneira equilibrada em face da demanda por eficiência na segurança social, não deixando de resguardar o indivíduo que é submetido à persecução penal em relação aos seus direitos fundamentais. O modelo penal garantista como aquele que tem como parâmetro os ditames constitucionais que servem como limites ao exercício do poder punitivo do Estado e paradigma para análise da sua validade substancial e não apenas formal. Um modelo de racionalidade e contenção da intervenção

estatal na seara criminal, baseada nos direitos fundamentais.

O paradigma constitucional válido para o exercício da investigação criminal consiste na observância de limites à incidência do sistema penal, contendo eventuais excessos da persecução penal, de forma a possibilitar a sua viabilidade jurídica, por meio de uma ação estatal válida, mas também pela sua viabilidade material, através da eficiente promoção de segurança pública, para que o sistema penal desempenhe seu papel vital de defesa do ordenamento jurídico como última instância de controle social e instrumento de garantia de segurança pública, sem violar os direitos humanos constitucionalmente consolidados dos investigados.

Dentre os três modelos de investigação criminal existentes no mundo, o constituinte brasileiro de 1988 adotou o modelo inglês do inquérito policial, cabendo à Polícia Judiciária a sua condução como regra, só podendo haver outros órgãos legitimados para essa atividade em caráter excepcional, mediante expressa previsão legal. Não se concebe a existência de um procedimento de investigação criminal ou com finalidade criminal, realizado sem amparo do direito e da lei. No caso, tais instrumentos de investigação não podem embasar, sem ofensa ao devido processo legal, ação penal cujo propósito final é a condenação do indivíduo a penas que poderão lhe restringir a vida, liberdade ou propriedade.

A investigação preliminar conduzida pela Polícia Judiciária sempre será necessária quando ainda não estiverem presentes elementos suficientes para a promoção da ação penal e tem três finalidades principais: a) servir de filtro processual, fundamentando a decisão do processo ou não processo, evitando uma acusação aventurada; b) esclarecimento de fato oculto que rompe com as regras de convivências social; c) salvaguarda da sociedade por meio de medidas cautelares com natureza pessoal, patrimonial ou probatória. A investigação criminal é uma proteção ao cidadão no sentido de que não será submetido a um processo abusivamente, mas também uma defesa conferida à sociedade de que os atos ilícitos serão efetivamente reprimidos, ainda que aquele que os praticou tente se furtar da responsabilização penal por meio da ocultação do fato criminoso ou de seus instrumentos e proveitos.

O atual sistema constitucional brasileiro, inaugurado pela Constituição Federal de 1988, caracteriza-se pela sua abertura e dinamicidade em razão da capacidade de mutação das significações normativas com o objetivo de se adaptar às novas realidades sociais, por meio da interpretação e aplicação das normas jurídicas. É composto por regras e princípios, sendo o conflito dos primeiros resolvido no campo da validade, por hierarquia, cronologia ou especialidade, enquanto a colisão dos segundos é solucionada pelo balanceamento de interesses, de acordo com seu peso no caso concreto.

Aos diversos direitos fundamentais previstos na Carta Maior, aplica-se a mesma teoria de resolução de conflitos por ponderação, de sorte que não há direto absoluto, pois podem ser limitados por outros direitos ou por outros

valores e bens da coletividade constitucionalmente protegidos. Nas investigações criminais que versam sobre crimes cibernéticos, a busca dos vestígios de autoria e materialidade frequentemente deve ser realizada por meio de técnicas de investigação que podem se chocar com os direitos fundamentais previstos nos incisos X, XI e XII do artigo 5º da Constituição Federal Brasileira, quais sejam, direito à privacidade, inviolabilidade do domicílio e das comunicações. No caso do conflito entre o direito à privacidade, fundamento para o sigilo de dados, e o dever do Estado de promover a persecução penal, deve ser feita a ponderação e prevalecer a possibilidade de acesso a esses dados, desde que seja adequado e necessário à investigação criminal, por meio de autorização judicial, apenas quando o núcleo do direito fundamental for atingido.

Dentre as principais técnicas investigativas utilizadas para a investigação de crimes cibernéticos, destacam-se o acesso a dados cadastrais, pesquisas em fontes abertas, acesso a dados armazenados nas nuvens, busca domiciliar e as interceptações telefônicas e telemáticas. A aplicação das duas primeiras técnicas prescindem de autorização judicial, pois não há privacidade a ser protegida na obtenção de informações relativas à qualificação dos investigados ou voluntariamente tornadas públicas, as quais são de livre manuseio pela autoridade policial responsável pela investigação criminal.

Para as demais técnicas, a reserva de jurisdição está presente. No que se refere à busca de dados armazenados em equipamentos informáticos e disponíveis por meio da rede mundial de computadores, a computação nas nuvens, cabe dizer que é indispensável para muitas apurações criminais desenvolvidas na atualidade, em especial devido à difusão do uso desses meios, que fez com que boa parte das informações relevantes passasse a ser guardada em meios digitais. Mas é preciso que essa coleta se dê de forma célere, sob pena de perecimento da prova ou perda da oportunidade de seu uso.

A maior parte desses dados está guardada fisicamente em outros países e o serviço de armazenamento é oferecido por companhias estrangeiras. Assim, a interpretação tradicional com base no princípio da territorialidade que implicaria na representação pela expedição pela demorada Carta Rogatória não se coaduna com a necessidade de rápido acesso à informação. Nem mesmo o procedimento mais simplificado dos acordos de cooperação bilateral é suficiente.

Nesse contexto, andou bem o Superior Tribunal de Justiça ao adaptar sua interpretação à nova realidade e aplicar o princípio da bandeira da empresa de provimento do serviço de armazenamento, quando houver representação legal da empresa no Brasil, não aceitando o argumento de que a matriz da empresa ou os dados estejam em outro país. Ora, se executa suas atividades aqui, deve obedecer às ordens das autoridades locais. E no caso da empresa que oferece a guarda de dados não ter representação legal no Brasil, deve ser aplicada a abordagem do poder de disposição para permitir um rápido acesso aos necessários à investigação criminal.

Quanto à técnica de busca domiciliar, é preciso observar sua regulamentação disposta a partir do artigo 240 do Código de Processo Penal, que já consagra a reserva de jurisdição em decorrência da inviolabilidade de domicílio prevista constitucionalmente, e apresentando os requisitos para requerimento, deferimento e execução da medida. Não se deve confundi-la com a apreensão, que não é técnica de investigação, mas meio cautelar de obtenção de provas que tem por objetivo assegurar elementos indispensáveis à comprovação do fato e convencimento do juiz. O conceito de casa também gera polêmica e deve-se levar em consideração o entendimento doutrinário e jurisprudencial que incluem na definição qualquer compartimento privado não aberto ao público onde alguém exerce profissão ou atividade, assim como qualquer aposento de habitação coletiva, desde que ocupado.

No que concerne à utilização da interceptação telefônica, deve-se observar os ditames da Lei nº 9.296/1996 para sua aplicação regular, onde constam os requisitos para requerimento, deferimento e execução da medida, também presente a reserva de jurisdição em decorrência da inviolabilidade de comunicações prevista constitucionalmente, que também não veda a utilização de interceptação telemática judicialmente autorizada. Por outro lado, considera-se mais acertado o entendimento já defendido em algumas decisões judicias de que não há quebra de sigilo de comunicações na obtenção apenas de registros de ligações para fins de investigação criminal.

REFERÊNCIAS

ALEXY, Robert. Teoria dos direitos fundamentais. São Paulo: Malheiros, 2008.

_____. A theory of legal argumentation. Oxford: Oxford University Press, 1989.

ALMEIDA NETO, Wilson Rocha de. Atividade de inteligência como instrumento de eficiência na tutela de direitos fundamentais. In: Garantismo penal integral: questões penais e processuais criminalidade moderna e a aplicação do modelo garantista no Brasil. Organizadores: Bruno Calabrich, Douglas Fischer e Eduardo Pelella. Salvador: Juspodivm, 2013.

ASSUMPÇÃO, Luciano Castilho. Dificuldades em interceptações autorizadas de chamadas VOIP. In Revista Criminal: ensaios sobre a atividade policial. Ano 03. Vol. 07. São Paulo: Fiuza, abr/jun 2009.

ÁVILA, Humberto. Teoria dos princípios: da definição à aplicação dos princípios jurídicos. São Paulo: Malheiros, 2005.

