MINISTÉRIO PÚBLICO FEDERAL
2ª CÂMARA DE COORDENAÇÃO E REVISÃO

CRIMES CIBERNÉTICOS

COLETÂNEA DE ARTIGOS

VOL. 3

MPF
Ministério Público Federal

CRIMES CIBERNÉTICOS

COLETÂNEA DE ARTIGOS

Volume.3

MINISTÉRIO PÚBLICO FEDERAL
2ª CÂMARA DE COORDENAÇÃO E REVISÃO

CRIMES CIBERNÉTICOS

COLETÂNEA DE ARTIGOS
Volume.3

Brasília - MPF
2018

Disponível também em:
<http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes>

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

B823c Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 2.

Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018.

275 p. – (Coletânea de artigos ; v. 3)

Disponível também em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes>

ISBN 978-85-85257-32-3

1. Crime por computador. 2. Pedofilia. 3. Moeda digital. 4. Racismo. 5. Espionagem eletrônica. I. Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. II. Título.

CDDir 341.532

Elaborado por Juliana de Araújo Freitas Leão – CRB1/2596

Coordenação e Organização
Fernanda Teixeira Souza Domingos
Jaqueline Ana Buffon
Luiza Cristina Fonseca Frischeisen
Neide Cardoso de Oliveira
Priscila Costa Schreiner Roder

Planejamento visual, revisão e diagramação
Secretaria de Comunicação Social

Normalização Bibliográfica
Coordenadoria de Biblioteca e Pesquisa (Cobip)

Procuradoria-Geral da República
SAF Sul, Quadra 4, Conjunto C
Fone (61) 3105-5100
70050-900 - Brasília - DF

www.mpf.mp.br

SUMÁRIO

APRESENTAÇÃO

Esta Coletânea de artigos sobre Crimes Cibernéticos é a terceira publicada pela 2ª Câmara de Coordenação e Revisão, e o tema, eleito como prioritário, reflete a importância no combate à criminalidade cibernética na sociedade contemporânea. A desejada universalização do uso da internet no Brasil e no mundo, infelizmente, também ocasiona efeitos colaterais. Esses efeitos são a prática dos delitos cibernéticos ou daqueles que, simplesmente, usam a internet como meio para a prática dos mais diversos crimes. E, no mundo todo, os órgãos de *Law Enforcement* e agentes públicos vêm se capacitando para o enfrentamento desse grande e urgente problema global.

Os artigos selecionados, em uma proposta multidisciplinar, foram escritos não só por membros e servidores do MPF, mas também por profissionais diversos, como os de fora do meio jurídico, e refletem uma discussão abrangente do tema. Cabe ressaltar que as posições expostas nesses artigos não significam o posicionamento institucional do MPF.

A Coletânea é composta por alguns artigos que possuem uma conotação mais técnica, e outros tratam de questões práticas, como os que versam sobre prova eletrônica e agente infiltrado, e que se pretende possam servir de consulta para os membros no seu dia a dia. Alguns inovam com propostas de alteração da legislação, outros trazem tema tão debatido na nossa sociedade atual, como o racismo, e sobre diversos vieses. A almejada prevenção aos crimes cibernéticos e sua adoção como política pública não poderia ser esquecida. Por fim, a importante e necessária discussão e implementação da Justiça Restaurativa.

A 2ª CCR e os membros que compõem o Grupo de Apoio sobre Criminalidade Cibernética agradecem todas as contribuições dos diversos profissionais que se dispuseram a colaborar com a formação da Coletânea, e esperam que os membros e servidores do MPF possam usufruir desse trabalho no combate aos crimes cibernéticos.

Neide M. C. Cardoso de Oliveira
Procuradora Regional da República
Coordenadora do Grupo de Apoio sobre Criminalidade Cibernética da 2ª CCR

1 COMBATE À PORNOGRAFIA INFANTOJUVENIL COM APERFEIÇOAMENTOS NA IDENTIFICAÇÃO DE SUSPEITOS E NA DETECÇÃO DE ARQUIVOS DE INTERESSE

Felipe B. Caiado[1]
Marcelo Caiado[2]

Resumo: Nos últimos anos, a tecnologia evoluiu em uma escala inigualável, não apenas melhorando os padrões de vida mundiais, mas também facilitando a criação de um dos crimes mais infames da sociedade moderna, a pornografia infantil, e também facilitando o acesso a ele e a distribuição de material a este relacionado. Desafortunadamente, as forças da lei não se atualizaram e estão aquém desses avanços, assim ficaram sem as ferramentas necessárias para perseguir esses crimes. Nesses novos desafios, hoje suspeitos de pornografia infantil são achados de diversas formas, e a quantidade de conteúdo e tráfico de PI (pornografia infantil) apenas cresce, deixando cada vez mais vítimas. Para então combater tal problema, é necessário que mais recursos sejam investidos e formas mais eficientes de investigação sejam implementadas, com uma integração de pesquisas e de técnicas, por parte da indústria, da academia e das forças da lei. Somente com uma automatização da detecção de novos arquivos de PI, os quais ainda não tenham sido categorizados em bibliotecas de hash pelas forças da lei, é que poderemos oferecer um futuro mais seguro para as crianças, em que as ocorrências de abuso sexual e seus danos resultantes são consideravelmente diminuídos e os seus criminosos hediondos devidamente encarcerados.

Palavras-chave: Direito Penal. Internet. Evidência. Pornografia Infantojuvenil. Perícia Computacional. Crimes cibernéticos

Abstract: *In the last years technology has evolved on an incomparable scale, not only improving living standards but also facilitating the creation, distribution and access to one of modern society's most infamous crimes, child pornography. Unfortunately, law enforcement agencies are not up to date and stayed behind these advances, so they don´t have the appropriate tools to prosecute these crimes. With these new challenges, child pornography suspects are found today in a variety of ways, and the amount of CP (child pornography) content and trafficking only grows, leaving more and more victims. In order to combat such a problem, more investments are necessary and more efficient forms of research be implemented, with integration of research and techniques by industry, universities and law enforcement. Only automating the detection of new CP files, which have not yet been categorized into hash libraries by law enforcement, we can offer a safer fu-*

1 Graduando em Computer Science pela University of British Columbia, Canadá.

2 Mestre em Ciência da Computação pela Universidade de Brasília, especialista em Gestão Pública pela FGV e perito em Tecnologia da Informação e Comunicação do MPF.

ture for children, where the occurrences of sexual abuse and its resulting damage are considerably diminished and their heinous criminals are imprisoned.

Keywords: *Criminal Law. Internet. Evidence. Child Pornography. Computer Forensics. Cyber Crimes.*

1 Introdução

No mundo moderno, a Tecnologia da Informação e Comunicação (TIC) está cada vez mais presente na rotina das empresas e da maioria da população urbana. Acerca do vertiginoso aumento da importância das TIC, Porter e Millar (1985) definem a sua relevância na cadeia de valor e apontam que elas geram novos negócios inteiros, muitas vezes de dentro das operações existentes na própria empresa, além de criar vantagens competitivas e mudar a estrutura da indústria, alterando as regras de competição. Tais características foram em grande parte as responsáveis pela propagação das novas tecnologias.

Com tal disseminação de uso das TIC, os recursos eletrônicos não estão sendo apenas empregados pelas empresas, mas também sendo mais utilizados na prática de diversos crimes, como estelionato, furto mediante fraude e pornografia infantojuvenil, entre outros. Não é nenhuma novidade que os computadores, smartphones, tablets, GPS, câmeras digitais, e outros dispositivos eletrônicos são utilizados e estão envolvidos em crimes e ações ilegais. Surge então um diferente modelo, que é a necessidade de lidar adequadamente com a análise e as investigações que envolvam o uso desses novos recursos tecnológicos utilizados na prática criminosa.

Com esse novo paradigma, é notável que, nos últimos anos, a tecnologia evoluiu em uma escala inigualável, não apenas melhorando os padrões de vida mundiais, mas também facilitando a consecução de diversas modalidades criminosas, entre elas a criação de um dos crimes mais infames da sociedade moderna: a pornografia infantojuvenil, e facilitando também o acesso a ele e a distribuição de material a este relacionado.

Tais crimes tomaram grandes proporções com o advento da sociedade digital e apresentam enormes desafios em seu combate, entre os quais se destacam as devidas identificação e persecução penal, bastante comprometidas pelo conceito de mundo virtual, em que as demarcações de um território em função dos seus recursos físicos e do raio de abrangência de determinada cultura serem rompidos, conforme definido por Pinheiro (2010).

Cumpre observar que a definição de crime inexiste em nosso atual Código Penal, sendo eminentemente doutrinária. Assim, de acordo com Greco (2014), vários doutrinadores, como Assis Toledo e Luiz Regis Prado, consideram que "para que se possa falar em crime é preciso que o agente tenha praticado uma ação típica, ilícita e culpável". Isso implica em que determinadas imagens e vídeos podem ser considerados de pornografia infantojuvenil em uma jurisdição, mas não em outra, como é o caso de quadrinhos que simulam crianças e adolescentes em situações eróticas e pornográficas.

Outrossim, para Welch (2007, p. 2781-2782) é notório que as mesmas novas tecnologias que "permitiram o avanço e a automação de processos de negócio, também abriram as portas para muitas novas formas de uso indevido de computadores", sendo que aqui devemos incluir as diversas modalidades de crimes cibernéticos. Ele ainda ressalta a importância da conscientização e da devida preparação para enfrentar uma "miríade de questões tecnológicas e jurídicas que afetam os sistemas e os usuários".

Assim, faz-se importante que as forças da lei estejam devidamente preparadas para auxiliar na apuração dos crimes cometidos por meio da internet ou de dispositivos inteligentes conectados em rede, bem como no uso dos vestígios tecnológicos para a elucidação de crimes e dos procedimentos para preservação da evidência digital. Inclusive, deve-se lembrar que a internet é intrinsecamente vulnerável, pois foi concebida utilizando-se de protocolos que não fornecem uma segurança adequada (MIT SLOAN MANAGEMENT REVIEW, 2007).

Conforme nos ilustram Farmer e Venema (2007), a perícia computacional é, basicamente, a preservação, aquisição, análise, descoberta, documentação e apresentação de evidência presente em meio digital (equipamentos computacionais e mídias de armazenamento). O intuito é de comprovar a existência de determinados eventos que possam ter levado à consecução de crimes ou atividades não autorizadas, ou que possam provar que o evento não foi realizado conforme pode estar sendo imputado. Ademais, a forense computacional requer a combinação de técnicas de investigação com as exigências das leis e normas de cada país, organização e empresa.

2 Legislação e investigação

Conforme bem apontado por Walls (2011), pesquisadores de segurança digital têm um elevado potencial de fazer mudanças drásticas para as forenses digitais, o que pode permitir melhor eficácia nas investigações. Contudo, eles primeiramente precisam en-

tender as limitações que afetam o contexto de investigações e as diferenças que este possui de modelos de segurança.

Um outro problema também advém da abordagem de serem observadas pesquisas de pouco impacto, pelo fato de os pesquisadores não possuírem contato direto com a indústria. Desafortunadamente, pesquisas que fazem uma abordagem realística para melhorar a situação são raras, sendo que a maioria fica na parte teórica e com impactos mínimos para o mundo prático da segurança.

Além disso, a maioria das políticas ou leis se preocupam também com as motivações existentes por detrás de uma infração, o que normalmente pode ser demonstrado por meio de uma coleta de dados e de evidências. Poderão inclusive haver restrições quanto ao conteúdo coletado, cujo procedimento deverá sempre observar o devido processo legal e a manutenção da cadeia de custódia (WALLS, 2011).

2.1 Ordenamento jurídico brasileiro

O atual ordenamento jurídico brasileiro passou por algumas significativas mudanças nos últimos anos em função da jurisprudência relacionada ao julgamento de crimes cibernéticos, e aqui especialmente se destaca a aprovação do novo Marco Civil da Internet (MCI) brasileira, sancionado em 23 de abril de 2014, pela Lei nº 12.965/2014.

Anunciado por alguns como tendo criado um grande avanço na área de neutralidade da rede, que exige tratamento igualitário a todo conteúdo que trafega na internet, admitidas algumas exceções, o MCI de fato apresentou alguns avanços, diversos dos quais ainda pendem de devida regulamentação. Contudo, foi duramente criticado por peritos em informática e advogados especialistas em direito digital, em diversos aspectos tais como a guarda de registros (*logs*) de acesso e privacidade de usuários e liberdade de expressão.

Nesse sentido, na subseção I da mencionada lei é estabelecido um período muito exíguo em relação ao prazo mínimo que os provedores de conexão à internet (por exemplo: Net, GVT, Oi etc.) e os provedores de aplicação de internet (por exemplo: Google, Facebook, Uol etc.) deverão manter os seus registros de acessos:

> Da Guarda de Registros de Conexão
> Art. 13. *Na provisão de conexão à Internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano*, nos termos do regulamento. [...]
> Art. 15. *O provedor de aplicações de Internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de Internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses*, nos termos do regulamento.

Os *logs* oferecem informações essenciais para iniciar adequadamente uma investigação, a qual fica bastante comprometida sem o fornecimento devido de dados que possibilitem a identificação de qual usuário estava vinculado a um endereço IP identificado como origem de um suposto crime.

Para piorar ainda mais esse exíguo prazo de armazenamento definido, o Decreto nº 8.771, de 11 de maio de 2016, que regulamentou a Lei nº 12.965/2014, definiu em seu art. 11 que "o provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados". Isso é praticamente um convite aos criminosos para utilizarem redes *WiFi* abertas para o cometimento de delitos.

Ainda em relação ao Decreto nº 8.771/2016, um grande equívoco foi gerado ao definir que os provedores possuem a obrigação de apagarem os dados de logs após o período previsto em lei, conforme estipula o parágrafo 2º do art. 13:

> § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, *os quais deverão ser excluídos:*
> I – tão logo atingida a finalidade de seu uso; ou
> II – *se encerrado o prazo determinado por obrigação legal.*

Não obstante, a Lei nº 12.737/2012 (conhecida na mídia como Lei Carolina Dieckmann, que havia sido vítima recente de uma divulgação indevida de fotos íntimas, pouco tempo antes da votação da lei) já havia finalmente trazido para o ordenamento

jurídico criminal o crime de "invasão de dispositivo informático", alterando o Decreto-Lei nº 2.848, de 7 dezembro de 1940, em que foram incluídos os arts. 154-A e 154-B.