AVOLIO, Luiz Torquato. Provas ilícitas – Interceptações telefônicas, ambientais e gravações clandestinas. 3. ed. São Paulo: Revista dos Tribunais, 2003.

BADARÓ, Gustavo Henrique. Direito processual penal. Rio de Janeiro: Elsevier, 2008. BARATTA, Alessandro. Criminologia crítica e crítica do direito penal: introdução à sociológica do direito penal. Rio de Janeiro: Revan, 2011.

BATISTA JÚNIOR, Onofre Alves. Princípio constitucional da eficiência administrativa. Belo Horizonte: Lumen Juris, 2004.

BECK, Ulrich. La sociedad del riesgo: hacia una nueva modernidad. Trad. Jorge Navarro, Daniel Jimenez e Maria Rosa Borras. Buenos Aires: Ed. Paidós, 1998.

BITENCOURT, Cezar Roberto. A inconstitucionalidade dos poderes investigatórios do ministério publico. Doutrinas Essenciais Processo Penal, vol. 2 . São Paulo: Revista dos Tribunais, Jun. 2012.

BONAVIDES, Paulo. Curso de direito constitucional. 15ª ed. São Paulo: Malheiros, 2004. BOLT, Raphael. Criminologia midiática: do discurso punitivo à corrosão simbólica do garantismo. Curitiba: Juruá, 2013.

BRAVO, Rogério. "Open sources" na investigação do cibercrime: conceito e implicações. Lisboa: ed. do a., 2014.

BUENO, Amilton; CARVALHO, Salo de. Aplicação da pena e garantismo. Rio de Janeiro: Lumen Juris, 2001.

BULOS, Uadi Lammêgo. Constituição Federal anotada. 7ª ed. São Paulo: Saraiva, 2007.

CADEMARTORI, Sérgio. Estado de direito e legitimidade. Porto Alegre: Livraria do advogado, 1999.

CANOTILHO, José Joaquim Gomes. Direito constitucional e teoria da constituição. 6ª ed. Coimbra: Almedina, 1993.

_____. Hermenêutica constitucional: métodos e princípios específicos de

interpretação. Florianópolis: Obra Jurídica, 2008.
CARNELUTTI, Francesco. Derecho Procesal Civil y Penal. Trad. Enrique Figueroa Alfonzo. Mexico: Episa, 1997.
CARVALHO, Márcia Haydée Porto de. Sigilo Bancário. Curitiba: Juruá, 2007.
_____. Hermenêutica constitucional: métodos e princípios específicos de interpretação. Florianópolis: Obra Jurídica, 2008.
CASTELLS, Manuel. A Sociedade em rede – a era da informação: economia, sociedade e cultura. v.1. Trad. Roneide Venancio Majer. 6ª ed. São Paulo: Paz e Terra, 1999.
CASTRO, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2ª ed. Rio de Janeiro: Lumen Juris, 2003.
CHOUKR, Fauzi Hassan. Garantias constitucionais na investigação criminal. 3ª ed. Rio de Janeiro: Lumen Juris, 2006.
COLLI, Maciel. Cibercrimes: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.
COLLIARD, Claude-Albert. Libertés publiques. Paris: Dalloz, 1972.
COPETTI NETO, Alfredo. Uma perspectiva garantista do liberalismo e da democracia - Marcos históricos e possibilidades contemporâneas edificados a partir de Principia Iuris. In: Tulio Vianna; Felipe Machado. (Org.). Garantismo Penal no Brasil- Estudos em Homenagem a Luigi Ferrajoli. 1a ed. Belo Horizonte: Forum, 2013.
_____; FISCHER, Ricardo Santi. O paradigma constitucional garantista em Luigi Ferrajoli: a evolução do constitucionalismo político para o constitucionalismo jurídico. In: Revista de Direitos Fundamentais e Democracia. Curitiba. V.14, nº14. P. 409-421, julho/dezembro de 2013.
COSTA, Helena Regina Lobo da; LEONARDI, Marcel. Busca e apreensão e acesso remoto a dados em servidores. Revista Brasileira de Ciências Criminais. Vol.88, p. 203-217. São Paulo: Revista dos Tribunais, Jan. 2011.
DEL CARMEN, Rolando V.; HEMMENS, Graig. Criminal procedure and the supreme court: a guideline to the major decisions on search and seizure, privacy, and individual rights. Plymouth: Rowman & Littefield Publisher Inc, 2010.
DOTTI, René Ariel. A liberdade e o direito à intimidade. SENADO FEDERAL, Revista de informação legislativa. a. 17, n. 66. Brasília, 1980.
FANTINI, Daniel Fábio. Devido processo legal e investigação criminal. In: Revista Brasileira de Ciências Policiais. Brasília, vol. 1, nº 2, p. 11-40, jul/dez 2010.
FERNANDES, Antônio Scarance. Teoria geral do procedimento e o procedimento no processo penal. São Paulo: Revista dos Tribunais, 2005.
_____. O equilíbrio na repressão ao crime organizado. In: Crime organizado: aspectos processuais. Coordenação de Antônio Scarance, José Raul Gavião de Almeida e Maurício Zanoide de Moraes. São Paulo: Revista dos

Tribunais, 2009.
_____. Processo penal constitucional. 6ª ed. São Paulo: Revista dos Tribunais, 2010.
FERRAIOLI, Marzia; DALIA, Andrea Antonio. Manuale di diritto processuale penale. 4ª ed. Milão: Cedam, 2001.
FERRAJOLI, Luigi. Garantismo: una discusión sobre derecho y democracia. Madrid:
Editorial Trotta, 2006.
_____. Principia Iuris: teoría del derecho e de la democracia. 1. Teoría del derecho. Madrid: Editorial Trotta, 2011.
_____. Direito e Razão: teoria do garantismo penal. 4ª ed. Trad. Ana Paula Zomer Sica et al. São Paulo: Revista dos Tribunais, 2014.
FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado. In Revista da Faculdade de Direito da Universidade de São Paulo.Vol.88, p. 439-459. São Paulo: USP, 1993.
FERREIRA, Helder; FONTOURA, Natália de Oliveira. Sistema de justiça criminal no brasil: quadro institucional e um diagnóstico de sua atuação. Brasília: IPEA, 2008.
FERREIRA, Júlio Danilo Souza. A investigação criminal no Brasil e no direito comparado. In: Revista Segurança Pública e Cidadania. Brasília, Vol. 5, nº 1, p.91-110, jan/jun 2012.
FREGADOLLE, Luciana. Direito à intimidade e a prova ilícita. Belo Horizonte: Del Rey, 1998.
GIDDENS, Anthony. Mundo em descontrole: o que a globalização está fazendo de nós. 2º ed. Trad. Maria Luiza X. de A. Borges. Rio de Janeiro: Record, 2002.
GILMAN, Rick. Cloud Computing Evolves. American Agent &Broker.Vol.83, Núm.3, março 2011. Disponível em http://vlex.com/vid/cloud-computing-evolves-259496154, Acesso em 11 jun 2013.
GOMES, Luiz Flávio; CERVINI, Raul. Interceptação telefônica. São Paulo: RT, 1997
GOMES FILHO, Antônio Magalhães. Direito à prova no processo penal. São Paulo: Revista dos Tribunais, 1997.
GRECO, Rogério. Atividade policial: aspectos penais, processuais penais, administrativos e constitucionais. 5ª ed. Niterói: Impetus, 2013.
GRECO FILHO, Vicente. Interceptação telefônica. São Paulo: Saraiva, 1996.
GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães Gomes. As nulidades no processo penal. 7ª ed. São Paulo: Revista dos Tribunais, 2001.
HABERMAS, Jürgen. Direito e democracia: entre facticidade e validade. 2 v. Trad. Flávio Beno Siebeneichler. Rio de Janeiro: Tempo Brasileiro, 1997.
KELSEN, Hans. Teoria pura do direito. São Paulo: Martins Fontes, 2006.