Aqui cabe a ressalva de que ainda não está pacificado nos tribunais o que é necessário que ocorra para caracterizar a violação indevida de mecanismo de segurança, conforme é definido no dispositivo legal, visto que nem sempre o usuário possui qualquer nível de segurança implementado ou que talvez seja inviável comprovar tal violação.

Um outro fato bastante significativo foi o relatório da CPI de Crimes Cibernéticos (2016), o qual ratificou a necessidade urgente de investimentos na área de perícia com a apresentação de vários projetos de lei, os quais buscam melhor tipificação para alguns crimes, além de auxiliar tanto na investigação de tais crimes como em uma melhor capacidade dos entes públicos para lidar com esse problema. Os investimentos nessa capacidade serão auxiliados com recursos oriundos do Fistel, conforme proposto no projeto de lei que visa à alteração da Lei nº 5.070, de 7 de julho 1966.

Entre as justificativas apresentadas nos projetos de lei mencionados no relatório da CPI de Crimes Cibernéticos (2016), algumas constatam claramente o fato de que é essencial uma melhor tipificação de alguns crimes, quando dizem que: "conforme apurado por esta Comissão Parlamentar de Inquérito, a legislação brasileira ainda é muito incipiente no que diz respeito aos crimes cibernéticos".

Isso também observado em outras duas distintas justificativas, que comentam a aprovação da Lei nº 12.737/2012, e as quais afirmam que:

> em que pese essa disposição legal, os trabalhos da Comissão Parlamentar de Inquérito dos Crimes Cibernéticos evidenciaram a falta de estrutura dos Estados no combate a esses tipos de crimes" e também "que não há dúvida que a legislação precisa ser aprimorada.

Essa questão de legislação adequada é muito bem ilustrada por Capanema (2009), o qual afirma que o importante em uma solução legislativa efetiva "não é impor um regime autoritário na internet, mas mostrar que, mesmo no mundo dos *bits e bytes*, deve haver uma presença efetiva da Lei, da Ordem e da Justiça".

Além disso, legislações anteriores ao advento da internet também são utilizadas na tipificação de crimes, pois a conduta já era prevista como criminosa, como é o caso de,

por exemplo, criar uma comunidade para se expressar contra grupos étnicos (este sendo inclusive um crime investigado pelo MPF), segundo dispõe o art. 20, da Lei nº 7.716/1989:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei nº 9.459, de 15 de maio de 1997)
> Pena: reclusão de um a três anos e multa. (Redação dada pela Lei nº 9.459, de 15 de maio de1997).

2.2 A atividade pericial

Observando a questão jurídica pela ótica de quem trabalha na investigação analisando alguma evidência, é importante mencionar o Código de Processo Civil (Lei nº 13.105/2015), em especial os arts. 156 a 158:

> Art. 156. *O juiz será assistido por perito quando a prova do fato depender de conhecimento técnico ou científico.*
> § 1º Os peritos serão nomeados entre os profissionais legalmente habilitados e os órgãos técnicos ou científicos devidamente inscritos em cadastro mantido pelo tribunal ao qual o juiz está vinculado. [...]
> Art. 157. O perito tem o dever de cumprir o ofício no prazo que lhe designar o juiz, empregando toda sua diligência, podendo escusar-se do encargo alegando motivo legítimo. [...]
> Art. 158. *O perito que, por dolo ou culpa, prestar informações inverídicas responderá pelos prejuízos que causar à parte* e ficará inabilitado para atuar em outras perícias no prazo de 2 (dois) a 5 (cinco) anos, independentemente das demais sanções previstas em lei, devendo o juiz comunicar o fato ao respectivo órgão de classe para adoção das medidas que entender cabíveis.

Assim, constata-se que o trabalho pericial é bastante especializado e além de demandar profundos conhecimentos técnicos e necessária constante atualização traz consigo uma enorme responsabilidade ao profissional que o executa, o qual responde juridicamente pelo resultado da perícia realizada.

Ainda, não se deve esquecer também da Seção X do mencionado CPC, e em especial do art. 465 que estipula prazos e define a possibilidade de inquirição somente pelo juiz competente:

> Art. 465. O juiz nomeará perito especializado no objeto da perícia e fixará de imediato o prazo para a entrega do laudo.
> § 1º Incumbe às partes, dentro de 15 (quinze) dias contados da intimação do despacho de nomeação do perito:
> I – arguir o impedimento ou a suspeição do perito, se for o caso;
> II – indicar assistente técnico;
> III – apresentar quesitos.
> § 2º Ciente da nomeação, o perito apresentará em 5 (cinco) dias:
> I – proposta de honorários;
> II – currículo, com comprovação de especialização;
> III – contatos profissionais, em especial o endereço eletrônico, para onde serão dirigidas as intimações pessoais.
> § 3º As partes serão intimadas da proposta de honorários para, querendo, manifestar-se no prazo comum de 5 (cinco) dias, após o que o juiz arbitrará o valor, intimando-se as partes para os fins do art. 95. […]
> § 5º Quando a perícia for inconclusiva ou deficiente, o juiz poderá reduzir a remuneração inicialmente arbitrada para o trabalho.

2.3 Crimes cibernéticos

Cumpre observar que são essencialmente duas as categorias utilizadas para categorização dos chamados crimes cibernéticos: a dos crimes digitais próprios (ou puros) e a dos crimes digitais impróprios (ou mistos), conforme bem indicado pelo Prof. Marcelo Crespo (2015):

> Crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (*hacking*), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas; e
> Crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio. (CRESPO, 2015)

A seguir são ilustradas algumas formas de crimes cibernéticos mais comuns, com as suas respectivas tipificações:

Tabela 1: Algumas tipificações de formas de crimes cibernéticos comuns

Crime	Tipificação
Estelionato e furto eletrônicos (fraudes bancárias)	arts. 155, §§ 3º e 4º, II, e 171 do CP
Invasão de dispositivo informático e furto de dados	art. 154- A do CP
Falsificação e supressão de dados	arts. 155, 297, 298, 299, 313-A, 313-B do CP
Armazenamento; produção; troca; publicação de vídeos e imagens contendo pornografia infantojuvenil	arts. 241 e 241-A, do ECA (Lei nº 8.069/1990)
Assédio e aliciamento de crianças	art. 241-D, do ECA (Lei nº 8.069/1990)
Ameaça	art. 147 do CP
Cyberbullying (veiculação de ofensas em blogs e comunidades virtuais)	arts. 138, 139, 140 do CP
Interrupção de serviço	art. 266, parágrafo 1º, do CP
Incitação e apologia de crime	arts. 286 e 287 do CP
Prática ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	art. 20 da Lei nº 7.716/1989
Crimes contra a propriedade intelectual artística e de programa de computador	art. 184 do CP e Lei nº 9.609/1998
Venda ilegal de medicamentos	art. 273 CP

Observa-se também que a velocidade vivenciada na mudança dos hábitos da população, em função dos usos de novas tecnologias, tem trazido consigo um enorme desafio na adaptação e definição de regras de boas condutas, as quais muitas vezes são indevidamente utilizadas e exploradas por mentes criminosas. No mesmo sentido, a internet possibilitou novas formas de interação social, as quais também facilitaram a aplicação de golpes e o cometimento de crimes.

De resto, Eleutério e Machado (2011) ratificam o entendimento de que, apesar da utilização de computadores não ser nada novo, de fato a legislação brasileira não está preparada e precisa ser revista, de forma a possibilitar a adequada tipificação das diversas modalidades de crimes cibernéticos.

2.4 Investigação de crimes de pornografia infantojuvenil

Tradicionalmente as forças da lei instalam programas de investigação em servidores que monitoram e informam cada vez que um arquivo suspeito é armazenado ou trafegado. Tais programas são baseados em bibliotecas de *hash* (hashes são assinaturas de um documento que o deixam distinguíveis de qualquer outro na internet) e como tal nem sempre são efetivos, pois dependem da prévia catalogação de uma imagem de pornografia infantojuvenil. Essa inefetividade ocorre nas situações em que novas imagens não são identificadas pelo programa, por inexistir o respectivo *hash* catalogado na biblioteca.

É essencial, então, que as forças da lei busquem alternativas viáveis e que possam ser rapidamente implementadas, tanto em termos de legislação nacional e quanto em termos de uma eficaz cooperação internacional, utilizando-se de ferramentas automatizadas que permitam a localização dos proprietários desses arquivos e a consequente persecução penal desses criminosos que os armazenam ou distribuem.

No Brasil, o problema da pornografia infantojuvenil é muito sério e precisa ser adequadamente tratado. Ainda que seja difícil definir o escopo exato desse problema, é certo que esse infortúnio aumentou significativamente com o estabelecimento da internet, sendo que, no ano de 2009, era apontado como um dos crimes mais comuns cometidos na internet (PINHEIRO, 2009).

Não obstante, cumpre destacar que o termo pedofilia representa uma doença (WHO, 1993), desordem mental ou desvio sexual caracterizado pela atração por crianças ou adolescentes, e portanto não deve ser confundido com pornografia infantojuvenil. Desse modo, conforme muito bem retratado por Silva (2017) "não existe crime de pedofilia, como é usual assim entender-se popularmente", que também evidencia que "o crime de pornografia infantojuvenil nem sempre é praticado por pedófilos", tendo em vista a busca de lucro financeiro com essa atividade por organizações criminosas.

Destarte, o pedófilo é a pessoa que apresenta a doença pedofilia, enquanto a pornografia infantojuvenil é encontrada em arquivos de imagens e vídeos (ELEUTÉRIO; MACHADO, 2011). A tipificação dos crimes de produção, reprodução, posse ou compartilhamento desses tipos de arquivos é definida nos arts. 240 e 241 do Estatuto da Criança e do Adolescente – Lei nº 8.069/1990, alterados pela Lei nº 11.829/2008.

2.4.1 Compartilhamento de arquivos de pornografia infantojuvenil

A divulgação de arquivos de pornografia infantojuvenil ocorre muito frequentemente via mensagens eletrônicas e em conexões que usam compartilhamento P2P, como eMule, Gnutella e Ares Galaxy (LIBERATORE; LEVINE; SHIELDS, 2010). Nesse caso, essas ferramentas de compartilhamento eliminaram a necessidade do uso de um servidor, fazendo com que os computadores se comuniquem via nós interconectados, em que a comunicação entre duas máquinas é direta e todos os nós da rede têm responsabilidades equivalentes. Desse modo, a estratégia de analisar e inspecionar os arquivos hospedados em um servidor tornou-se inefetiva.

Ademais, com a utilização de conexões P2P em que o servidor não é mais necessário, novas ferramentas de investigação foram desenvolvidas, como o programa CPS (*Child Protection System*), o qual realiza uma identificação automática e é utilizado em 77 países (CHILD RESCUE COALTION, 2018). Contudo, ainda faltam soluções mais avançadas de buscas em redes P2P, especialmente ao buscar arquivos que não sejam somente aqueles já categorizados. Essa atualização é bastante relevante, tendo em vista que os predadores podem alterar os arquivos de forma que não possuam uma correspondência com bibliotecas de *hash*.

Com esses novos desafios, atualmente, os suspeitos de pornografia infantojuvenil são identificados de diversas formas, as quais além da detecção automática podem incluir investigadores infiltrados que estabelecem um contato com os criminosos no mundo real ou no virtual. Uma vez que um suspeito seja determinado, um mandado pode ser obtido para que os seus computadores e dispositivos eletrônicos sejam investigados e analisados.

A experiência prática mostra que a identificação da existência de imagens de crianças em arquivos de pornografia infantojuvenil (PI) é fácil, enquanto a de adolescentes é mais complexa, tendo em vista um possível desenvolvimento mais rápido do que usual. Isso ocorre com mais frequência em adolescentes do sexo feminino, que podem ser confundidas com pessoas adultas, situação esta amplificada nos casos de arquivos com menor resolução gráfica.

Enquanto isso, a quantidade de conteúdo e tráfico de PI apenas cresce, deixando cada vez mais vítimas. Para combater tal problema, as forças da lei lutam para aumentar os recursos investidos na persecução penal desses predadores, o que nem sempre é possível. Contudo, mesmo havendo esse aumento de recursos, o qual se demonstra in-

suficiente, as forças da lei continuam, na maioria dos casos, dependentes dos métodos tradicionais para investigar tais crimes.

Assim, se esses recursos fossem investidos de uma forma mais eficiente, aportariam mais frutos. Um bom exemplo disso seria a criação e o uso de soluções que se utilizem de múltiplas técnicas, como o caso do *multi modal feature fusion* (MMFF). Esse método consiste em pegar uma combinação de programas que automatizam a investigação e diminuem o número de arquivos necessários para especialistas forenses examinarem, fazendo com que haja um número considerável menor de arquivos a serem analisados de forma mecânica pelo investigador.

2.4.2 Combinando soluções diferentes para uma abordagem efetiva

A técnica de MMFF usa uma combinação de métodos disponíveis como detecção de pele, o conceito de *visual words* e de SentiBank, que respectivamente detectam imagens de pele, olham por vocabulário relacionado à PI e categorizam alguns sentimentos relacionados a crianças sendo exploradas que aparecem na imagem. Sentimentos como medo e raiva são mais comumente encontrados nessas imagens, sendo que, em contraste, esses sentimentos são raramente identificados em outros tipos de pornografia. Dessa forma, podemos achar não apenas arquivos de PI já conhecidos, mas também outros novos.

Combater o abuso sexual infantojuvenil não é somente uma questão de categorizar um arquivo como PI, mas também de procurar em lugares onde esses arquivos estão potencialmente gravados. Um estudo de 2013, que analisava tráfego de PI em conexões P2P (HURLEY et al., 2013) identificou 1,8 milhões de nós de eMule (nesse caso instâncias do programa) que continham PI, sendo vários desses arquivos com as mesmas imagens de PI que já haviam sido identificadas e tiveram o seu *hash* categorizado por agências de forças da lei.

Nesse método, encontrar arquivos de PI pelo *hash* e pelo nome do arquivo tem uma alta relevância, mas estes só funcionam em material já identificado. Se um arquivo for modificado, mesmo que um mínimo bit, o que é uma mudança imperceptível para um humano, este não será mais identificado pela biblioteca de *hashes*. Da mesma forma, não se pode assumir que todos arquivos de PI já foram categorizados em um mundo onde só há um aumento no tráfego ilegal desse material. Então, torna-se crítico analisar automaticamente todos os arquivos como possíveis arquivos de PI e não apenas os que foram previamente categorizados.

Outrossim, Hurley et al. (2013) demonstram que somente 29.458 arquivos de interesse (do inglês, *files of interest* – FOI) foram encontrados em mais de 1,8 milhões de nós eMule. Considerando a imensa quantidade desses nós encontrados e a ínfima quantidade de arquivos de interesse identificados, pode-se inferir que imagens e vídeos de PI foram alterados, restando impossível serem pareados com bibliotecas de *hash* de PI, e assim complicando o trabalho de investigadores das forças da lei.

Logo, mesmo que utilizando os métodos antigos sejam revelados vários arquivos de PI, ainda existe a necessidade de introduzir novos mecanismos de buscas automatizados para continuar a par da incessante criação de PI. Consequentemente, com esse novo método, os arquivos novos também serão analisados, o que se torna crucial, já que vários deles contêm PI que não foi previamente catalogada em biblioteca de *hashes*. Em contraste com o velho processo de analisar mecanicamente cada um dos arquivos, esse processo novo deixará as investigações mais eficientes e consideravelmente diminuirá o tempo médio de resolução de casos.

Da mesma forma, já foi demonstrado que protocolos de busca particulares isolados, como os que detectam quantidade de pele em uma imagem, acabam por ter falsos positivos, conforme mostrado pelos autores de MMFF (SCHULZE et al., 2014). A detecção de pele então vem a ser eficiente para identificar qualquer tipo de pornografia, que é mais frequentemente a pornografia adulta, mas não PI, já que o número de arquivos de PI é mínimo comparado com aqueles de pornografia legal na internet, logo tais programas classificariam qualquer arquivo pornográfico como um arquivo de PI.

Um outro complicador na investigação de PI envolve as análises de dados coletados em que há imagens artificiais criadas por computadores, as quais parecem uma criança real sendo abusada por um predador. Isso resulta em taxas maiores de falsos positivos para as ferramentas MMFF, em função do fato de que nem as ferramentas existentes e nem os mais bem treinados humanos podem distingui-las da realidade com a tecnologia disponível atualmente (HOLMES, 2016).

Logo, uma ferramenta corretamente desenvolvida deve considerar esses desafios, inclusive para impedir a perseguição incorreta de desenhistas e cartunistas, os quais criam esse conteúdo em países onde é legal produzir imagens fictícias de crianças sendo sexualmente exploradas. Essas ferramentas tornariam o trabalho do investigador mais fácil, diminuindo o número de falsos positivos e, por conseguinte, o número de arquivos a serem analisados.

3 Conclusão

Podemos concluir, então, que o desenvolvimento da internet resultou em um avanço simultâneo no número de crimes por meio dessa rede mundial de computadores ou cometidos por meio de outra tecnologia computacional (HARVARD LAW REVIEW, 2009), como é o caso do compartilhamento de pornografia infantojuvenil (EUROPOL, 2017). Dessa forma, novas tecnologias também foram e devem continuar a ser pesquisadas para automatizar a procura e a persecução penal de predadores na internet, além de uma melhoria nas ferramentas atualmente disponíveis para agências de forças de lei, o que pode ser obtido com uma integração de pesquisas.

Além disso, o compartilhamento de arquivos com conteúdos de pornografia infantojuvenil, assim como outras formas de criminalidade, como venda de bases de dados governamentais e cursos para fraudes bancárias, também vêm sendo realizados intensamente por novos meios. Destaca-se atualmente a utilização do aplicativo The Onion Router (TOR), o qual permite a navegação anônima na chamada DarkWeb, que é uma rede de páginas web não indexadas, mais privativa e anônima do que a DeepWeb. Algumas técnicas específicas, como a inserção de vários nós na rede TOR para comprometer o anonimato e a exploração de vulnerabilidades *zero-day*, têm sido utilizadas para a investigação pelas forças da lei nesses casos (SHIMABUKURO; SILVA, 2017).

Finalmente, é importante que os governos, as universidades e as indústrias entendam as mudanças no *modus operandi* dessas atividades criminais, trabalhando continuamente em conjunto para desenvolver novas tecnologias e soluções de investigação, que melhorarão a performance da tecnologia disponível para encontrar material de pornografia infantojuvenil de uma maneira forense e com um correto estabelecimento da cadeia de custódia. Somente assim poderemos vislumbrar um futuro mais seguro para as crianças, em que todas as ocorrências de abuso sexual e seus danos resultantes.

Referências

CAPANEMA, Walter Aranha. **O Spam e as Pragas Digitais**: uma visão jurídico-tecnológica. São Paulo: Ltr, 2009.

CHILD RESCUE COALTION. **The Solution**. Disponível em: <https://childrescuecoalition.org/the-solution/>. Acesso em: 15 jan. 2018.

CRESPO, Marcelo. **Crimes Digitais**: do que estamos falando?. Disponível em: <http://canalcienciascriminais.com.br/artigo/crimes-digitais-do-que-estamos-falando/>. Acesso em: 17 set. 2017.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense**. São Paulo: Novatec, 2011.

EUROPOL. **The European Union (EU) Serious and Organized Crime Threat Assessment (SOCTA) 2017** – Crime in the age of technology. Disponível em: <https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf>. Acesso em: 15 set. 2017.

FARMER, Dan; VENEMA, Wietse. **Perícia Forense Computacional** – teoria e prática aplicada. São Paulo: Pearson, 2007.

GRECO, Rogério. **Curso de Direito Penal** – parte geral. 16. ed. Rio de Janeiro: Editora Impetus, 2014. v. I.

HARVARD LAW REVIEW. **Child Pornography, The Internet, and The Challenge of Updating Statutory Terms**. Disponível em: <http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol_122_child_ pornograph_ the_Internet.pdf>. Acesso em: 16 set. 2017.

HOLMES, O.; BANKS, M.; FARID, H. **Assessing and Improving the Identification of Computer-Generated Portraits**. ACM Trans. Appl. Percept 13, 2, Article 7 (February 2016), 12 pages. ACM 1544-3558/2016/02-ART7.

HURLEY, Ryan et al. **Measurement and Analysis of Child Pornography Trafficking on P2P Networks**. INTERNATIONAL WORLD WIDE WEB CONFERENCE 2013. May 13-17. Rio de Janeiro, Brazil. ACM 978-1-4503-2035-1/13/05.

LIBERATORE, M.; LEVINE, N.; SHIELDS, C. **Strengthening Forensic Investigations of Child Pornography on P2P Networks**. ACM CoNEXT 2010, November 30 Dec. 2010. Philadelphia, USA. ACM 1-4503-0448-1/10/11.

MIT SLOAN MANAGEMENT REVIEW. **How Secure Is the Internet?** Spring 2007 – v. 48, Issue # 3. Disponível em: <https://sloanreview.mit.edu/article/how-secure-is-the-Internet/>. Acesso em: 11 jan. 2018.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. rev., atual. e ampl. São Paulo: Saraiva, 2010.

PORTER, Michael; MILLAR, Victor. **How Information Gives You Competitive Advantage**. Disponível em: <https://hbr.org/1985/07/how-information-gives-you-competitive-advantage/ar/1>. Acesso em: 16 set. 2017.

SCHULZE, C., HENTER, D., BORTH, D., DENGEL, A. **Automatic Detection of CSA Media by Multi-modal Feature Fusion for Law Enforcement Support**. In: INTERNATIONAL CONFERENCE ON MULTIMEDIA RETRIEVAL. Glasglow, United Kingdom, 2014. ACM 353.

SHIMABUKURO, Adriana; SILVA, Melissa G. Internet, Deep Web e Dark Web. In: SILVA, Ângelo (Org.). **Crimes Cibernéticos**: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017.

SILVA, Ângelo Roberto Ilha. Pedofilia, pornografia infantojuvenil e os tipos penais previstos no Estatuto da Criança e do Adolescente. In: SILVA, Ângelo (Org.). **Crimes Cibernéticos**: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017.

WALLS, Robert J. et al. **Effective Digital Forensics Research is Investigator-Centric**. HOTSEC'11 PROCEEDINGS OF THE 6TH USENIX CONFERENCE ON HOT TOPICS IN SECURITY. San Francisco, 2011.

WELCH, Thomas. Computer Crime Investigation and Computer Forensics. In: TIPTON, Harold; KRAUSE, Micki (Org.). **Information Security Management Handbook**. 6th ed. Florida: Auerbach Publications, 2007.

WORLD HEALTH ORGANIZATION – WHO. **The ICD-10 Classification of Mental and Behavioural Disorders** – Diagnostic criteria for research. 1993. Disponível em: <http://www.who.int/classifications/icd/en/ GRNBOOK.pdf>.

CRIMES CIBERNÉTICOS

2 OBTENÇÃO DE PROVAS DIGITAIS E JURISDIÇÃO NA INTERNET[1]

Fernanda Teixeira Souza Domingos[2]
Priscila Costa Schreiner Röder[3]

Resumo: Este artigo pretende investigar a obtenção, pelos agentes de investigação no Brasil e no mundo, das provas digitais de delitos, sejam eles cibernéticos ou não, em poder de provedores de *internet*, em virtude das diferentes tecnologias que permitem o armazenamento dessas informações nos mais diferentes locais do planeta, desafiando os tradicionais conceitos de soberania, territorialidade e jurisdição.

Palavras-chave: Jurisdição. Internet. Territorialidade. Provas. Digital.

***Abstract**: This article intends to investigate possible solutions to difficulties faced, in Brazil and in the world, by law enforcement agents in obtaining cybercrime or real crime digital evidence from internet providors, considering different technologies that allow this information to be stored in many different places in the world, challenging the traditional concepts of sovereignty, territoriality and jurisdiction.*

Keywords: Jurisdiction. Internet. Territoriality. Evidence. Digital.

1 Introdução

O advento de novas tecnologias revolucionou a guarda e o armazenamento de documentos. A tecnologia digital possibilitou que quantidade imensa de informações pudesse ser trocada e passasse a ser armazenada, principalmente em virtude do incremento na comunicação e de transações na comunidade global que migraram para o mundo digital, representando facilidade e rapidez para a mobilidade de dados.

Documentos virtuais passam a fazer parte das relações sociais, tanto com referência às transações reais quanto às transações plenamente virtuais. Acompanhando essa

1 Este artigo foi publicado primeiramente para o Caderno de Estudos 1: Investigação e prova nos crimes cibernéticos, publicado pela Escola de Magistrados (Emag) da Justiça Federal da 3ª Região, São Paulo, 2017, sendo agora apresentado com pequenas atualizações.

2 Graduada pela Faculdade de Direito da Universidade de São Paulo. Procuradora da República em São Paulo, nas áreas cível e criminal. Coordenadora do Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República em São Paulo e vice-coordenadora do Grupo Nacional de Combate aos Crimes Cibernéticos da 2ªCCR/PGR. E-mail: fernandadomingos@mpf.mp.br.

3 Graduada pela Faculdade de Direito da Universidade de São Paulo. Procuradora da República em São Paulo, nas áreas cível e criminal. Coordenadora substituta do Grupo de Combate aos Crimes Cibernéticos da Procuradoria da República em São Paulo e membro do Grupo Nacional de Combate aos Crimes Cibernéticos da 2ªCCR/PGR. E-mail:.priscilaschreiner@mpf.mp.br.

tendência, a investigação dos ilícitos do mundo atual depende de evidências digitais, independentemente de terem ocorrido, total ou parcialmente, no mundo real ou no mundo virtual.

Atualmente, a obtenção de provas digitais torna-se crucial para elucidar delitos, deparando-se essa questão, porém, com as diferentes jurisdições nas quais as evidências digitais estão armazenadas.

É de fato possível saber onde tais evidências se encontram armazenadas? É possível ater-se aos tradicionais conceitos de soberania e jurisdição quando as relações ocorreram na internet? Qual a solução para as relações do mundo real, que dependem de evidências deixadas na internet?

Pretendemos neste artigo debater acerca das principais questões que afligem a elucidação de delitos que dependem da obtenção da prova digital produzida na internet, bem como discorrer sobre algumas soluções existentes.

2 Soberania, jurisdição e territorialidade

Extremamente importante para a elucidação das questões acima propostas a definição e análise dos conceitos de soberania e jurisdição, pois estão intrinsecamente ligados às respostas encontradas na legislação pátria sobre o tema, que culminaram na redação do art. 11 da Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MCI), a ser comentado adiante.

Para Dallari (2016), o *conceito de soberania* tem evoluído desde a Antiguidade, alcançando o auge, com as características que hoje conhecemos como um poder absoluto, perpétuo e inalienável, a partir do século XVI com a obra *Lex six livres de la République*, de Jean Bodin[4].

Dallari explica que entre os autores há diferentes concepções a respeito do conceito de soberania. Alguns se referem a ela como "poder do Estado"; outros, como "qualidade essencial do Estado"; e, outros, ainda, como "a expressão da unidade de uma ordem". Porém, na síntese de todas as teorias, observa o autor que a noção de soberania está sempre ligada à concepção de poder, seja quando concebida em termos puramente po-

4 Para Bodin, "*soberania* é o poder absoluto e perpétuo de uma República, palavra que se usa tanto em relação aos particulares quanto em relação aos que manipulam todos os negócios de Estado de uma República". (expressão *República* no significado moderno de Estado).

líticos como *poder incontrastável de querer coercitivamente e de verificar competências*, seja na evolução para uma concepção puramente jurídica, vista como o *poder de decidir em última instância sobre a atributividade das normas*, isto é, sobre a eficácia do Direito.

No entanto, considerando-se que o Estado compreende fenômenos sociais, jurídicos e políticos, o conceito de soberania para Reale (1960, p. 127) deve integrar todos eles, definindo-a assim, como "o poder de organizar-se juridicamente e de fazer valer dentro do seu território a universalidade de suas decisões nos limites dos fins éticos de convivência".