LASSALE, Ferdinand. A essência da Constituição. 3ª ed. São Paulo: Liber Juris, 1988.
LASSO, José Ayala. Direitos humanos e aplicação da lei: manual de formação em direitos humanos para forças policiais. Genebra: Nações Unidas, 2001.
LEHMAN, Jeffrey; PHELPS, Shirelle. West encyclopedia of american law. Thomson Gale: Farmington Hills, 2005.
LOPES JÚNIOR, Aury. Sistemas de investigação preliminar no processo penal. Lumen Juris: Rio de Janeiro, 2001.
LOPES JÚNIOR, Aury; GLOECKNER, Ricardo Jacobsen. Investigação preliminar no processo penal. 6ª ed. São Paulo: Saraiva, 2014.
MACHADO, Marta Rodriguez de Assis. Sociedade de risco e direito penal: uma avaliação de novas tendências políticos-criminais. São Paulo: IBCCRIM, 2005.
MASON, Stephen e GEORGE, Esther. Digital evidence and "cloud" computing. In Computer Law & Security Review. Vol. 27. Elsevier: Londres, 2011.
MEDRONI, Marcelo Batlouni. Crime Organizado: aspectos gerais e mecanismos legais. 4ª ed. São Paulo: Atlas, 2012.
MENDES, Gerri Adriani. O paradigma constitucional de investigação criminal. 363 f. Dissertação (Mestrado em Ciências Criminais). PUC/RS: Porto Alegre, 2010.
MENÉNDEZ, Agustín José. Constitutional rights through discourse: on Robert Alexy's legal theory – european and theoretical perspectives. Oslo: ARENA, 2004.
MODESTO, Paulo. Notas para um debate sobre o princípio da eficiência. Revista Interesse Público, Ano 2, n º 7, julho/setembro de 2000, São Paulo: Ed. Notadez, 2000, p. 65-75.
NEVES, Marcelo.Teoria da inconstitucionalidade das leis. São Paulo: Saraiva, 1988.
NUCCI, Guilherme de Souza. Código Penal Comentado. 7ª edição revista, atualizada e ampliada. São Paulo: Editora Revista dos Tribunais, 2007.
_____.A investigação criminal e a atuação do ministério público. Doutrinas Essenciais de Processo Penal. Vol.2. p.181-186. São Paulo: Revista dos Tribunais, jun.2012.
OLIVEIRA, Marcelo Andrade Cattoni de. Argumentação jurídica e decisionismo: um ensaio de teoria da interpretação jurídica enquanto teoria discursiva da argumentação jurídica de aplicação. In: SAMPAIO, José Adércio Leite (Coord.). Crise e desafios da Constituição: perspectivas críticas da teoria e das práticas constitucionais brasileiras. Belo Horizonte: Del Rey, 2004.
OLIVEIRA, Eugênio Pacelli de. Curso de processo penal. 6ª ed. Belo Horizonte: Del Rey, 2006.
PAREJO, Luciano Alfonso. Seguridad pública y policía administrativa de seguridad – problemas de siempre y de ahora para el deslinde, la decantación y la eficacia de una responsabilidad nuclear del estado administrativo. Valencia:

Tirant lo Blanch, 2008.
PERAZZONI, Franco. O delegado de polícia no sistema jurídico brasileiro: das origens inquisitoriais ao garantismo penal de Ferrajoli. In: Revista segurança pública & cidadania. Brasília. Vol. 4, nº 2, p.77-110, jul/dez 2011.
PITOMBO, Cleunice A. Valetim Bastos. Considerações sobre a tutela da intimidade de vida privada no processo penal. Doutrinas Essenciais de Direito Penal I. Vol.1. p.685-703. São Paulo: Revista dos Tribunais, Jun.2012.
_____. Da busca e apreensão no processo penal. São Paulo: RT, 2005.
PRADO, Geraldo. A interceptação das comunicações telefônicas e o sigilo constitucional de dados operados em sistemas informáticos e telemáticos. Boletim IBCCRIM. São Paulo n.15, 1997.
RODATÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
SANCTIS, Fausto Martin de. Constituição e regime das liberdades. IN: CUNHA, Rogério Sanches; TAQUES, Pedro; e GOMES, Luís Flávio. Limites constitucionais da investigação. São Paulo: Editora Revista dos Tribunais, 2009.
SARLET, Ingo Wolfgang. Dignidade da pessoa humana e direitos humanos fundamentais. Porto Alegre: Livraria do advogado, 2001.
_____. A eficácia dos direitos fundamentais. 9. ed. Porto Alegre: Livraria do Advogado, 2007.
SCHMITT, Carl. Teoría de La constitución. Trad. Francisco Ayala. Madri: Alianza, Universidad Textos, 1982.
SILVA, José Afonso da. Curso de direito constitucional positivo. 27ª ed. São Paulo: Malheiros, 2006.
_____. Em face da constituição federal de 1998, o ministério público pode realizar e/ou presidir investigação criminal, diretamente?. Doutrinas Essenciais de Direito Constitucional.
SMEND, Rudolf. Trad. José María Beneyto Pérez. Constitución y derecho constitucional. Madri: Centro de Estudios Constitucionales, 1985.
SYDOW, Spencer Toth. Crimes Informáticos e suas vítimas. São Paulo: Saraiva, 2013.
TOFOLLI, José Antonio Dias Toffoli e CESTARI, Virgínia Charpinel Junger. Mecanismos de cooperação jurídica internacional no Brasil. In Manual de Cooperação Jurídica Internacional e Recuperação de Ativos – Matéria Penal. 1ª ed. Brasília: Artecor, 2008, p. 31-38.
TUCCI, Rogério Lauria. Direitos e garantias individuais no processo penal brasileiro. Tese para concurso de Professor Titular de Direito Processual Penal, da Faculdade de Direito da Universidade de São Paulo. São Paulo : Saraiva, 1993.
_____. Busca e apreensão (direito processual penal). Doutrinas Essenciais de Processo Penal I. Vol.3. p.1231-1239. São Paulo: Revista dos Tribunais, Jun. 2012.
VACIAGO, Giuseppe. Remote forensics and cloud computing: italian and

european legal overview. In Digital evidence and electronic signature law review. Núm 8, outubro 2011, p. 124-129. Disponível em http://internacional.vlex.com/vid/forensics-cloud-an-andeuropeanoverview-330829794. Acesso em 15 mar 2014.

VALENTE, Manuel Monteiro Guedes. Teoria geral do direito policial. 2ª ed. Coimbra: Almedina, 2009.

_____. Processo Penal. Tomo I. 3ª ed. Lisboa: Almedina, 2012.

VALLE, Juliano Keller do. Crítica à delação premiada: uma análise através da teoria do garantismo penal. São Paulo: Conceito, 2012.

XAVIER, Luciano Bittencourt e. Crítica de Habermas a teoria alexyana dos direitos fundamentais no aborto por anencefalia fetal. Revista da Faculdade Mineira de Direito. Vol. 15, nº 30, jul/dez. 2012.

Capítulo XIV

A parte inconstitucional da lei 12.965/2014 (Marco Civil da Internet)

Delegado de Polícia Civil Ruchester Marreiros Barbosa[251]

1. INTRODUÇÃO

O ordenamento Constitucional ao adotar o sistema acusatório como sistema processual penal norteador da *persecutio criminis* no Estado Democrático de Direito atribui ao Estado-investigação, presentado pelo Delegado de Polícia, um feixe de poderes-deveres meios, muitas das vezes de natureza decisória e também cautelar para consecução dos fins da investigação criminal, qual seja a apuração a verdade eticamente construída da infração penal e dos indícios de sua autoria.

2. RESERVA ABSOLUTA E RELATIVA DE JURISDIÇÃO

A Constituição da República e por intermédio das normas infraconstitucionais adotou um sistema de reserva absoluta e relativa da jurisdição, ou seja, na investigação criminal haverá medidas de natureza investigatória que deverão ser decididas exclusivamente pelo Estado-juiz, hipótese de reserva absoluta, e outras

[251] Delegado da Polícia Civil do Rio de Janeiro, especialista em Penal e Processo Penal, doutorando em Direitos Humanos na Universidad Nacional de Lomas de Zamora (Argentina), professor de Processo Penal da Escola da Magistratura do Estado do Rio de Janeiro, professor de Penal e Processo Penal da graduação e da pós-graduação em Direito Penal e Processo Penal da Universidade Estácio de Sá; Professor de Direito Penal da pós-graduação em Direito Ambiental da UNESA; Processual de Direito Penal da pós-graduação em Direito Tributário do Portal F3; Professor de Professo Penal da Pós-graduação da FACTOPAR, Apucarana, Paraná; Professor de Penal e Processo Penal da Secretaria de Segurança Pública do Estado do Rio de Janeiro; Professor de Processo Penal do curso preparatório da FAEPOL; Professor de Direito Penal do curso preparatório CURSO CEI; Professor de programas de vídeo aulas preparatório para OAB e ENADE da UNESA; coautor de obras jurídicas; colunista do portal Consultor Jurídico e do portal Canal Ciências Criminais; Professor convidado da Escola Nacional de Polícia Judiciária, Brasília/DF; Membro da International Association of Penal Law e da Law Enforcement Against Prohibiton.

medidas decididas pelo Estado-investigador, hipótese de reserva relativa, que passa por um controle posterior ao Estado-juiz.