A soberania possui como características o ato de ser *una* (inadmissível a convivência num mesmo Estado de duas soberanias), *indivisível* (aplica-se à universalidade dos atos ocorridos no Estado, sendo inadmissível a existência de partes separadas da mesma soberania), *inalienável* (seu detentor desaparece quando ficar sem ela) e *imprescritível* (não possui prazo certo de duração, aspira à existência permanente). Desse modo, atentando-se às características da soberania, é inadmissível que uma empresa estrangeira que possua filial, ou venha a prestar serviços no Brasil, submeta-se a apenas parte da soberania nacional: concorda com a submissão à legislação comercial ou tributária brasileira, porém descumpre ou não atende de maneira correta às decisões emanadas do Poder Judiciário brasileiro para o fornecimento de informações telemáticas, sob o equivocado argumento de necessidade de cooperação jurídica internacional com o país onde estão suas sedes ou servidores.

Observe-se que não há qualquer entrave a que empresas estrangeiras operem no Brasil. A nossa própria Constituição Federal, no seu art. 170, parágrafo único, assegura a todos "o livre exercício de qualquer atividade econômica, independentemente de autorização de órgãos públicos", porém estas devem se submeter igualmente à soberania do Estado brasileiro, consoante dispõe o inciso I do mesmo art. 170, ao prever que

> *o exercício de atividade econômica por empresa ou corporação sediada em outro país está necessariamente condicionado ao respeito à soberania nacional*, princípio conformador de toda a ordem econômica. (grifo nosso)

Como expressão da soberania nacional, a jurisdição é a atividade tendente à declaração do direito no caso concreto, que pode ser definida como o poder do Estado de aplicar a lei e administrar a Justiça, nos limites da sua soberania e no alcance do território nacional. Para Dinamarco (2006, p. 145), jurisdição "é uma das funções do Estado,

mediante a qual este se substitui aos titulares dos interesses em conflito para, imparcialmente, buscar a pacificação do conflito que os envolve, com justiça".

A soberania nacional, e, consequentemente, a jurisdição, serão exercidas dentro dos limites do território de cada Estado, não sendo possível a existência de Estado sem território. Dentro dos seus limites territoriais, a ordem jurídica do Estado prevalece, pois é a única dotada de soberania.

O Brasil adotou como regra, conforme art. 5º, *caput*, do Código Penal, o Princípio da Territorialidade, segundo o qual aplica-se a lei penal brasileira aos crimes cometidos no território nacional, ressalvados os casos do art. 7º, II, do mesmo diploma legal.

Nos dizeres de TOLEDO (1991),

> são submetidos à lei brasileira os crimes cometidos dentro da área terrestre, do espaço aéreo, e das águas fluviais e marítimas, sobre as quais o Estado brasileiro exerce sua soberania, pouco importando a nacionalidade do agente. Porém, nos dias atuais, o conceito de território para fins de aplicação da jurisdição deve englobar também o espaço virtual, com todos os serviços de Internet prestados no Brasil. (TOLEDO, 1991, p, 45)

Portanto, uma empresa estrangeira que possui filial e presta serviços de internet no Brasil está constituída sob as leis brasileiras, sem o que não poderia operar no país. Negar-se a cumprir decisão válida emanada de juiz brasileiro, para que sejam fornecidos os dados telemáticos armazenados em seus servidores, exigindo para tanto pedido de cooperação jurídica internacional, traduz-se em desrespeito à jurisdição brasileira como expressão da soberania nacional.

Essa ideia deve ficar bem clara, pois haverá ainda casos em que obviamente será necessário o pedido de cooperação internacional, sobretudo com os avanços e facilidades trazidos pela internet e o aumento do volume das provas produzidas ou armazenadas em meio cibernético. Nessas circunstâncias é bastante comum o atributo da transnacionalidade.

Bechara (2011) explica que prova transnacional

> é aquela cujo meio de prova se encontra num Estado distinto ao da autoridade judicial competente, ou ainda quando os meios de prova de um mesmo fato se encontram em Estados diversos. (BECHARA, 2011, p. 37-38)

E continua:

> Em outras palavras, a prova transnacional é aquela cuja fonte de prova encontra-se dentro dos limites da soberania de outro Estado, e que, portanto, requer a cooperação e o auxílio deste para a obtenção do dado ou elemento probatório. (BECHARA, 2011, p. 37-38)

É preciso aclarar essa afirmação para que não dê margem a dúvidas quanto à jurisdição do Estado brasileiro sobre o fornecimento de documentos e informações constituídos a partir do território nacional.

Assim, uma conta-corrente bancária, aberta numa instituição financeira estabelecida em território nacional e, portanto, constituída sob as leis brasileiras, (nos termos do Decreto-Lei nº 4.657 de 4 de setembro de 1942, Lei de Introdução às Normas do Direito Brasileiro – LINDB)[5] está sujeita a ter seus documentos e informações apresentados ao juiz brasileiro, mesmo que tais informações estejam arquivadas em uma filial ou matriz da instituição financeira situadas no exterior.

Por outro lado, uma conta-corrente bancária aberta no exterior, isto é, sob a soberania e jurisdição de outro Estado, somente terá seus dados e informações disponibilizados ao Judiciário brasileiro mediante pedido de cooperação internacional, mesmo que tal instituição financeira possua congênere no território brasileiro, pois neste último caso o serviço, ou seja, a abertura da conta-corrente e sua manutenção, não foi prestado em território nacional, mas sim no Estado estrangeiro. Exemplo claro disso foi citado por Aras (apud ROCHA et al., 2006): o caso Banestado (Banco do Estado do Paraná), no qual houve evasão de divisas e lavagem de dinheiro por meio de contas CC5, contas de não residentes, abertas na praça de Foz do Iguaçu em alguns bancos brasileiros, inclusive o Banestado, mediante autorização especial do Banco Central do Brasil, e que foram utilizadas de forma fraudulenta, já que os titulares das contas-correntes eram "laranjas". Grande parte dos valores foi destinada a contas abertas na agência do Banestado de Nova Iorque e, a partir delas, os valores foram distribuídos para outros bancos.

No que toca às contas abertas no Brasil, a documentação e a movimentação financeira foram obtidas sem problemas, mediante decisão judicial de quebra do sigilo bancário do Juízo brasileiro. No entanto, para obtenção da documentação relativa às

5 Art. 9º Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituírem.
§ 1º Destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada, admitidas as peculiaridades da lei estrangeira quanto aos requisitos extrínsecos do ato.

contas do Banestado de Nova Iorque, foi imprescindível a cooperação internacional da Promotoria de Nova Iorque (*District Attorney of the New York County*) e de outros órgãos americanos, já que nesse caso o serviço de abertura e manutenção das contas ocorreu no exterior.

3 Jurisdição na internet

A internet não possui fronteiras e, assim, foi arquitetada para que seja, a princípio, acessada de qualquer parte do globo. Isso significa a criação de uma realidade virtual sem as barreiras físicas das delimitações territoriais dos Estados.

As relações humanas multiplicaram-se com essa ferramenta, que, embora criada para ser global, esbarra nas diferenças culturais refletidas nas diferentes legislações. O mesmo conteúdo pode ter tratamento diverso em países diferentes e ser tratado como legal ou ilegal.

No que toca aos delitos reais ou virtuais que deixaram evidências digitais, a sua investigação torna-se mais complexa, uma vez que aumenta a dificuldade em precisar o local onde estão as provas a serem coletadas.

Embora a internet pareça uma rede etérea, seu funcionamento depende de uma infraestrutura bem real. Assim, para acessar essa comunidade virtual, são necessários provedores de conexão à rede, que atribuem ao usuário um número IP (*Internet Protocol*) por meio do qual ele passa a navegar no ciberespaço. O conteúdo a ser acessado ou as plataformas que possibilitam a produção de conteúdo pelo próprio usuário, incluindo-se aí as mensagens de *e-mail* ou outras formas de comunicação via internet, dependem de estrutura disponibilizada pelos provedores de aplicações de internet.

O funcionamento correto dessa rede obedece a critérios organizacionais matemáticos, que permitem a fluidez dessa estrutura. Isso significa que as empresas provedoras de internet detêm as informações referentes aos passos que os usuários percorrem na rede: acessos, postagens e comunicações.

São essas informações que em geral permitem, de forma precisa, desvendar um crime cibernético ou obter uma prova digital para elucidar um crime real. O que tem aturdido o mundo jurídico é a obtenção dessas informações, desses dados que consubstanciam a prova digital.

As empresas provedoras de internet, englobando todos os tipos envolvidos nessa atividade, passaram a ser assoberbadas de pedidos de informações sobre os dados, recebendo solicitações e ordens de toda parte do mundo.

Uma vez que tais empresas podem possuir sede física em um país, mas armazenar suas informações em servidores em qualquer local do planeta, os operadores do Direito depararam-se com a perplexidade de não saber qual local teria jurisdição para decidir acerca do fornecimento de tais dados. Além disso, cada país possui uma percepção peculiar acerca da proteção da privacidade, o que se reflete nas diferenças legislativas sobre requisitos para fornecimento de dados e conteúdo. Some-se a isso a volatilidade da prova digital, pois a enorme quantidade de informações em circulação no mundo faz com que a sua manutenção pelas empresas seja a menor possível, ditada pelos custos que o armazenamento de dados gera.

A necessidade de as próprias empresas armazenarem essa grande quantidade de informações por questões internas gerenciais, ou por determinação das legislações às quais se consideram submetidas, resultou em que o armazenamento de dados ocorresse em servidores nos mais diversos países, seguindo critérios econômicos e fiscais. Também, por razões de segurança, há servidores replicados em locais diferentes do globo e informações que são armazenadas de forma fracionada.

Segundo La Chapelle e Fehlinger (2016), os possíveis critérios aventados para definir qual a lei aplicável na obtenção de dados digitais são:

a. a lei do local em que está o usuário, do qual se pretende obter os dados;
b. a lei do local onde estão os servidores que armazenam os dados;
c. a lei do local de incorporação da empresa que presta o serviço;
d. a lei do local dos registradores de onde o domínio foi registrado.

Todas as possíveis soluções apresentam dificuldades e podem conflitar com as regras de aplicação da lei penal de cada país. A primeira opção, que sujeitaria os provedores de internet a fornecerem dados nos termos da legislação do local onde está o usuário, pode se deparar com a situação em que o usuário esteja em um determinado país cometendo uma ação criminosa pela internet e produzindo resultado criminoso no país que necessita dos seus dados para investigação e processo, utilizando-se de provedor de internet com sede em um terceiro país!

A opção que pretende que se utilizem as leis do local onde estão os servidores que armazenam os dados, e que tem sido advogada pelas grandes empresas provedoras de internet, sob o argumento de precisarem cumprir as leis de proteção de dados e privacidade, impõe uma tarefa ingrata ao operador do Direito que necessita da prova digital. Isso porque, como exposto acima, os dados podem estar duplicados em vários servidores espalhados simultaneamente pelo mundo, ou até fragmentados, guardados em diferentes locais. Ou seja, não haveria nem mesmo certeza absoluta a respeito do local exato em que determinado dado imprescindível a uma investigação estaria armazenado. A opção sobre a utilização da lei da região em que a empresa foi incorporada também soa estranha, quando o local onde o serviço está sendo prestado não coincide com aquele da incorporação, já que estariam sendo aplicadas leis estrangeiras no território nacional. A opção sobre a aplicação da legislação do Estado de origem do registrador também implica em aplicação de leis estrangeiras a fatos que possuem impacto no território nacional.

Todas essas opções, ao assumirem que, para fornecimento de dados digitais, as empresas provedoras de internet devem obedecer aos parâmetros legais de jurisdições diversas do local onde os fatos ocorreram ou o serviço foi prestado, implicam a necessidade de pedidos de cooperação internacional.

Tais pedidos, conhecidos como *Mutual Legal Agreement Treaties* (*MLATs*) – Acordos de Assistência Mútua em Matéria Penal, tradicionalmente têm um processamento muito lento, pois dependem de que os pedidos sejam feitos de forma correta, de que sejam traduzidos e enviados pelas autoridades competentes, para que uma autoridade no país requerido dê início à execução do pedido.

Esse procedimento protocolar, que já se apresentava por demais demorado para os pedidos tradicionais, é no mais das vezes inócuo em face da volatilidade das provas digitais e da necessidade de investigação célere, não estando adequado às novas tecnologias.

Assim, os pedidos dos operadores do Direito para obtenção de provas digitais, direcionados às empresas provedoras de internet, têm proliferado, principalmente quando tais empresas possuem algum vínculo com o local onde os efeitos da ação criminosa são sentidos e onde o caso está sendo investigado ou processado.

Muitas vezes, também, as empresas que proporcionam serviços de internet, os quais acabam sendo utilizados para uma ação criminosa e, portanto, detêm provas digitais,

não possuem vínculo com o local onde o caso está sendo investigado, complicando ainda mais a obtenção das informações digitais.

3.1 Jurisdição e internet: Convenção de Budapeste

A Convenção de Budapeste é o tratado internacional sobre crimes cibernéticos, firmado no âmbito do Conselho da Europa, que procura harmonizar as legislações penal e processual penal, a fim de permitir a cooperação para obtenção de provas digitais. Foi assinada em 23 de novembro de 2001 e aberta para adesão e ratificação dos demais países, tendo sido homologada por 52 signatários.

O Brasil não é signatário da Convenção de Budapeste, mas por ser o único tratado sobre crimes cibernéticos existente, acaba sendo o modelo e parâmetro para as demais legislações.

No que toca à preservação e obtenção das provas digitais, a Convenção de Budapeste determina que haja preservação de dados, quando requerido, pelo prazo de 90 (noventa) dias, prorrogável por igual período. Também fala em auxílio mútuo para fornecimento de dados de tráfego e para a interceptação de conteúdo.

Quanto ao acesso a dados armazenados fora do território de cada Estado Parte da Convenção, a previsão disposta no art. 32 é tímida:

> Art. 32. Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público
>
> Uma Parte pode, sem autorização de outra Parte:
> a) Aceder a dados informáticos armazenados acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou
>
> b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

Assim, há a possibilidade de obtenção dos dados digitais armazenados fora do território nacional de cada Parte, sendo válidos para o processo, quando esses dados são

públicos, isto é, podem livremente ser acessados de qualquer localização (fonte aberta), ou quando há o consentimento voluntário de quem estaria legalmente autorizado a fornecê-los. Logo, ou o próprio criminoso teria que voluntariamente concordar em fornecer esses dados, ou a empresa provedora de internet, detentora desses dados, teria que possuir uma autorização expressa nesse sentido, o que não parece facilitar o trabalho dos agentes investigadores.

No entanto, há casos decididos por Cortes europeias, americanas e também brasileiras, que têm servido de norte para solucionar essa necessidade de obtenção de provas digitais, que não seriam alcançadas pela jurisdição do país onde a investigação e/ou processo se desenvolvem.

3.2 Jurisdição e internet no Código Penal brasileiro

Para a aplicação da Lei Penal, o Estado brasileiro titular do *jus puniendi* adotou, como regra, o princípio da territorialidade, conforme já citado art. 5º do Código Penal, sem prejuízo da incidência de outros princípios nos casos dispostos no art. 7º, inciso II, do mesmo diploma legal. E, para a definição do lugar do delito, optou o legislador penal pela adoção do Princípio da Ubiquidade (art. 6º do CP), estabelecendo que se considera praticado o crime "no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde produziu ou devera produzir-se o resultado".

Da análise dos artigos acima mencionados, infere-se que, na prática de crimes por meio da internet, ocorrida no território nacional, torna-se completamente irrelevante para a aplicação da lei penal o local em que fica a sede da empresa provedora do serviço de internet ou onde estão armazenadas as informações telemáticas.

Portanto, se um crime cibernético ocorreu no Brasil, estará sujeito à jurisdição brasileira, sendo dever do Estado investigar e reprimir as condutas delituosas praticadas e fazer cumprir as decisões emanadas de juiz brasileiro para a efetiva apuração do delito, sem a necessidade de cooperação internacional para o cumprimento da decisão.

3.3 Jurisdição e internet no Código de Processo Civil brasileiro

O Código de Processo Civil de 1973 disciplinava os limites da jurisdição nacional no art. 88. No novo CPC, instituído pela Lei nº 13.105/2015, a matéria encontra-se disciplinada no Título II ("Dos Limites da Jurisdição Nacional e da Cooperação Internacional"), Capítulo I ("Dos Limites da Jurisdição Nacional"), inaugurado pelo art. 21 a seguir transcrito:

> Art. 21. Compete à autoridade judiciária brasileira processar e julgar as ações em que:
> I – o réu, qualquer que seja a sua nacionalidade, estiver domiciliado no Brasil;
> II – no Brasil tiver de ser cumprida a obrigação;
> III – o fundamento seja fato ocorrido ou ato praticado no Brasil.
> Parágrafo único. Para o fim do disposto no inciso I, considera-se domiciliada no Brasil a pessoa jurídica estrangeira que nele tiver agência, filial ou sucursal. (grifos nossos)

Ao comentar o artigo acima, Miller (apud CABRAL; CRAMER, 2016, p. 73), relata que este guarda estreita correspondência com o art. 88 do CPC de 1973, na sua estrutura e nos seus termos, ao definir o alcance da jurisdição brasileira, vista esta como desdobramento lógico-jurídico do atributo da soberania estatal. Miller chama a atenção para o parágrafo único do citado art. 21 que, ao se reportar ao inciso I do mesmo dispositivo legal, acabou por alargar, para fins processuais, o conceito de domicílio da pessoa jurídica.

Sabe-se que várias das empresas provedoras de internet, que prestam serviços no Brasil, principalmente os grandes provedores, atuam sob a forma de um único grupo econômico transnacional, composto de empresas controladoras e controladas[6], muitas das quais com filiais ou representação no Brasil. Pois bem, por força do antigo art. 88 e atual art. 21 do CPC, tanto a pessoa jurídica aqui instalada como toda a corporação estrangeira possuirão como domicílio o Brasil nas demandas originadas de serviço prestado neste país.

6 É controlada:
I – a sociedade de cujo capital outra sociedade possua a maioria dos votos nas deliberações dos quotistas ou da assembleia geral e o poder de eleger a maioria dos administradores;
II – a sociedade cujo controle, referido no inciso antecedente, esteja em poder de outra, mediante ações ou quotas possuídas por sociedades ou sociedades por esta já controladas." (Art. 1.098 do Código Civil)

3.4 Jurisdição e internet no Código de Defesa do Consumidor

Os serviços prestados por meio da *web* são considerados relações de consumo, assim como o usuário dos serviços de internet enquadra-se na definição de "consumidor", e os provedores de serviços e conexão de internet, no conceito de "fornecedor", consoante os termos dos arts. 2º e 3º, do Código de Defesa do Consumidor.

Desse modo, nas relações de consumo derivadas de serviços de internet prestados por empresas nacionais ou estrangeiras no Brasil, há *responsabilidade subsidiária* entre as sociedades controladoras e controladas, para fins de proteção aos direitos do consumidor, usuário da internet (art. 28, § 2º, CDC).

Os tribunais têm aplicado cada vez mais o entendimento de que há responsabilidade subsidiária, e mesmo solidária, entre as empresas controladoras e controladas, nos casos de responsabilidade civil das empresas provedoras de serviços de internet, quando há dano causado pela má prestação do serviço ou dano causado a outrem por meio da internet.

A doutrina e a jurisprudência reconhecem a necessidade de proteger o jurisdicionado contra práticas comerciais abusivas, exercidas em economias globalizadas, como demonstram vários julgados[7].

7 Jurisprudência: STJ, REsp nº 1021987/RN, Rel. Min. Fernando Gonçalves, julg. 7 out. 2008; STJ, REsp nº 566468/RJ,Rel. Min. Jorge Scartezzini, julg. 23 nov. 2004; TJDFT, ApCiv nº 20060110068265ACJ, julg. 31 out. 2006; STJ, REsp nº 1117633/RO, Rel. Min. Herman Benjamin, julg. 9 mar. 2010; TJRJ, Ap nº 0035977-12.2009.8.19.0203, Rel. Roberto Guimarães, julg. 08. fev. 2012 (MARQUES, BENJAMIN e MIRAGEM, 2012, p. 191 e p. 214-216).

4 Decisões judiciais acerca da jurisdição na internet

4.1 Caso Yahoo! Inc. na Bélgica

Em 18 de janeiro de 2011, a Suprema Corte belga decidiu[8] que o provedor de aplicações Yahoo! preenchia os requisitos do Código de Processo Penal belga, sendo considerado um provedor de serviços de comunicações eletrônicas e, portanto, nos termos da legislação belga (art. 46 *bis* do Código de Processo Penal) obrigado a cooperar com as investigações criminais, sob pena de multas altíssimas. No caso, a Yahoo! foi condenada a pagar uma multa de 55 (cinquenta e cinco) mil euros, equivalente a 80.260 (oitenta mil, duzentos e sessenta) dólares americanos e mais uma multa diária, por não fornecer os dados correspondentes a uma conta de *e-mail* do serviço Yahoo!, aptos a permitir a identificação do usuário no bojo de uma investigação criminal de fraude numa compra e venda, e não pagamento por aquisição de equipamento eletrônico, em uma loja em Dendermonde, na Bélgica.

O promotor belga havia intimado a empresa em seus escritórios na Califórnia, Estados Unidos, que alegou a ilegalidade do procedimento, o qual deveria ter obedecido aos trâmites do MLAT por meio dos respectivos Departamentos de Justiça de ambos os países. A Suprema Corte belga decidiu que, embora a Yahoo! não tivesse um escritório na Bélgica, ela estava presente virtualmente no território belga, submetendo-se portanto, de modo voluntário à jurisdição belga, já que participava da economia do país, disponibilizando o domínio http://www.yahoo.be, utilizava as línguas locais em seu *website*, com pop-ups de propaganda baseados na localização dos usuários e era acessível a partir do território belga com foco nos consumidores belgas[9].

Esse caso foi o primeiro a ser decidido no sentido de haver jurisdição de um Estado sobre uma empresa, com base na oferta de serviços direcionados ao público de determinado Estado, mesmo sem a presença física da empresa no território desse Estado.

8 Disponível em : <https://www.wsgr.com/attorneys/BIOS/PDFs/burton-yahoo-0411.pdf>; <http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters>; <http://www.stibbe.com/en/news/2014/july/court-of-appeal-of-antwerp-confirms-yahoos-obligation-to-cooperate-with-law-enforcement-agencies> Acesso em: 10 mar. 2017.

9 Disponível em: <https://gavclaw.com/2015/12/07/its-true-belgian-supreme-court-confirms-order-for-yahoo-to-hand-over-ip-addresses/>. Acesso em: 11 mar. 2017.

4.2 Caso Microsoft Irlanda x US. (The North Ireland Case)[10]

Numa investigação sobre tráfico de drogas, os promotores americanos conseguiram uma ordem de busca e apreensão para que a Microsoft Inc., empresa baseada nos Estados Unidos da América, entregasse os dados de IP e o conteúdo de *e-mails* de um usuário do serviço de correio eletrônico da empresa.

A Microsoft recusou-se a entregar as informações, dizendo que seria necessário o procedimento de cooperação internacional conhecido como MLAT, uma vez que os dados estavam armazenados em seu servidor localizado na Irlanda.

O Departamento de Justiça Norte-Americano alegou que o mandado de busca e apreensão poderia ter efeitos de uma intimação e que, portanto, não se tratava de efeito extraterritorial da ordem, pois a Microsoft Inc. poderia trazer os dados requisitados de volta ao território americano apenas acionando um terminal situado no próprio território americano e entregá-los aos promotores. Os argumentos utilizados para a obtenção de dados localizados fora do território americano baseiam-se na "tese do controle" sobre os dados. Assim, se a empresa possui controle, isto é, acesso aos dados requisitados, não importa onde esses dados estão armazenados, deve entregá-los (SILVA, 2016).

No entanto, o 2º Distrito de Nova Iorque[11], em sede recursal, decidiu que, segundo a lei americana, um mandado de busca e apreensão não pode ter efeitos de uma intimação (*subpoena*) e que a entrega de conteúdo implica a necessidade de um mandado de busca e apreensão (*search warrant*) o qual não pode ter efeitos além do território americano. A decisão foi objeto de recurso pelo Departamento de Justiça Americano, mas, em janeiro de 2017, a Corte do 2º Circuito de Nova Iorque negou a reanálise do caso. No entanto, destacou-se o voto discordante do Magistrado Beeler ao apontar que não importa onde as informações estão armazenadas e que caberia à Microsoft trazer os dados ao território americano onde se daria então a sua apreensão pelas autoridades americanas, não havendo que falar em extraterritorialidade do mandado de busca e apreensão.

10 Disponível em: <https://www.lawfareblog.com/microsoft-ireland-case-brief-summary>. Acesso em: 11 mar. 2017.

11 In the Matter of a Warrant to Search a Certain E-mail Account Controlled And Maintained By Microsoft Corporation, United States Court of Appeals for the Second Circuit, Docket N. 14-2985, julg. em 14 jul. 2016.

4.3 4.3. Caso Google Inc. na Corte Federal da Pennsylvania

A decisão do Juiz Federal Thomas J. Rueter da Corte Federal do Distrito da Pennsylvania, vinculada à Corte de Apelação do 3º Distrito, em 3 de fevereiro de 2017, determinou à Google Inc. que entregasse dados relativos a dois *e-mails* necessários para uma investigação criminal. Num movimento contrário à decisão proferida pela Corte de Apelação do 2º Distrito de Nova Iorque no caso Microsoft Ireland, o fundamento da decisão baseou-se em informação da própria empresa Google Inc. que esclareceu não armazenar os dados de seus clientes em um único local. Ao contrário, tais dados estariam fragmentados e muitas vezes duplicados, a fim de permitir uma eficiência no seu sistema de busca e gerenciamento. Dessa forma, se fosse levado em conta o critério do local de armazenamento dos dados para definição da jurisdição nesse caso, a Google Inc. não teria como apontar um só local, inviabilizando a obtenção dos dados pretendidos pelos investigadores. Sendo assim, o juiz entendeu que o procedimento da Google para compilar os dados pretendidos não configurava uma busca e apreensão com efeitos extraterritoriais, pois essa apreensão somente ocorreria no momento da entrega dos dados pela Google Inc. às autoridades americanas, dentro, portanto, do território americano.

4.4 O Caso Google Brasil Internet Ltda: fundamentos precursores do art. 11 do MCI

Em 2006, foi proposta Ação Civil Pública[12] promovida pelo Ministério Público Federal em face da empresa Google Brasil Internet Ltda., que findou em 2 de julho de 2008 com a assinatura de Termo de Ajustamento de Conduta (TAC) entre as partes, no bojo da Comissão Parlamentar de Inquérito do Senado Federal, a chamada CPI da Pedofilia. Conhecido como "Caso Google", esse foi um dos casos de maior repercussão sobre a obrigação das empresas provedoras de internet colaborarem com a Justiça brasileira na persecução penal de crimes cibernéticos ocorridos no país.

Resumidamente, o Caso Google surgiu em razão das dificuldades na apuração, pelas autoridades brasileiras, dos crimes de distribuição de pornografia infantil e delitos de discurso do ódio, que vinham sendo largamente cometidos na extinta rede social Orkut, serviço pertencente ao grupo Google[13]. Com efeito, a empresa vinha desrespeitando a

12 Autos nº 2006.61.00.018332-8 – 17ª Vara Cível da Subseção Judiciária de São Paulo.

13 A Google Brasil Internet Ltda., constituída sob as leis brasileiras, é uma sociedade controlada pelas *holdings* transnacionais Google International LLC. e Google Inc., constituindo-se em um único grupo econômico transnacional.

jurisdição brasileira ante o não atendimento das ordens emanadas dos juízes brasileiros para o fornecimento dos dados telemáticos, imprescindíveis à apuração desses crimes. Argumentava a empresa ré, Google Brasil Internet Ltda., que os dados requisitados estariam hospedados em servidores localizados nos Estados Unidos, cujo gerenciamento caberia à empresa Google Inc., o que demandaria pedido de cooperação jurídica internacional.