Insta salientar, que este controle posterior em algumas vezes será de ofício e em outras ocasiões somente quando provocado, que na nossa visão, deve ser comunicado ao judiciário imediatamente após a decisão por restrição ou privação de direitos de ir e vir, face ao necessário atendimento ao um sistema de dupla cautelaridade.[ii]

Este sistema também é apontado pelo jurista Luiz Flávio Gomes[iii], que nos citando em artigo de sua lavra, sobre audiência de custódia, deixa clara a sua manifestação pela total constitucionalidade de se reconhecer o poder decisório de liberdade provisória pelo delegado, que por sua vez, possui natureza de uma contracautela.

Nas lições de Canotilho, a reserva de jurisdição se divide em relativa e absoluta. A distinção em síntese, consiste, em se compreender que na absoluta a ingerência na esfera subjetiva das pessoas é realizada primeira mente pelo juiz, na qual é garantida a revisão desta decisão no próprio âmbito do judiciário. Trata-se, portanto, o que ele denomina de esfera da primeira e última palavra pelo judiciário. Em outras palavras, o judiciário é o primeiro chamado a decidir e o último também, porquanto responsável pela revisão desta primeira decisão.

Na reserva relativa a ingerência é realizada por outra autoridade pública, podendo ser revisada pelo judiciário. Neste caso a revisão será dará por ato de ofício, por força de lei, ou por provocação do interessado. Vale a pena trazer a colação a explicação do festejado autor Tércio Sampaio, *ipsis literis*:

> *"Esta garantia de justiça tanto pode ser reclamada em casos de lesão ou violação de direitos e interesses particulares por medidas* ***e decisões de outros poderes e autoridades públicas (monopólio da última palavra contra actos do Estado****) como em casos de litígios particulares e, por isso, carecidos de uma decisão definitiva e imparcial juridicamente vinculativa (monopólio da última palavra em litígios jurídicos-privados)"*[iv] (Destaque nosso).

Ainda neste mesmo sentido, Luiz Flávio Gomes[v]:

> "*Desde logo é preciso distinguir: uma coisa é a "comunicação telefônica" em si, outra bem diferente são os registros pertinentes às comunicações telefônicas, registros esses que são documentados e armazenados pela companhia telefônica, tais como: data da chamada telefônica, horário, número do telefone chamado, duração do uso, valor da chamada, etc. Pode-se dizer que esses registros configuram os 'dados' escritos correspondentes às comunicações telefônicas. Não são 'dados' no sentido utilizado pela ciência da informática ('informação em forma codificada'), senão referências, registros de uma comunicação telefônica, que atestam sua existência, duração, destino, etc. (....)"*

A conclusão do estudo em Canotilho nos permite inferir de que a

Constituição definirá quais direitos estarão sob a exige de uma reserva absoluta e quais sob a reserva relativa.

2.1 Incidência da reserva relativa

Ora, se a liberdade é uma contracautela é porque a prisão em flagrante decidida pelo delegado de polícia tem natureza cautelar. Ou então, em nome da lógica, a liberdade provisória seria uma contra precautela? Não há amparo teórico ôntico-ontológico na teoria geral das cautelares para esta conclusão.

Por uma questão de simples coerência, se a doutrina é uníssona em entender que a liberdade provisória é uma espécie de medida cautelar, ou contracautela[vi], não há outra conclusão lógica existente quando o delegado de polícia ao determinar e presidir a lavratura do auto de prisão em flagrante, concede liberdade provisória mediante fiança, por exemplo, estaremos diante de duas decisões (e não despacho, por favor.) de naturezas cautelares. Seja emanado por autoridade administrativa ou não, o rótulo não altera o conteúdo e a finalidade.

Por oportuno, registramos que a natureza cautelar de atos administrativos não é novidade na doutrina de João Gualberto Garcez[vii]:

> *"O inquérito policial é uma medida complexa, pois é formada por diversas outras medidas, todas direcionadas à sua meta optata: servir de base e apoio a atividades que se desenvolverão em juízo. Não parece, outrossim, que haveria inconveniência em designar o inquérito policial como um procedimento administrativo cautelar."*

Não é por outra razão que defendemos há muito tempo que o delegado de polícia não é uma figura autômata no âmbito da investigação criminal, pois a todo instante exerce função imanente de decidir, e uma das mais importantes, que dá sentido à sua função democrática, além da exclusiva função de investigar, é assegurar que ninguém será levado à prisão ou nela mantido quando por cabível liberdade provisória, ou até mesmo decidir pela não lavratura do auto de prisão em flagrante por estar calçada em prova ilícita, exercendo o papel de verdadeira autoridade de garantias[viii], função tipicamente judicial, que não se confunde com a estritamente jurisdicional, segundo interpretação da Corte Interamericana de Direitos Humanos[ix].

2.1.1 A natureza cautelar e não autoexecutória do estado-investigação

Há um mito de que todas as garantias fundamentais para serem afastadas dependam única e exclusivamente de uma decisão primeira do judiciário, ou seja, uma autorização prévia do juiz para que o Estado-investigação possa empregar seus métodos de investigação para alcançar sua finalidade precípua que é a descoberta da verdade eticamente construída, e dentro dos limites da vedação à prova ilícita.

Há um equívoco nesta lenda urbana. Nem mesmo nas lições de Canotilho encontramos tamanha leviandade epistemológica.

Não se trata, contudo de que o fundamento na atuação da polícia judiciária seja toda ela pautada em atos de emergência. Nem por isso sejam atos na ceara da autoexecutoriedade dos atos administrativos, em razão da necessidade de se analisar cada caso concreto de forma independente para aplicar a norma penal e processual penal, ainda que em cognição sumária.

Qualquer medida ou mecanismo que vislumbre a reconstrução histórica dos fatos com o fim de se delinear a responsabilidade criminal em sede de investigação criminal é um caminhar para atos invasivos na esfera da intimidade do investigado. Sobre isso não há dúvidas.

A questão é: que desenho constitucional adotamos?

Todos os atos de polícia judiciária devem possuir controle prévio do judiciário? Todos são invasivos? Em qual grau se dá esta afetação de direitos e garantias fundamentais? É evidente que este modesto artigo não tem como propósito esgotar um tema tão complexo, mas devemos amadurecer nossa doutrina e desvendar contos de fadas. Já estamos em uma faixa etária democrática de que não podemos mais acreditar mantras e dogmas que reproduzem desequilíbrio na divisão das funções no sistema acusatório. Ou seja, não há que se demonizar qualquer ato de Estado, ou deslegitima-lo pela simples razão de não estar "ratificado" pelo poder judiciário. O Estado-investigação também possui legitimidade e não há inconstitucionalidade em se realizar controle posterior de seus atos. A Constituição é o norte a ser seguido.

A reposta gira em torno do que se entende por reserva da jurisdição, conforme a distinção que elaboramos, com base nas lições de Canotilho em tópico acima.

O desafio é traçar os limites ou em que situações qual órgão será detentor da primeira palavra, o Estado-investigação ou o Estado-juiz, já que este exercerá sempre a última palavra, seja de quem for a primeira (delegado ou juiz).

Um dos temas mais polêmicos sobre este limite está na decisão sobre o afastamento da reserva da intimidade, como por exemplo a identificação de usuários de telefonia, e seus dados correspondentes, ou quebra do sigilo fiscal pelas CPI´s, ou acesso aos dados das contas reversas (ligações efetuadas e recebidas) pelo usuário etc.

A este respeito defendemos, especificamente para este estudo, sobre acesso a dados que permitam a identificação do investigado, que o Estado-investigação possui a primeira palavra por se tratar de uma reserva relativa da jurisdição, sendo a absoluta, jungida às hipóteses do conteúdo das relações, mas não seus vestígios, como os dados referentes com quem os interlocutores se comunicaram. É esse o sentido do sigilo das comunicações telefônicas, telegráficas e telemática previsto no art. 5º, XII, CR.