Importante mencionar que os fundamentos jurídicos trazidos pelo Ministério Público Federal no caso Google, que propiciaram a concessão da decisão liminar requerida à época e posterior realização do Termo de Ajustamento de Conduta, com várias cláusulas que impunham obrigações à empresa quanto à guarda e fornecimento de dados telemáticos, foram os precursores no reconhecimento do dever de uma empresa estrangeira provedora de internet submeter-se à jurisdição brasileira e de colaborar com a Justiça do país na investigação dos crimes cibernéticos ocorridos no território nacional.

Assim, quase uma década antes da entrada em vigor do Marco Civil da Internet, a questão da aplicação da lei brasileira aos crimes praticados por meio da rede mundial de computadores já demandava a atenção – e preocupação – dos aplicadores do Direito, principalmente em razão das dificuldades enfrentadas pela Justiça brasileira na obtenção de dados e elementos de prova a serem fornecidos pelas empresas provedoras de serviço de internet que operavam no Brasil.

Da leitura do art. 11 do MCI, observa-se que sua redação resultou do que já estabelecia de maneira esparsa a legislação brasileira, em uma interpretação sistemática e lógica do ordenamento jurídico pátrio. Tais fundamentos podem ainda hoje ser empregados para desconstruir alegações utilizadas por alguns provedores de internet na tentativa de se esquivar do cumprimento de decisões emanadas do Poder Judiciário brasileiro, sob a equivocada alegação da necessidade de cooperação jurídica internacional.

5 Solução da legislação brasileira: art. 11 do Marco Civil da Internet (Lei nº 12.965/2014)

No Brasil, tanto para obtenção de dados de IP, data e hora, quanto para a obtenção de conteúdo estático de comunicação, isto é, conteúdo de comunicações armazenadas nos servidores das empresas, é necessária a quebra de sigilo telemático e a autorização judicial, para que os provedores de aplicações de internet os forneçam. Para a obtenção

do conteúdo dinâmico da comunicação, é necessária ordem judicial que autorize a interceptação telemática, observando-se os rigores da Lei nº 9.296/1996.

Para o acesso pelas autoridades previstas pelo art. 10, § 3º do MCI, aos dados cadastrais do usuário de determinada conexão de internet, não há necessidade de ordem judicial, estando os dados cadastrais definidos no Regulamento do Marco Civil da Internet, Decreto nº 8.771, de 11 de maio de 2016, em seu art. 11, § 2º, como a filiação, o endereço e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

É importante notar que os registros de conexão à internet, bem como os registros de acesso a aplicações de internet podem ser obtidos mediante ordem judicial para formação de conjunto probatório em processo judicial cível ou penal, nos termos do art. 22 do MCI. Já as comunicações telemáticas somente podem ser obtidas para formação de conjunto probatório em investigação criminal ou instrução processual penal, a exemplo das comunicações telefônicas, nos termos do parágrafo único do art. 1º da Lei nº 9.296, de 24 de julho de 1996, que regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal.

Devido à perplexidade que a rede mundial de computadores causou para a obtenção de provas digitais, ao ensejar dúvidas quanto à jurisdição do Estado requisitante sobre as empresas detentoras desses dados, o legislador brasileiro editou o Marco Civil da Internet.

Conforme explanado, o Sistema Jurídico Brasileiro já apresentava preceitos claros quanto aos limites de sua jurisdição no Código Penal, no Código de Processo Civil e no Código de Defesa do Consumidor. A estes acrescentaram-se as normas trazidas com a entrada em vigor do Marco Civil da Internet, especialmente no seu art. 11:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo

O art. 11, § 1º do MCI explicita que a todos os dados coletados no território nacional por provedores de conexão e de aplicações de internet, bem como ao conteúdo das comunicações aplica-se o *caput* do artigo, isto é, deve ser respeitada a legislação brasileira nas operações de coleta, armazenamento, guarda e tratamento, observados os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Resta claro que, para o afastamento desses direitos, proteção e sigilo, os requisitos a serem observados são os da legislação brasileira. O § 1º ainda destaca que pelo menos um dos terminais deve estar localizado no Brasil. Porém o § 2º mitiga essa exigência ao estabelecer que o disposto no *caput*, isto é, a aplicação da legislação brasileira ocorre 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.

Assim, as dúvidas são suscitadas em relação aos provedores estrangeiros de internet. A legislação é clara ao dizer que, se a empresa possui filial no Brasil, esta filial se sujeita à jurisdição nacional, já que está situada fisicamente no país, onde somente poderá operar se os seus atos constitutivos forem aprovados pelo governo brasileiro. Fica, portanto, sujeita à legislação brasileira, nos termos dos arts. 11 e12 da Lei de Introdução às Normas do Direito Brasileiro (LINDB) (BRANT, 2014), que estabelece ser competente a autoridade judiciária brasileira quando o réu for domiciliado no Brasil ou aqui tiver de ser cumprida a obrigação. Dessa forma, a filial da empresa estrangeira integra o grupo econômico estrangeiro, mas as atividades da empresa estrangeira em relação aos serviços prestados no território nacional estão submetidas à legislação brasileira. Consequentemente, não importa à autoridade requisitante onde os dados digitais foram armazenados, pois essa é uma decisão gerencial da empresa, e, como vimos, podem estar armazenados em qualquer local do planeta. O que importa, conforme foi aventado no

caso Microsoft Irlanda X USA, é que a empresa provedora de internet tem o domínio, o controle dos dados digitais (SILVA, 2016), sendo possível a ela fornecê-los e, por integrar grupo econômico com presença física no país, prestando serviços em seu território, está submetida à jurisdição nacional tendo o dever de cumprir as ordens judiciais que lhe determinam a entrega das informações consubstanciadas em provas digitais.

A segunda hipótese do § 2º do art. 11 diz respeito à pessoa jurídica sediada no exterior, que oferta serviços ao público brasileiro e, interpretando o parágrafo a *contrario sensu*, não possui filial no território brasileiro. Mesmo nesses casos aplica-se a jurisdição brasileira, restando determinar em que situações pode-se dizer que os serviços estão sendo ofertados ao público brasileiro, já que na internet as ofertas são, em princípio, globais.

Para melhor entendimento da terminologia *serviço ao público brasileiro*, trazemos a definição esclarecedora constante de texto de Oliveira (apud SENADO FEDERAL, 2014):

> Por oferta de serviço ao público brasileiro, há de compreender-se o comportamento da empresa estrangeira em que vem, de forma direcionada e específica, promover marketing ao mercado de consumo brasileiro. O simples fato de determinados sites estrangeiros disponibilizarem textos em português não é suficiente para caracterizar oferta ao público brasileiro, pois, em uma era globalizada, é comum os sites estrangeiros vazarem seus textos em vários idiomas. (SENADO FEDERAL, 2014)

Assim, seguindo-se o exemplo do texto, se um brasileiro acessa um *site* de compras norte-americano com *marketing* direcionado ao mercado nacional, ainda que não haja filial no Brasil, haveria duas observações:

a. não será aplicada a legislação brasileira quanto à disciplina do contrato de compra e venda, e sim a norte-americana, por força do art. 9º, § 2º, da LINDB[14] e jurisprudência à época;

b. será aplicada a legislação brasileira quanto à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações, por força do art. 11 do Marco Civil da Internet.

14 Decreto-Lei nº 4.657, de 4 de setembro de 1942.

Esclarecendo-se o real alcance da norma prevista no art. 11, § 2º, do MCI, observe-se a posição sistemática do § 2º em relação ao *caput* do art. 11, além de referência expressa a ele, do que se conclui que para qualquer operação de coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações telemáticas (art. 11, *caput*, MCI) será aplicada a legislação brasileira à empresa provedora nacional ou estrangeira, com filial ou não no Brasil. Desde que ofereça seus serviços de internet ao público brasileiro, deverá submeter-se à jurisdição brasileira.

Assim, qualquer provedor estrangeiro que *ofertar serviço ao público brasileiro*, ainda que não tenha filial no Brasil, deve respeitar a legislação brasileira relativamente aos dados pessoais, aos registros de conexão e de acessos a aplicações, o que abrange as normas para que a privacidade seja afastada mediante a quebra do sigilo telemático com a entrega de dados que são prova digital.

Observe-se que o Marco Civil da Internet, *salvo no tocante à coleta, guarda, armazenamento ou tratamento de registros, dados pessoais ou de comunicações telemáticas*, não cuida de definir a legislação que disciplinará, por exemplo o contrato celebrado por um brasileiro que adquire um produto em site estrangeiro. Para isso, será observada a LINDB e a jurisprudência. Assim, se um brasileiro acessou site de compra estrangeiro pertencente a uma multinacional *com filial no Brasil* e com oferta de serviço voltado ao mercado de consumo brasileiro, o Código de Defesa do Consumidor disciplinará o contrato. Se o site pertencer a empresa sem filial no Brasil e cujo serviço não seja voltado ao público brasileiro, é aplicável a lei estrangeira para a disciplina do contrato (art. 9º, § 2º, da LINDB); mas se a empresa estrangeira oferecer serviços ao público brasileiro, com ou sem filial no Brasil, será aplicada a legislação brasileira e o MCI para as hipóteses constantes do caput do art. 11.

Desse modo, de acordo com a legislação brasileira, após o advento do MCI, em nosso entendimento a cooperação internacional somente será acionada em duas hipóteses:

a. a primeira, nos casos em que seja necessário transmitir uma ordem judicial a provedor de internet que não tenha presença física no território nacional. Ou seja, embora o serviço tenha sido prestado ou oferecido ao público brasileiro, não há sede ou filial da empresa no Brasil e, para se dar *efetividade* às decisões judiciais, é preciso se valer da cooperação com o país onde seja possível alcançar o provedor de internet. Note-se que, no caso Yahoo! x Bélgica, a Corte belga entendeu válida a intimação da empresa Yahoo! com endereço nos Estados Unidos da América, para que apresentasse os *logs* do *e-mail* investigado, isto é, informação do IP,

data e hora, formulada diretamente pelo promotor do caso, sem necessidade de cooperação internacional por meio dos departamentos de Justiça de ambos os países. No caso do Brasil, essas informações de IP, data e hora que possibilitam a identificação do endereço de onde o usuário enviou o *e-mail*, somente podem ser prestadas com autorização judicial, nos termos do art. 15, § 3º do MCI, de forma que o correto seria a utilização da cooperação internacional, com a remessa da ordem judicial pelas vias diplomáticas para cumprimento. Porém, entendemos que seria válida a prova fornecida diretamente pela empresa estrangeira sem sede no país que prestasse as informações requeridas na forma da lei brasileira.

b. a segunda hipótese para utilização da cooperação jurídica internacional é aquela em que as empresas provedoras de internet não ofertam seus serviços ao público brasileiro, mas o acesso foi feito a partir de conexão iniciada no território nacional. Nesses casos, a empresa não possui filial ou representação no Brasil e o público-alvo para utilizar os seus serviços não se encontra no território brasileiro. Se utilizado um serviço desse provedor estrangeiro de internet com consequências criminais ou cíveis no Brasil, será necessária a realização de cooperação internacional para a obtenção de uma ordem judicial que determine ao provedor estrangeiro a entrega das informações telemáticas.

6 Sanções pelo descumprimento dos arts. 10 e 11 do Marco Civil da Internet - art. 12 MCI

A fim de garantir efetividade à jurisdição brasileira na matéria regulada pelo MCI, o seu art. 12 prevê, sem prejuízo da aplicação de outras sanções de natureza cível, criminal ou administrativa, as sanções de advertência, multa de até 10% do faturamento do grupo econômico no Brasil no seu último exercício, a suspensão temporária das atividades e a proibição de exercê-las quando envolverem os atos previstos no art. 11. Tratando-se de empresa estrangeira, a filial, sucursal, escritório ou estabelecimento situado no país, responderá solidariamente pela multa.

Entendemos que, quando o MCI se refere à possibilidade de aplicação de sanções pelo descumprimento dos arts. 10 e 11 precedentes, resta claro que as atividades mencionadas devem estar de acordo com a legislação brasileira, inclusive no que se refere ao cumprimento de ordens judiciais que, nos termos da legislação pátria, afastam a proteção e o sigilo de dados e determinam o seu fornecimento.

Dessa maneira, quaisquer dos provedores de internet, nacionais ou estrangeiros, podem estar sujeitos às sanções do art. 12. Dentre elas, pensamos que a medida mais efetiva é sem dúvida a sanção prevista no inciso II do artigo que se refere à multa que pode chegar a 10% do faturamento do grupo econômico no Brasil, no seu último exercício. Haverá de fato um problema se a empresa estrangeira não possuir nenhuma filial, sucursal ou representação no país, nem estiver presente no país empresa que integre o mesmo grupo econômico, de forma que não possa ser alcançada pela multa. Nesse caso, pode-se aplicar a suspensão temporária ou mesmo a proibição do exercício das atividades. Essas modalidades de sanção, sendo mais gravosas, já que inibem a prestação do serviço, devem ser aplicadas somente em relação a descumprimentos graves e quando não for possível alcançar os provedores por meio da multa ou outras sanções de natureza econômica.

7 Conclusão

No que concerne à obtenção de provas digitais produzidas a partir da internet, o legislador brasileiro foi sensível à natureza dessas provas, que, por serem em essência voláteis, necessitam chegar rapidamente às mãos dos agentes de investigação e Justiça do Estado brasileiro, a fim de propiciar a rápida e efetiva investigação e processamento judicial dos delitos e ilícitos cibernéticos, ou não, mas que dependam das provas digitais para sua elucidação.

Assim, o legislador optou, nessa seara, por firmar a jurisdição brasileira a partir do conceito de serviço ofertado ou prestado em território nacional, pois, embora a internet se revele como espaço virtual sem fronteiras, o seu ponto de ligação com o mundo real ocorre em um território existente e delimitado de um Estado.

Desse modo, embora provedores de internet possam vir a confrontar-se com legislações diferentes, ao se verem compelidos a cumprir diretamente ordens judiciais de entrega de provas digitais, não há no presente momento outro modo de garantir a efetividade das investigações e dos processos que não pela afirmação da soberania do Estado em que as atividades dos provedores ocorreram.