A doutrina já aponta esta interpretação conforme se destaca abaixo:

> *"Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos - como o nome, endereço, profissão, idade, estado civil, filiação, número de*

registro público oficial, etc., condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido."[x]

Por uma questão de premissa e não de conclusão, ousamos discordar da conclusão do ilustre jurista. Na verdade, esses dados podem estar protegidos pelo sigilo, posto que a ninguém é resguardado o direito de ter acesso a essas informações acaso o usuário não conceda autorização para divulgação de suas informações, seus dados.

No entanto, tais sigilos, em verdade não estão sujeitos à reserva absoluta da jurisdição, mas sim sob a reserva relativa, o que significa dizer, que o Estado-investigação tem o poder-dever de requisitar tais informações no profícuo propósito de identificar os sujeitos (autor, partícipe, testemunhas e vítimas) relacionados ao fato crime.

Ao Estado-investigação é permitido enveredar por medidas invasivas, e que eventualmente, esteja relacionado ao sopesamento de direitos e que deva decidir qual deles tenha que prevalecer, quando a estes direitos não tenham sido albergados prioritariamente a primeira palavra ao judiciário, como por exemplo a interceptação telefônica, na qual a Constituição definiu como hipótese de reserva absoluta. Por esta razão não se trata de uma atividade autômata e autoexecutável, mas de natureza cautelar para preservação da prova. Não se trata de atos meramente administrativos, mas que pairam análise técnico jurídica sobre cada caso concreto, o que gera um cariz de atividade judicial ou jurídica-judicial, ainda que por órgão que não seja tipicamente jurisdicional.

Até mesmo a busca e apreensão domiciliar é muito bem delineada sobre o que está sobre a reserva absoluta e relativa de jurisdição, haja vista que o próprio constituinte originário autoriza que a decisão sobre a busca tenha como primeira palavra o Estado-investigação, nas hipóteses delineadas pela concepção do flagrante delito, e, aquelas fora deste contexto, a primeira palavra pertence ao judiciário.

Primeira ou última palavra implica dizer quem definirá a Constitucionalidade ou não desta decisão de determinar a busca e apreensão domiciliar. Nos concentraremos, por limitação de espaço às hipóteses do Delegado de Polícia como sendo a autoridade que possua esta atribuição.

2.1.2 Caso prático de decisão de natureza cautelar de reserva relativa

Imagine que seja levado ao conhecimento do Delegado um fato narrado por agentes da autoridade de polícia judiciária, como por exemplo, agentes da polícia militar (soldado ao coronel), qualquer do povo, ou por agentes da própria polícia judiciária de hipótese, em tese, apreciada por eles como flagrante delito,

conduzindo coercitivamente um suspeito de furtar um relógio. Orientados pela própria vítima chegaram à casa do suspeito, que não possuía muros, e lá chegando, viram pela janela que o relógio objeto do crime estava no interior da residência em cima da cômoda.

Os agentes, de cujo cargo não é exigido formação de bacharel em direito, embora alguns deles possam tê-lo cursado, supondo estar o suspeito em situação de flagrante delito, ingressam na residência, apreendem o bem e conduzem o homem até a presença do Delegado, que narram este fato, bem como narra a vítima, que o furto ocorrera somente há duas semanas atrás.

Ora, não há outra resposta senão entender que se trata de uma prova ilícita, pela simples razão de ingresso em domicílio fora de uma hipótese de flagrante delito, haja vista que o crime de furto é instantâneo e a utilização do objeto é mero exaurimento dele.

O Delegado nesta hipótese não poderia lavrar auto de prisão em flagrante. Trata-se de uma hipótese em que o conduzido coercitivamente, e algemado, por exemplo, será imediatamente libertado por se tratar de uma prisão ilegal de cujas evidências, sequer poderão ser utilizadas como prova para evidenciar eventual justa causa para a denúncia.

Este exemplo deixa muito claro que foi o delegado de polícia quem decidiu pela não prisão em flagrante e atendeu à constituição da República de cuja norma anuncia em seu art. 5º, LXI, que ninguém será preso senão em flagrante delito. A captura pode ser realizada por qualquer um, mas a detenção e sua manutenção somente o Delegado de Polícia.

Como já dissemos na obra jurídica Diálogos Jurídicos na Contemporaneidade[xi], em coautoria com outros juristas, é plenamente pacífico o convívio de medidas cautelares sob a gestão da autoridade de garantias e o monopólio da jurisdição, ou seja, coexistem no ordenamento constitucional mecanismos aptos a ensejar um procedimento investigatório criminal com autonomia e efetividade garantista, nas quais engendram decisões fora da reserva absoluta da jurisdição, sob controle posterior, alcance do real sentido do art. 5º, XXXV da CR.

Em outras palavras, a reserva absoluta da jurisdição não significa que o Estado-investigação não possa praticar atos de natureza decisória[xii], pelo contrário, a constituição e as normas infraconstitucionais prevêem medidas acautelatórias e requisições pelo Delegado de Polícia, v.g. art. 23, VII,30 31§4º31 e art. 33, III32, todos da Lei 12.527/11, art. 17-B da Lei 12.683/1233, art. 2º,§2º da lei 12.830/1334 e art. 15 da lei 12.850/1335, mas que a toda evidência não estão no âmbito de incidência da reserva absoluta da jurisdição. Neste caso, os atos são praticados sem prejuízo do controle judiciário, conforme dispõe o art. 5º, XXXV da CRFB, mas com fundamento igualmente constitucional, conforme art. 5º, XXXIII da CR/88.

2.1.3 Precedente do supremo sobre reserva relativa

Não nos deixa mentir recentíssima decisão do STF, da lavra do eminente Constitucionalista, Min. Luís Roberto Barroso por ocasião do julgamento do HC 124.322/RS, na qual não deixou dúvidas de que a obtenção direta de dados cadastrais telefônicos pelo Delegado de Polícia não configura quebra de sigilo das comunicações telefônicas.

Ao negar seguimento ao referido *habeas*, o ministro confirmou jurisprudência da Corte[xiii], destacando que o fornecimento de registros sobre hora, local e duração de chamadas, ainda que sem decisão judicial, não contraria o art. 5º, XII, da Constituição da República, que protege apenas o conteúdo da comunicação telefônica. Esta decisão ratificou, no caso concreto, o mesmo posicionamento do STJ[xiv] e do TRF da 4ª Região[xv].

Não há como se negar, doutrinária e jurisprudencialmente, a existência de medidas acautelatórias sob a gestão do Delegado e se reconhecer o poder geral cautelar administrativo como função imanente à investigação criminal, verdadeiro elemento de democraticidade, verdade e constitucionalidade, para além de um sistema acusatório.

3. O TRATAMENTO INCONSTITUCIONAL DO MARCO CIVIL DA INTERNET À INVESTIGAÇÃO CRIMINAL

Não há dúvidas que A lei 12.695/14 definiu alguns parâmetros de regras técnicas – ainda que superficiais – a serem consideradas pelo intérprete, diminuindo a margem de erros jurídicos por ausência de conhecimento técnico provenientes da ciência da computação, a despeito da distinção, por exemplo, da atividade de distribuição de sinal realizada por provedores de acesso à internet (art. 5º, III), serviço realizado, por operadores de distribuição de acesso à internet (provedores de acesso: Empresa OI, por exemplo) e uma atividade realizada por provedoras de aplicação (art. 5º, VII), serviço oferecido pelos sítios ou web sites (provedores de serviço: de email "Hotmail" da Microsoft; ou sítio: yahoo.com.br, por exemplo).

Por outro lado, o legislador ao tentar, desnecessariamente, regulamentar o sigilo das comunicações, que surge do fluxo de dados, entrou em uma contradição sistêmica, criando uma verdadeira antinomia, exagerando na jurisdicionalização de tudo que se relaciona à internet, criando reserva da jurisdição onde a constituição não prevê, conseqüentemente eivando de inconstitucionalidade algumas normas.

Importante salientar, que os argumentos a respeito da inconstitucionalidade estão em plena sintonia com o garantismo penal, pois até mesmo para a atuação do Estado há balisas constitucionais pelos quais se respalda ao argumento de que os atos de investigação quando voltados à preservação da reserva da intimidade possui contornos garantidores, como já alerta a doutrina, *in verbis*[xvi]:

"...a segurança pessoal é uma variável das mais importantes a serem consideradas nas estratégias de respeito aos direitos humanos. E segurança – tanto quanto saúde, educação, trabalho, etc. – é um benefício que um Estado democrático deve aos seus cidadãos. Sem ela, voltamos ao chamado "estado de natureza" – que talvez seja menos idílico do que pintaram os contratualistas da nossa predileção. Ou seja: lemos tanto Rousseau, que esquecemos Hobbes...".

3.1 Violação ao princípio da vedação à proteção deficiente

Outrossim, além dos atos de investigação, sob o prisma de um inquérito penal de garantias[xvii], serem voltados para a proteção da reserva da intimidade do investigado, também não restam dúvidas que haja necessidade de um procedimento sob o crivo da duração razoável da investigação[xviii] de modo que se permita lançar mão de providências eficazes e velozes no intuito de se proteger o mesmo bem jurídico da vítima, sob pena de **violação do princípio da proibição à proteção deficiente**.

O marco civil através de uma regulamentação positiva, e até bem intencionada, acaba por desproteger as vítimas de crimes praticados na internet ou por meio da internet, incidindo em uma insuficiente proteção desta, quando se estabelece reserva de jurisdição onde a constituição federal e o STF não previram, inviabilizando uma investigação rápida e resposta eficaz na proteção de direitos fundamentais da vítima, se fazendo necessário o que a doutrina denomina de **garantismo positivo**.

O professor Luiz Flávio Gomes sobre o tema, no artigo "Princípio da Proibição de Proteção Deficiente"[xix], cita Lênio Streck, na qual dispõe sobre a dupla face do princípio da proporcionalidade:

"Trata-se de entender, assim, que a proporcionalidade possui uma dupla face: de proteção positiva e de proteção de omissões estatais. Ou seja, a inconstitucionalidade pode ser decorrente de excesso do Estado, caso em que determinado ato é desarrazoado, resultando desproporcional o resultado do sopesamento (Abwägung) entre fins e meios; de outro, a inconstitucionalidade pode advir de proteção insuficiente de um direito fundamental-social, como ocorre quando o Estado abre mão do uso de determinadas sanções penais ou administrativas para proteger determinados bens jurídicos. Este duplo viés do princípio da proporcionalidade decorre da necessária vinculação de todos os atos estatais à materialidade da Constituição, e que tem como conseqüência a sensível diminuição da discricionariedade (liberdade de conformação) do legislador."(Streck, Lênio Luiz. A dupla face do princípio da proporcionalidade: da proibição de excesso (Übermassverbot) à proibição de proteção deficiente (Untermassverbot) ou de como não há blindagem

contra normas penais inconstitucionais. Revista da Ajuris, Ano XXXII, nº 97, marco/2005, p.180)"

A lei 12.965/14 foi leniente neste mister protetivo, pois cria uma confusão primária entre dados qualificativos para identificação e rastreamento do criminoso com os dados oriundos do fluxo de informações travadas entre o usuário e uma outra pessoa (jurídica ou privada).

No art. 7º, II, III e VII o legislador faz distinção entre fluxo de dados que se referem a conversações em tempo real no inc. II; fluxo de dados em geral travados com terceiros que ficam armazenados nos provedores de aplicação somente (por força do art. 14 é proibido este tipo de armazenamento pelos provedores de conexão) no inc. III; e os dados que identificam o usuário do serviço que teria praticado o crime no inc. VII.

Para o acesso aos dados dos incisos II e III deve o delegado de polícia jungir-se da ordem judicial por decorrência do princípio da reserva jurisdicional, já dispostas no art. 5º, XII da CRFB, no entanto, o inciso VII não, por se tratar de meros dados identificativos do usuário criminoso, sendo princípio norteador, conforme art. 5º, IV da CRFB, a vedação ao anonimato.

No art. 7º, VII se referem aos dados que identificam o criminoso, como se fossem suas pegadas e impressões digitais deixadas em local público, ou seja, seus rastros e seus vestígios, sobre os quais o legislador em diversas leis federais[xx], atendendo às diversas decisões do STJ[xxi] e STF[xxii], entendem que esses dados não estão acobertados sob o primado da reserva absoluta da jurisdição, por uma interpretação conforme ao o art. 5º, IV (vedação ao anonimato) e XII (autorização judicial para captação de fluxo de dados telefônicos e não os dados em si).

No entanto, este mesmo legislador, na mesma lei, em uma mesma ocasião histórica de sua elaboração, coloca em choque essas premissas basilares em seu art. 10, §1º e §3º, estabelecendo uma antinomia entre esses parágrafos e o seus princípios norteadores dispostos no art. 5º, em especial, o inciso VI.

No §1º entende que os dados de identificação do usuário da internet devem ser precedidos de autorização judicial e já no §3º entende que os dados "que informem qualificação pessoal, filiação e endereço" podem ser requisitados "pelas autoridades administrativas que detenham competência legal para a sua requisição"[xxiii], ou seja, o delegado de polícia na investigação criminal, conforme art. 17-B da Lei 12.683/12, art. 2º, §2º da lei 12.830/13 e art. 15 da lei 12.850/13. Hipóteses de reserva relativa de jurisdição.

Mais adiante, confrontando os dispositivos acima com o art. 13, §2º e o art. 15, §3º os dispositivos passam a prever hipóteses de reserva absoluta da jurisdição para os dados de registros de conexão e registros de aplicação. Em outras palavras, respectivamente os "logs de IP[xxiv]" registrados nos provedores de conexão como, OI, Net, GVT etc e os "logs de IP" dos provedores de aplicação ou software como facebook, Google etc.

3.2 A previsão de reserva absoluta de jurisdição não previstos pela constituição

O legislador elevou os registros de conexão à dimensão da reserva absoluta sob vestígios do crime pelo qual a Constituição de 88 não criou. Esses registros dizem respeito apenas à origem da conexão, isto é, do terminal utilizado pelo criminoso até o provedor, e não o conteúdo dos pacotes de dados que são transportados através dos protocolos de comunicação (TCP/IP).

Em termos práticos, imaginemos um sujeito que pratica crimes de exploração sexual em geral contra vulnerável, v.g. o art. 218 ao 218-B, 241-A; B ou 241-D da lei 8.069/90 utilizando-se de um "fake" pelas redes sociais ou email anônimo, navegando por um terminal instalado em uma "lan house", mesmo possuindo um computador em sua residência. Senão vejamos:

Suponhamos que este criminoso se comunique através de um email de domínio @hotmail.com ou através do facebook com uma criança induzindo-a e atraindo-a para praticar ato libidinoso e à prostituição, respectivamente art. 241-D da lei 8.069/90 e 218-B do Código Penal. A mãe toma conhecimento e comunica o fato à delegacia de polícia, informando que o mesmo está naquele momento se comunicando em tempo real com a criança em sua residência monitorada pelo pai.

O delegado de polícia então requisita imediatamente por fax e contato telefônico que a provedora empresa Microsoft no Brasil o IP do email do "pedófilo", como vulgarmente as mídias denominam pessoas nestas circunstâncias criminógenas, (ticio@hotmail.com) que se comunicou com o IP pertencente ao email da criança (criança@hotmail.com). A partir daí a Microsoft informaria o IP do terminal (computador) que fez conexão com o terminal (computador) onde estaria a criança.

Sabendo-se que aquela utiliza o provedor de conexão da empresa "OI" para acessar a internet, o delegado com base na informação do IP do criminoso fornecido pela Microsoft (chamemos de IP 171.0.30.218), solicita à OI o número telefônico que utilizou este IP pelo qual se conectou com o IP da criança (chamemos de IP 010.0.10.11), que utilizava o número telefônico fixo 555-1010.

A OI então informa que o telefone que utiliza o IP 171.0.30.218 (do criminoso) é o número fixo 555-0171. Com esta informação em mãos o delegado de polícia requisita os dados cadastrais à operadora de telefonia na qual o número é administrado, recebendo o endereço de uma pessoa jurídica que exerce atividade de "lan house", não conseguindo, neste momento identificar o "usuário pedófilo", tendo em vista que no momento da diligência o mesmo teria saído a poucos instantes antes da chegada da polícia para sua prisão em flagrante.