Resta claro que o melhor caminho a ser seguido é o do entendimento entre os Estados, para que harmonizem suas legislações com o fim de possibilitar uma investigação mais célere e efetiva. Entendemos que a legislação brasileira apresenta uma solução

razoável, até porque não inova desmedidamente, baseando-se em conceitos, princípios e práticas sempre utilizados pelo direito pátrio, apenas se adaptando à nova realidade.

Porém, enquanto não se obtém um tratado internacional único, cabe às empresas provedoras de internet, detentoras das provas digitais, cumprirem a lei dos locais onde prestam serviços, colaborando para a solução dos conflitos e a manutenção da paz social.

Referências

ARAS, Vladimir. Lavagem de dinheiro, evasão de divisas e cooperação internacional: o caso Banestado. In: ROCHA, João Carlos de Carvalho; HENRIQUES FILHO, Tarcísio Humberto Parreiras; CAZETTA, Ubiratan (Coord.). **Crimes contra o Sistema Financeiro Nacional**: 20 anos da Lei n. 7.492/1986. Belo Horizonte: Editora Del Rey, 2006.

_____. Direito Probatório e Cooperação Jurídica Internacional. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). **A prova no enfrentamento à Macrocriminalidade**. Salvador: Editora JusPodivim, 2015.

BECHARA, Fábio Ramazzini. **Cooperação jurídica internacional em matéria penal**: eficácia da prova produzida no exterior. São Paulo: Ed. Saraiva, 2011.

CABRAL, Antonio do Passo; CRAMER, Ronaldo. **Comentários ao Novo Código de Processo Civil**. 2. ed. São Paulo: Ed. Forense, 2016.

DALLARI, Dalmo de Abreu. **Elementos de Teoria Geral do Estado**. São Paulo: Ed. Saraiva, 2016.

DINAMARCO, Cândido Rangel; GRINOVER, Ada Pellegrini; CINTRA, Antonio Carlos de Araújo Cintra. **Teoria Geral do Processo**. São Paulo: Ed. Malheiros, 2006.

DOMINGOS, Fernanda Teixeira Souza Domingos. As provas digitais nos delitos de pornografia infantil na internet. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). **A prova no enfrentamento à macrocriminalidade**. Salvador: Editora JusPodivim, 2015.

_____. A obtenção das provas digitais na investigação dos delitos de violência e exploração sexual online. In: SILVA, Ângelo Roberto Ilha da (Org.). **Crimes Cibernéticos**. Porto Alegre: Livraria do Advogado Editora, 2017.

LA CHAPELLE, Bertrand; FEHLINGER, Paul. Jurisdiction on the Internet: from legal arms race to transnational cooperation. **Internet & Jurisdiction Paper**, April 2016. Acesso em: <www.internetjurisdiction.net>.

MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor**. São Paulo: Revista dos Tribunais, 2013.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet**: subsídios à comunidade jurídica. Brasília: Núcleo de Estudos e Pesquisas da Consultoria Legislativa Senado Federal, 2014.

RAMOS, André de Carvalho; GRAMSTRUP, Erik Frederico. **Comentários à Lei de Introdução às Normas do Direito Brasileiro – LINDB**. São Paulo: Ed. Saraiva, 2015.

REALE, Miguel. **Teoria do Direito e do Estado**. São Paulo: Ed. Martins, 1960.

SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Coord.). **A Prova no Enfrentamento à Macrocriminalidade**. 2. ed. Salvador: Juspodvim, 2016.

SILVA, Ângelo Roberto Ilha da (Org.). Crimes Cibernéticos. Porto Alegre: Livraria do Advogado, 2017.

SILVA, Melissa Garcia Blagitz de Abreu e. **The Microsoft Ireland Case and Access to Data: An International Perspective**.Trabalho apresentado durante o curso de Mestrado em Direito na Universidade de Chicago nos Estados Unidos da América na matéria *Computer Crime* ministrada pelo Professor William Ridgway. 2016.

TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal**. São Paulo: Ed. Saraiva, 1991.

CRIMES CIBERNÉTICOS

3 AS INVESTIGAÇÕES NA ERA DAS MOEDAS DIGITAIS

Adriana Shimabukuro[1]

Resumo: Para entender como atuar e combater crimes que ocorrem na Rede Mundial dos Computadores, é necessário conhecer as tecnologias que permeiam esse ambiente. As moedas digitais ganharam força nesta década e passam a atuar como um personagem extremamente importante nas transações financeiras que envolvam as aquisições ilícitas, lavagem de dinheiro e financiamento do terrorismo. Termos como *blockchain*[2], bitcoin[3], darkcoins[4], entre outros, devem ser de conhecimento de qualquer pesquisador ou entidade que pretende desenvolver mecanismos de investigação e conhecer a atuação da criminalidade cibernética. Atualmente, com mais de mil diferentes tipos de criptmoedas[5], este artigo pretende focar no bitcoin e esclarecer o funcionamento do *blockchain*. Em uma segunda parte, detalharemos como falhas de segurança podem abrir brechas para o rastreamento e como ocorreram algumas das investigações que envolveram os bitcoins.

Palavras-chave: Bitcoins. Criptomoeda. *Blockchain*. Investigação. Crimes cibernéticos.

Abstract: *To understand how to act and fight crimes that occur in the World Wide Web, it is necessary to know the technologies that permeate this environment. Digital currencies have gained momentum in this decade and have come to play an extremely important role in financial transactions involving illicit acquisitions, money laundering and terrorist financing. Terms such as blockchain, bitcoin, darkcoins, among others, should be known to any researcher or entity that intends to develop mechanisms of investigation and to know the modus operandi of cyber crime. Currently, with over a thousand different types of cryptmoedas, this article intends to focus on Bitcoin and clarify how Blockchain works. In a second part, we'll detail how security breaches can open crawl cracks and how some of the investigations involving bitcoins have occurred.*

Keywords: Bitcoins. Criptomoeda. Blockchain. Investigation. Cyber crimes.

1 Matemática, especialista em redes de computadores, servidora do Ministério Público Federal.

2 Cadeia de registros que garante a segurança das transações de uma criptomoeda.

3 É uma rede de pagamento descentralizado, em que usuários gerenciam o sistema sem necessidade de um órgão centralizador.

4 Moeda digital baseada no bitcoin, que promete mais privacidade aos usuários.

5 É um meio de troca que se utiliza da criptograrfia para garantir as transações.

1 Introdução

A possibilidade de criar um sistema financeiro completamente distribuído, sem autoridades centrais, foi o principal objetivo dos desenvolvedores da tecnologia das criptomoedas. O bitcoin é o principal exemplo da aplicação dessa tecnologia e é considerada a primeira moeda digital na história humana que não requer uma autoridade central de controle.

O bitcoin é estruturado sob um sistema distribuído, *peer-to-peer*[6], sem servidor ou ponto central. Os bitcoins são criados por meio de um processo chamado "mineração", que basicamente envolve submeter computadores a cálculos matemáticos. Qualquer pessoa pode se tornar um minerador, entrando nessa rede de criptomoedas.

Apesas do conceito de bitcoin estar relacionado a uma moeda, o real valor do bitcoin fica armazenado na chamada "transação", isto é, valores pertencentes a um usuário dessa tecnologia não ficam necessariamente em sua carteira digital,[7] e sim representados por transações que originaram aquele valor.

Por exemplo, se você possui 3,21 BTC (em valores de transação 0,2 BTC, 0,01 BTC e 3 BTC) e precisa pagar 0,15 BTC para outra pessoa, o software do bitcoin iniciará uma transação que identifica como "origem" o valor de 0,2 BTC, "destrói" esse valor e recria o valor de 0,15 BTC, que será transferido para o destinatário e 0,05 BTC que volta para a origem como se fosse um "troco".

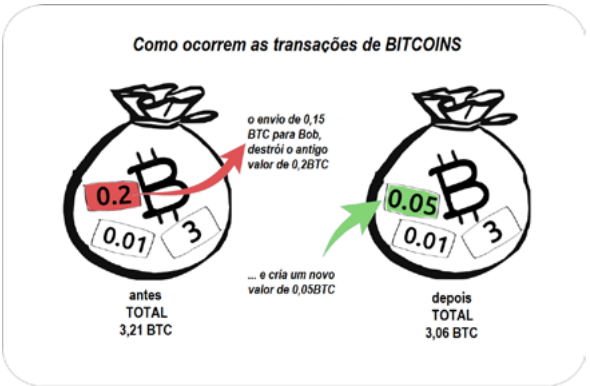


Figura 1: Representando os bitcoins por meio do conceito de TRANSAÇÕES
Fonte: Cryptocoinnews (2014).

6 Rede de computadores que compartilha dados via internet, sem uma autoridade centralizadora.

7 Solução eletrônica que permite o armazenamento de dados financeiros.

Esse conceito de "destruir" e "reconstruir" valores de bitcoin e armazená-los como transação é o que permite dar velocidade ao sistema, já que o software do bitcoin não precisa controlar saldos de carteira, e sim, procurar as transações em que aquela mesma moeda foi gasta. A existência de uma transação mais nova do que a especificada implica que esse valor não pode ser usado, pois ele já foi gasto.

Todas essas autenticações de transações financeiras, realizadas pelos chamados "mineradores", não precisam ser identificadas e trabalham com pouca coordenação. Esses nós podem deixar e voltar à rede a qualquer momento, utilizando os recursos de atualização e coordenação automática da própria tecnologia.

2 A infraestrutura do bitcoin

Baseado no artigo de Sakamoto (2008), listamos a seguir conceitos essenciais no entendimento da estrutura do bitcoin.

2.1 2.1 Transações

Conforme explica Antonopoulos (2015), os bitcoins são inteiramente virtuais, isto é, não há moedas físicas ou mesmo moedas digitais. O valor financeiro do bitcoin fica implícito em transações que são controladas por chaves públicas e privadas[8].

Essas transações de bitcoin ficam registradas em blocos que se ligam como correntes. Cada elo dessa corrente é ligado ao próximo por meio de cálculos matemáticos (*hash*[9]), deixando transparente toda a movimentação financeira da moeda.

Didaticamente, seria como se cada transação de bitcoin gerasse uma cédula naquele exato valor. Se o usuário precisa fazer uma nova negociação que seja diferente do valor que ele possui em sua carteira, o sistema destrói aquela cédula inicial e cria duas novas nos valores respectivos para pagamento e troco.

Dentro dessa estrutura, cada transação recebe um carimbo de tempo que impede que o valor seja duplicado. Com o controle de carimbo de tempo, as transações são pro-

8 É uma classe de protocolos de criptografia que trabalha com duas chaves, a pública e a privada.

9 Algoritmo que mapeia dados grandes e representa-os em dados menores e de tamanho fixo.

cessadas seguindo a ordem cronológica e a duplicação de valores é automaticamente rejeitada pelo sistema. Todas as transações são públicas e podem ser monitoradas, garantindo a confiabilidade de toda a cadeia de transações.

2.2 Servidor de carimbo de tempo

O servidor de carimbo de tempo é responsável pelo controle da data e do horário de cada transação. Esse carimbo é formado por uma parte dos dados da transação (*hash*) combinado com os dados do tempo. Esse valor é publicado para todos e se torna a garantia que a transação é válida.

Considerando que o *hash* utilizado já trazia a informação de assinatura eletrônica da transação, esse carimbo do tempo também garante que o novo bloco gerado esteja interligado matematicamente ao bloco anterior.

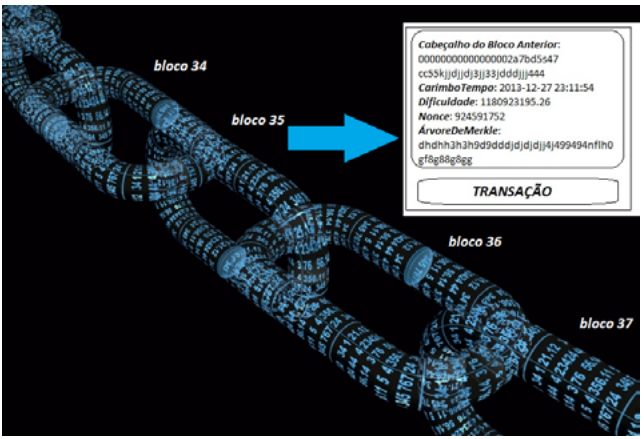


Figura 2: Detalhe de dados que cada bloco carrega
Fonte: Elaboração própria.

Esses novos blocos se ligam aos blocos anteriores, criando a cadeia de transações chamada *blockchain*. Esse histórico de transações cresce rapidamente, obrigando que novos cálculos de autenticação de blocos gerados obriguem os mineradores a utilizar um poder computacional cada vez maior. No ínicio do uso do bitcoin, computadores de mesa podiam autenticar transações. Atualmente, verdadeiras "fazendas de mineração" são usadas, até com o uso de equipamentos especiais para gerar os novos blocos.

Figura 3: Placas de vídeo AMD e nVidia são criadas especialmente para minerar bitcoin
Fonte: Disponível em: <https://www.asus.com/Graphics-Cards/MINING-RX470-4G/>

2.3 Prova de trabalho

Com o objetivo de garantir a segurança do sistema de bitcoins, é utilizado o conceito de prova de trabalho, que nada mais é que garantir que determinado tipo de ação seja realizada.

Especificamente no sistema de bitcoins, essa prova de trabalho é baseada numa série de cálculos matemáticos que são realizados por uma série de computadores. A resposta desses cálculos é divulgada e identificada pelo número randômico "*nonce*[10]", permitindo que os computadores que divulgaram a informação correta possam autenticar aquela transação.

Se a resposta for incorreta, a transação é invalidada.

Como as transações são encadeadas no *blockchain*, a tentativa de autenticar uma transação inválida implicaria no uso da prova de trabalho para toda a cadeia de blocos. Esse recálculo de várias provas de trabalho para incluir um bloco inválido exigiria um poder computacional imenso, garantindo novamente a idoneidade das transações autenticadas.

10 Número arbitrário que só pode ser usado uma única vez.

Figura 4: O passo a passo de uma transação de bitcoins
Fonte: Elaboração própria.

2.4 Rede

No artigo de Sakamoto, essa seção descreve a estrutura da rede bitcoin:

* anúncio das transações;
* cada nó adiciona cada transação em um novo bloco;
* os nós iniciam a prova de trabalho;
* anúncio do resultado da prova de trabalho;
* o resultado é aceito se o enigma foi resolvido ou negado, se a resposta estiver incorreta; e
* processo se repete para outro bloco.