Evidentemente que o "pedófilo" se utilizou, metaforicamente, um caminho (computador de lan house), utilizando-se de um "capacete" (computador de acesso público) para esconder seu "rosto digital" ou "impressão digital", impedindo sua "visualização digital" e física, consequentemente, sua identificação e posterior localização. É muito comum que o criminoso utilize este

mesmo email para outras comunicações não criminosas, e estas são realizadas de sua residência, posto que estaria em uma situação "normal", e portanto, não teria motivos para se esconder. É como se nesta situação o mesmo percorresse um caminho não clandestino e, portanto, deixa seu "rosto digital" ou "impressões digitais virtuais" visualizável.

Em prosseguimento ao incauto do criminoso, quando o mesmo utiliza o email da sua casa, ele para a ser "visualizado digitalmente", pois não estaria utilizando nenhum anteparo (lan house) em seu "rosto digital". Diante desta circunstância bastaria uma requisição à empresa Microsoft para que a mesma fornecesse os registros de conexão (os chamados "logs de IP") para identificar os números telefônicos relacionados à lista de IPs constatados na utilização do email ticio@hotmail.com.

Evidentemente, ciente de que os números telefônicos relacionados estariam ligados ao email de um criminoso e o fornecimentos dos dados cadastrais destes números ou outro número utilizado repetidamente que não fosse o da "lan house" permitiria identificar o telefone "pedófilo", consequentemente, seu endereço físico. Diante deste quadro e se cercando das cautelas necessárias, o delegado de polícia providenciaria aparato policial para cercar a residência enquanto diligenciaria até o juiz para representar pela busca apreensão (esta sob a reserva absoluta da jurisdição), logrando êxito em encontrar o criminoso e prendê-lo em flagrante, na forma do art. 302, III do CPP, na modalidade de flagrante impróprio, em razão da perseguição até seu encontro pelas diligências do Estado-investigação.

3.3 Ausência de prova produzida por meios ilícitos

Destaca-se que a prisão em flagrante se daria com a representação com uma busca e apreensão deferida pelo judiciário, por não ter a certeza visual da prática do delito no interior da residência do criminoso, bem como todos os dados fornecidos por requisições do delegado de polícia foi **sem nenhuma interceptação de conversações por fluxo de dados dos email´s entre remetente e destinatário ou armazenamento de dados de conversações**, conforme preconizaria o art. 7º, II e III como uma interpretação análoga ao art. 5º, XII da CRFB.

É importante lembrar que identificação do ser humano no mundo real (plano físico) é distinta no mundo virtual (cyber espaço) se dá com a simples utilização de documento e o fornecimento dos dados qualificativos de forma escrita (documentada) ou verbal (a ser documentada), como quer fazer entender o art. 10, §3º. O mesmo não ocorre no mundo virtual, pois a realidade virtual enseja inúmeras formas de se mostrar e aparecer através diversos caminhos denominados "camadas". Em outras palavras, a identificação na realidade virtual é dinâmica e não significa somente a revelação do nome e endereço físico, mas a revelação de toda a identificação virtual ou digital do criminoso pelo cyber espaço.

No mundo real, após a identificação do endereço pelos dados cadastrais, basta localizá-lo no mapa e percorrer o caminho necessário até chegar ao caminho destino. Esses caminhos possuem caráter público. No cyber espaço o endereço IP (identificado pelo email, por exemplo), também percorre caminhos virtuais chamados de "camadas" e permite saber a trajetória utilizada pelo IP, conforme o exemplo acima.

No entanto, nos parece que careceu o legislador de dados e informações técnicas necessárias para não realizar esta confusão entre os dispositivos supramencionados, acabando por não proteger a vítima de forma efetiva.

Conforme bem ilustrou o exemplo narrado acima, na atualidade é assim que vem agindo a polícia para tramitar de forma célere e efetiva à proteção de direitos humanos fundamentais, no entanto, conforme os artigos 10, §1º, 13, §5º e 15, §3º os logs de registro utilizados pelo criminoso pelo provedor de aplicação somente podem ser concedidos mediante autorização judicial. É como se o delegado tivesse que pedir autorização judicial para retirar as impressões digitais deixadas pelo criminoso no local do crime ou em local público, e pior de tudo, em situação de flagrante delito, para realização da perícia para posteriormente se chegar a qualificação do titular da digital do dedo.

Se, no exemplo acima, para cada requisição de registros de aplicação e de conexão fosse necessária representação por autorização judicial teríamos que ter representado três vezes da seguinte forma:

Após a elaboração da representação pelo Delegado se remeteria os autos ao Ministério Púbico, retornando após alguns meses para a delegacia, posteriormente seria remetido ao judiciário, retornando por mais alguns meses com a medida de quebra do número do IP dos email´s dos interlocutores (autor e vítima). Após, representação à operadoras de telefonia (provedor de conexão) para saber o cadastro do telefone relacionado ao IP, que foi informado pelo provedor de serviços (Microsoft). Diante do endereço, diligenciaria ao local e se descobriria que o telefone é de uma lan house. Diante disso o delegado representaria pela lista de telefones utilizados por aquele IP, de aproximadamente dos últimos 3 meses, para a operadora de serviços. Após a aquisição dos números, representaria para as empresas de telefonia fornecerem os endereços dos números suspeitos de ser da casa ou trabalho do investigado.

Como se percebe, seriam 4 representações, mas por quatro vezes seguidas, totalizando oito idas e vindas do procedimento, o que nos daria, se fosse em média um mês para cada remessa, um total de aproximadamente 8 meses para se descobrir, pasmem, **APENAS o NOME** e endereço do "pedófilo", evidenciando, como numa lógica cartesiana, um sistema absolutamente inconstitucional de investigação criminal no marco civil da internet, levando muito tempo para se investigar um crime que pode acontecer com certa freqüência na rotina da polícia judiciária, e enquanto isso, o criminoso fica livre para fazer mais crianças vítimas.

O prof. Henrique Hoffman[xxv] em seu artigo publicado na revista eletrônica do conjur nos lembra bem que o STJ já se pronunciou sobre o tema e concluiu pela total desnecessidade de autorização judicial:

> *"A obtenção dos dados do usuário de determinado IP* — Internet Protocol *consistentes tão-só na identificação de propriedade do computador e do endereço em que instalado, de caráter cadastral, pois não descortina qualquer aspecto do modus vivendi da pessoa, prescinde de autorização judicial. STJ, HC 83.338, Rel. Min. Hamilton Carvalhido, julgado em 29/9/2009."*

Assim também se pronunciou o II encontro Nacional dos Delegados de Polícia para o aperfeiçoamento da Democracia e Direitos Humanos em seu enunciado 19:

> *"Os dados cadastrais de clientes de instituições financeiras, operadoras de telefonia fixa e móvel, dentre outras, não têm seu sigilo condicionado à reserva de jurisdição, podendo ser requisitados diretamente pelo delegado de polícia, que deverá estabelecer prazo razoável para a sua resposta, cujo descumprimento ensejará a ocorrência do crime previsto no art. 21 da lei nº 12.850/13, ou subsidiariamente, o do art. 330 do Código Penal."*

4. CONCLUSÃO

Desta forma, não resta outra conclusão, que não seja da inconstitucionalidade das normas que exigem autorização judicial para a identificação virtual do criminoso através dos registros de conexão do terminal ou registros de aplicações pelos usuários, por violação ao princípio da vedação proibição à proteção deficiente, que definiu equivocadamente uma hipótese de reserva absoluta de jurisdicional não prevista pela CRFB.

A Polícia Judiciária deve, diante do poder requisitório de natureza cautelar que lhe é atribuído pela Constituição da República, como meios necessários aos fins propostos pelo Constituinte Originário, qual seja a atuação eficaz na descoberta de indícios de autoria e prova do crime determinar aos órgãos privados ou públicos diretamente.

Outrossim, por não haver prazo expresso para o cumprimento nos diplomas que fundamentam este poder-dever requisitório, v.g. art. 17-D da Lei 9.613/95 c/c art. 2º, §2º da Lei 12.830/13 e art. 15 da lei 12.850/13, que torna explícito o poder de requisição do Estado investigação, deve determinar pelo prazo de até 15 dias à luz do art. 3º do CPP c/c art. 8º da Lei 7347/85, na qual por alusão a caso semelhante ao que ocorre no inquérito civil público, que possui a mesma natureza jurídica do inquérito policial, aplica-se o brocardo *ubi eadem ratio ibi*

idem jus, que significa, onde houver o mesmo fundamento haverá o mesmo direito.

Nesta feita, acaso não seja cumprida a ordem, incidirá o responsável pela informação o empregado particular no crime de desobediência, nos termos do artigo 330 do Código Penal ou art. 21 da lei 12.850/13, e acaso seja funcionário público, no crime de prevaricação, previsto no art. 319 do Código Penal, evidentemente, todos a serem analisados em cada caso concreto.

5 - REFERÊNCIAS

1. BARBOSA, Marreiros Ruchester; et al, Cood. Geral, DELGADO, Ana Paula Teixeira; MELLO, Cleyson de Moraes; PACHECO, Nívea Maria Dutra. As Novas Fronteiras do Direito Estudos Interdisciplinares em Homenagem ao Professor Francisco de Assis Maciel Tavares. In Audiência de Custódia (Garantia) e o Sistema da Dupla Cautelaridade Como Direito Humano Fundamental. Juiz de Fora: Editar, 2015, p. 176 e 177.
2. GOMES, Luiz Flávio. Disponível em <http://luizflaviogomes.com/nucci-como-juiz-rasgou-a-convencao-americana/>, acesso em 06/12/2015.
3. CANOTILHO, J.J. Gomes, Direito Constitucional e Teoria da Constituição. 7. ed., 11. reimp., Almedina, Almedina, p.584.
4. GOMES, Luiz Flávio. A CPI e a quebra do sigilo telefônico. Consulex: revista jurídica, v. 1, n. 5. Brasília/DF, maio 1997, p. 40.
5. TÁVORA, Nestor e ALENCAR, Rosmar Rodrigues. Curso de Direito Processual Penal. 10ª Ed. Bahia: JusPodivm, 2015, p. 920.
6. RAMOS, João Gualberto Garcez. A tutela de urgência no processo penal brasileiro. Belo Horizonte: Del Rey, 1998, p. 260
7. BARBOSA, Ruchester Marreiros, Revista Síntese Direito Penal e Processual Penal, Porto Alegre: Síntese, v.13, nº 74, jun./jul. 2012, p. 26 a 28. Sugerimos no referido artigo científico a alteração do nome Delegado de Polícia para Autoridade de Garantias, por não mais subsistiram as razões do termo empregado hoje, apesar de ser ainda empregada não só pelo projeto do novo código de processo penal, como também pelo art. art. 144, § 4º, da CRFB/88.
8. Corte IDH. Caso Vélez Loor Vs. Panamá. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 23 de noviembre de 2010 Serie C N.218, par. 108, disponível: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_218_esp2.pdf>, acesso em 08 de agosto de 2014.
9. FERRAZ JUNIOR, Tercio Sampaio. Sigilo de Dados: o Direito à Privacidade e os Limites à Função Fiscalizadora do Estado. In Sigilo Fiscal e Bancário. PIZOLIO, Reinaldo e GAVALDÃO JR, Jayr Viégas (coord.). São Paulo. Quartier Latin. 2005. p. 28/29.
10. BARBOSA, Ruchester Marreiros; et al. Cood. Geral: MELLO, Cleyson de Moraes e GÓES, Guilherme Sandoval. In Poder Geral de Natureza Administrativo-cautelar pelo Delegado de Polícia e sua Função Inerente ao Sistema Acusatório Garantista. Juiz de Fora: Editar, 2015, p. 252.
11. BARBOSA, Ruchester Marreiros. Sobre a natureza decisória de determinados atos praticados pelo Delegado de Polícia citamos trabalho científico publicado na Revista Síntese Direito Penal e Processual Penal, Porto Alegre: Síntese, v.13, nº 74, jun./jul. 2012, p. 10 a 17.
12. Pedido de Reconsideração no MS 23.576/DF, Rel. Min. Celso de Mello, em 14/12/99 e STF, Rel. Min. Celso de Mello, MS nº 23.851-8/DF, Pleno, Ementário nº 2074-2, DJ de 2074-2, DJ de 21/06/2002.
13. HC 131.836/RJ, Rel. Min. Jorge Mussi, em 04/11/2012, p. no DJe em 06/04/2011 e cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270
14. HC 0002029-54.2012.404.0000/RS – 7ª T. – Rel. Juiz Fed. José Paulo Baltazar Junior – DJe 31.05.2012, p. 563
15. Luciano Oliveira, in: Segurança: um direito humano para ser levado a sério. – Anuário dos Cursos de Pós-Graduação em Direito n. 11 – UFPE. Apud STRECK, Lênio Luiz, em artigo O Princípio Da Proibição De Proteção Deficiente (Untermassverbot) E O Cabimento De Mandado De Segurança Em Matéria Criminal: Superando O Ideário Liberal-Individualista-Clássico. disponível em < http://www.leniostreck.com.br/site/wp-content/uploads/2011/10/1.pdf>, acesso em 29/04/2014.

16. BARBOSA, Ruchester Marreiros. Revista Síntese de Direito Penal e Processual Penal, Porto Alegre: Síntese, v.13, nº 74, jun./jul. 2012, p. 26 a 28.

17. Recentemente, em 15 de abril de 2014 foi divulgado no site do Centro de Estudos de Direito Penal e Processual Penal Latino-americano, na Alemanha, a conclusão sobre a "investigação policial no Brasil", com participação de juristas protagonistas da persecução criminal, perito, Delegado de Polícia, Advogados, Juízes, Desembargadores, Promotores e Procuradores de Justiça. Dentre os itens conclusivos a despeito das mudanças positivas que devem ocorrer na investigação criminal é o 7 - observância escrupulosa do devido processo legal no âmbito da investigação criminal, dentre outros, com a previsão legal de prazo máximo de duração da prisão e demais medidas cautelares. Ou seja, uma duração razoável da investigação criminal.

18. RE 418.376/STF, "Quanto à proibição de proteção deficiente, a doutrina vem apontando para uma espécie de garantismo positivo, ao contrário do garantismo negativo (que se consubstancia na proteção contra os excessos do Estado) já consagrado pelo princípio da proporcionalidade. A proibição de proteção deficiente adquire importância na aplicação dos direitos fundamentais de proteção, ou seja, na perspectiva do dever de proteção, que se consubstancia naqueles casos em que o Estado não pode abrir mão da proteção do direito penal para garantir a proteção de um direito fundamental."

19. Art. 23, VII, 31§4º e art. 33, III, todos da Lei 12.527/11; art. 17-B da Lei 12.683/12; O art 2º, §2º da recente lei 12.830/2013; artigo 15 da, ainda mais recente, lei 12.850/13.

20. HC 131.836/RJ julgado em 04/11/2012 frise-se que o inciso XII do artigo 5º da Constituição Federal assegura o sigilo das comunicações telefônicas, nas quais, por óbvio, não se inserem os dados cadastrais do titular de linha de telefone celular.

21. HC 103425 / AM, julgado em 26/06/2012; (....)Desnecessidade de prévia ordem judicial e do assentimento do usuário temporário do computador quando, cumulativamente, o acesso pela investigação não envolve o próprio conteúdo da comunicação(....)."; RE 418416/SC A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270; Julgado em 2006.

22. O legislador deixou bem clara a submissão dos provedores de conexão que estão submetidos a ordem ou determinação do delegado de polícia, não se tratando se um simples requerimento na qual os mesmos poderão se recusar a fornecer, sob pena de incorrerem em crime de desobediência ou dependendo do caso, crime previsto no art. 21 da lei 12.850/13.

23. O TCP/IP (também chamado de pilha de protocolos TCP/IP) é um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Internet, ou ainda, protocolo de interconexão) disponível em < http://pt.wikipedia.org/wiki/TCP/IP>, acesso em 29/04/2014.

24. CASTRO, Henrique Hoffmann Monteiro de. Requisição de dados é imprescindível na busca do delegado pela verdade. Revista **Consultor Jurídico**, fev. 2016. Disponível: <http://www.conjur.com.br/2016-fev-02/academia-policia-poder-requisitorio-delegado-essencial-busca-verdade#sdfootnote15anc>, acesso em 20 de março de 2016.

Rettec
artes
gráficas
e editora

Rua Xavier Curado, 388 • Ipiranga - SP • 04210
Tel.: (11) 2063 7000 • Fax: (11) 2061 8709
rettec@rettec.com.br • www.rettec.com.br