2.5 Incentivos (ou "mineração de bitcoins")

O ato de minerar bitcoins implica no processo de adicionar registros de transações no “BlockChain”. Conforme explicado, o *blockchain* serve para confirmar transações para publicação em toda a rede e distinguir transações legítimas de tentativas de reúso de moedas.

A mineração é intencionalmente feita para utilizar de maneira massiva os recursos de um computador, que, ao resolver os extensos cálculos, necessários para autenticar uma transação, recebe bitcoins em troca dessas resoluções.

A primeira transação em um bloco de um novo bitcoin é de direito do computador que autenticou aquele bloco, permitindo a entrada de novos bitcoins no sistema. O montante total de bitcoins aceitos no sistema é de 21 milhões que será atingido provavelmente em 2140.

A cada ano, a dificuldade em obter novos bitcoins cresce. No início de 2015, essa recompensa era de 25 bitcoins; esse valor reduzirá pela metade a cada 210.000 blocos.

Veja as principais ações de um minerador de bitcoin, conforme a Wikipédia (2017):

* escutar novos blocos é o primeiro passo de um minerador;
* antes mesmo de entrar na rede, mineradores atualizam seu histórico de transações para depois iniciar a validação de novos blocos;
* neste momento, o minerador agrupa transações que escutou num novo bloco que estende o último bloco que ele recebeu do blockchain e inclui transações válidas;
* encontrar um nonce que torne seu bloco válido. Esse passo requer a maior parte do trabalho, pois é feito por meio dos cálculos matemáticos submetidos ao seu computador;
* o minerador deve torcer para que outros mineradores aceitem seu bloco e comecem a minerar a partir dele, e não no bloco de outro minerador;
* se todos os mineradores aceitam um bloco, o minerador que criou o bloco novo recebe o valor destinado a ele.

2.6 Reivindicando espaço em disco

Esta seção explica de que maneira transações antigas do *blockchain* podem ser descartadas para evitar o acúmulo de dados nos computadores de mineradores.

Cabe ressaltar que mesmo descartadas, as transações ficam registradas de maneira mínima (rastro da raiz) para manter a estrutura do *blockchain* intacta. Conforme publica o site do *blockchain*[11], a sua estrutura chega a 140GB de dados.

11 Disponível em: <https://blockchain.info/pt/charts/blocks-size>.

2.7 Verificação simplificada de pagamento

Considerando que as transações de bitcoin não podem ser autenticadas por um único nó (ou minerador), essa pessoa deve se conectar à rede de bitcoins por meio de outros nós para obter cópias de outros blocos e o carimbo de tempo.

Essa conexão permitirá que esse minerador obtenha a versão do *blockchain* atualizada e proceda aos cálculos para validar aquela transação.

É possível que nós fraudulentos tentem confirmar transações falsas, por meio da inserção de vários outros nós fraudulentos, que criam uma rede de mineradores que tentam inserir blocos falsos no *blockchain*.

Para evitar esse tipo de ataque, é importante que empresas que usam essa estrutura tentem manter nós legítimos na rede.

2.8 Combinando e dividindo valores

Bitcoins podem ser processados individualmente, mas isso tornaria a transação ineficiente e muito demorada. Para isso, o recurso de recombinar os valores auxilia nas transações, oferecendo a elas mais flexibilidade.

Exemplo prático: é mais fácil encaminhar uma transação de 5BTC para quitar um valor de 4BTC do que encaminhar 4 transações de 1BTC cada.

2.9 Privacidade

O que garante a privacidade das transações de bitcoins são as chaves públicas que identificam as carteiras digitais utilizadas nessa tecnologia. Por as transações serem declaradas publicamente no *blockchain*, o usuário pode acompanhar transações entre a carteira A e a carteira B, mas não sabe a quem pertence essas carteiras.

2.10 Cálculos

Esta seção explica os conceitos matemáticos envolvidos nos cálculos realizados pelos nós da rede *blockchain*, mostrando que os nós legítimos possuem mais chance de localizar um novo bloco legítimo que qualquer transação fraudulenta.

3 Onde ficam armazenados os Bitcoins?

De maneira simples, podemos exemplificar que os bitcoins ficam armazenados em "*hot wallets*" (carteiras quentes) ou em "*cold wallets*" (carteiras frias). Uma boa analogia seria comparar as carteiras quentes a contas-correntes em que a movimentação financeira é imediata e a carteira fria a uma conta poupança.

As chamadas carteiras quentes sempre estão ligadas à internet e possuem mais chances de terem seus valores roubados. Requerem dispositivos de segurança, inclusive mantendo pequenos valores nesse ambiente. Por outro lado, as carteiras frias, comumente representadas por computadores ou dispositivos físicos como discos externos, são consideradas mais seguras, desde que possuam dispositivos de cópia para evitar a perda de bitcoins, segundo Buntinx (2017).

Ainda conforme explica Stephens (2017), as carteiras quentes costumam ficar em bolsas de ativos digitais (corretora on-line de bitcoins), pois essas empresas detêm fundos para manter infraestruturas e servidores de armazenamento. No Brasil, podemos exemplificar o Mercado Bitcoin e a FoxBit como grandes corretoras de bitcoins que fornecem esse tipo de serviço para investidores.

Soluções intermediárias, mas ainda consideradas como carteiras quentes, são fornecidas por corretoras como a Exodus.io, que não armazena as chaves privadas dos clientes em sua estrutura, permitindo que o cliente mantenha seus bitcoins em seu computador pessoal.

Outras soluções são as novas carteiras frias, mas que permitem a conexão à internet, combinando a segurança da carteira fria com a praticidade da carteira quente.

Figura 5: KEEPKEY, exemplo de carteira fria que permite a conexão à internet quando necessário
Fonte: Disponível em: <https://www.keepkey.com/>.

Por fim, ainda é possível imprimir bitcoins e mantê-los ativos e guardados fisicamente em cofres.

Figura 6: O bitcoin em papel agrupa o endereço da carteira digital mais a senha, em um QRCode
Fonte: Disponível em: <http://www.coindesk.com>.

4 A variedade das moedas digitais

Apesar da notoriedade dos bitcoins desde 2009, é possível considerar que o conceito de criptomoedas é mais antigo e pode ser visto em 1998, por meio de um programador chamado Eric Hughes.

Hughes (1998) publicou um documento chamado “Manifesto Cypherpunk”, que defendia o uso de criptografia para proteger nossa privacidade na era da informação. Hughes afirmou que devemos garantir que cada parte de uma transação financeira tenha conhecimento apenas do que é estritamente necessário para que aquela operação ocorra.

Uma relação das principais criptomoedas do mercado, atualmente em torno de mais de 1.100 tipos, pode ser acompanhada em tempo real no site https://coinmarketcap.com/:

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	%
1	Bitcoin	$65,310,941,363	$3940.15	16,575,750 BTC	$1,488,000,000	
2	Ethereum	$26,867,638,391	$283.67	94,715,752 ETH	$633,104,000	
3	Bitcoin Cash	$8,270,280,214	$498.35	16,595,325 BCH	$513,902,000	
4	Ripple	$7,100,435,952	$0.185178	38,343,841,883 XRP *	$53,317,800	
5	Litecoin	$2,816,501,863	$53.14	53,004,732 LTC	$287,733,000	
6	Dash	$2,420,127,167	$319.81	7,567,296 DASH	$33,917,700	
7	NEM	$2,181,384,000	$0.242376	8,999,999,999 XEM *	$5,614,950	
8	IOTA	$1,585,324,554	$0.570357	2,779,530,283 MIOTA *	$13,663,500	
9	Monero	$1,451,723,411	$96.11	15,104,906 XMR	$38,586,800	
10	Ethereum Classic	$1,091,316,778	$11.41	95,669,958 ETC	$71,131,300	
11	NEO	$1,027,245,000	$20.54	50,000,000 NEO *	$33,806,500	
12	OmiseGO	$995,409,243	$10.13	98,312,024 OMG *	$34,125,700	
13	BitConnect	$789,600,778	$117.19	6,737,783 BCC	$9,524,170	

Fonte: Coinmarketcap.com (capturado em 19/9/2017).

5 Bitcoin Cash, a nova versão do bitcoin

Com o intuito de dar mais eficiência às transações de bitcoin, foi criada uma nova versão dessa moeda chamada Bitcoin Cash (BCC). Nessa nova versão, os blocos são até 8 vezes maiores, dando mais velocidade à autenticação das transações.

Apesar do nome, o Bitcoin Cash não substitui o bitcoin tradicional, e suas criptomoedas, embora tenham sido criadas no mesmo *blockchain*, seguirão seus registros de maneira independente.

Conforme explica Alecrim (2017), essa divisão foi possível utilizando o conceito de *hard fork*, cujas mudanças propostas na atualização da moeda são tão expressivas que os nós antigos não conseguem validar os blocos formados pelas novas regras.

Conforme explicado, a justificativa para a criação dessa nova criptomoeda é dar mais velocidade às autenticações das transações. No bitcoin, uma transação pode demorar dias. No Bitcoin Cash, alguns minutos.

6 A nova modalidade de lavagem de dinheiro

Diferente da lavagem de dinheiro tradicional, que deixa rastros por onde as autoridades perseguem os criminosos, quando falamos em moedas digitais, temos interessados na aquisição de moeda procurando sites de câmbio que transformam o dinheiro ilícito em moeda legal.

A promessa desse tipo de serviço é que dinheiro pode ser reinjetado em novas transações legais sem qualquer suspeita de sua origem.

Um exemplo desse serviço é detalhado pelo site Deepdotweb (2017), que apresenta o serviço Helix[12]. O desenvolver da tecnologia explica que as técnicas utilizadas são sigilosas, mas de maneira geral os bitcoins são misturados e depois trocados por novas transações legais. Essas transações geradas perdem sua ligação com as compras ilícitas, tornando os valores ideais para novos usos. Para pequenos valores, o Helix promete a liberação imediata dos bitcoins "limpos". Para valores maiores, é necessário esperar até 4 horas.

12 Disponível em: <http://grams7enufi7jmdl.onion/helix> (endereço na DarkWeb) e <https://gramsflow.com/helix> (endereço na Web Aberta).

Figura 8: O processo de lavagem de dinheiro via bitcoin.
Fonte: Disponível em: <https://www.youtube.com/watch?v=WqZBeGodfEI>.

Técnicas mais simples, como comprar ativos, cartões de débito pré-pagos ou troca de moeda estrangeira desses ativos para outros ativos em espécie e, em seguida, transferi-los para o bitcoin podem ajudar na ocultação da origem de recursos ilícitos.

Crawford (2013) explica uma técnica de lavagem de bitcoins usando o serviço "*Shared Service*". Nesse serviço, seus bitcoins são relacionados a bitcoins de outros usuários, e as moedas são trocadas várias vezes.

Para testar a eficácia do método, é possível verificá-lo por meio de serviços de "*taint analysis*". Esse serviço mostra a porcentagem de chance de determinado valor ter sido recebido de outro. Essa chamada "mancha", cria um link entre duas carteiras que podem auxiliar na descoberta de algum esquema de pagamento (NOVETTA, 2015).

O serviço de "*taint analysis*" gratuito e público foi desativado do site oficial do *blockchain*, no entanto outras ferramentas pagas prometem substituir a ferramenta.

7 O desafio do rastreamento

É comum que usuários de bitcoins tenham a impressão de que utilizam uma moeda completamente anônima. Esse seria um atrativo para pessoas que precisam de anonimidade ou que se preocupam com a sua privacidade. No entanto, não é assim que funciona a estrutura do *blockchain*.

Todas as transações ficam inscritas de forma transparente no registro público (*blockchain*) do bitcoin e, apesar de nenhum usuário precisar se identificar, isso não é o suficiente para dar anonimidade.

A seguir, vamos listar alguns casos e estudos que podem auxiliar quando autoridades precisam desanonimizar transações ilícitas.

7.1 O ataque dos 51%

Podemos considerar como falha da estrutura do bitcoin a possibilidade de uma única entidade inserir vários nós controlados que possam manipular as transações no *blockchain*.

Esse ataque seria realizado por uma empresa com suficiente poder computacional (inserção de milhares de mineradores na rede) que poderia causar impacto na confiança da moeda e na autenticação das transações legítimas. Os mineradores controlados podem escolher transações legítimas e invalidá-las, reverter transações e impedir que outros mineradores encontrem novos blocos.

Como a dificuldade em minerar novos blocos aumenta continuamente, a possibilidade desse tipo de ataque fica mais difícil, pois aumenta na mesma proporção a necessidade de mais poder computacional para realizá-lo. No entanto, dois ataques de 51% foram detectados nas estruturas do *blockchain*: o Ghash.io (julho de 2014), em que um grupo de mineração excedeu brevemente 50% do poder de computação da rede bitcoin, e o Krypton e Shift (agosto de 2016), quando duas cadeias de blocos baseadas na moeda Ethereum[13] sofreram esse ataque.

13 Plataforma de autenticações que utiliza a tecnologia *blockchain*.

7.2 *Selfish mining attack*

Nesse tipo de ataque, o atacante minera seus blocos de forma privada e os libera no exato momento que os mineradores honestos tentam incluir seus blocos legítimos no *blockchain*.

7.3 *Eclipse attack*

De acordo com Heilman et al. (2015), o atacante cerca a vítima na rede *blockchain* (p2p) para que ele possa filtrar sua visão sobre os eventos. Esse ataque é bem mais efetivo quando combinado com os outros ataques de "Selfish" ou "51% Attack".

8 O caso *Silk Road*[14]

De acordo com a Softpedia (2015), trata-se da investigação de lavagem de dinheiro via bitcoins que envolveu dois agentes federais que atuavam na operação do mercado negro Silk Road em 2012/2013.

Na época, esses dois agentes usaram personagens fictícios, não autorizados oficialmente, para repassar informações sobre a investigação para o próprio dono do site. Essas informações privilegiadas eram pagas por meio de bitcoins, totalizando cerca de US$ 1,5 milhão.

O ex-agente iniciou o processo de lavagem de bitcoins transferindo os valores para uma conta no Panamá e para a corretora japonesa de bitcoins Mt. Gox (agora desaparecida).

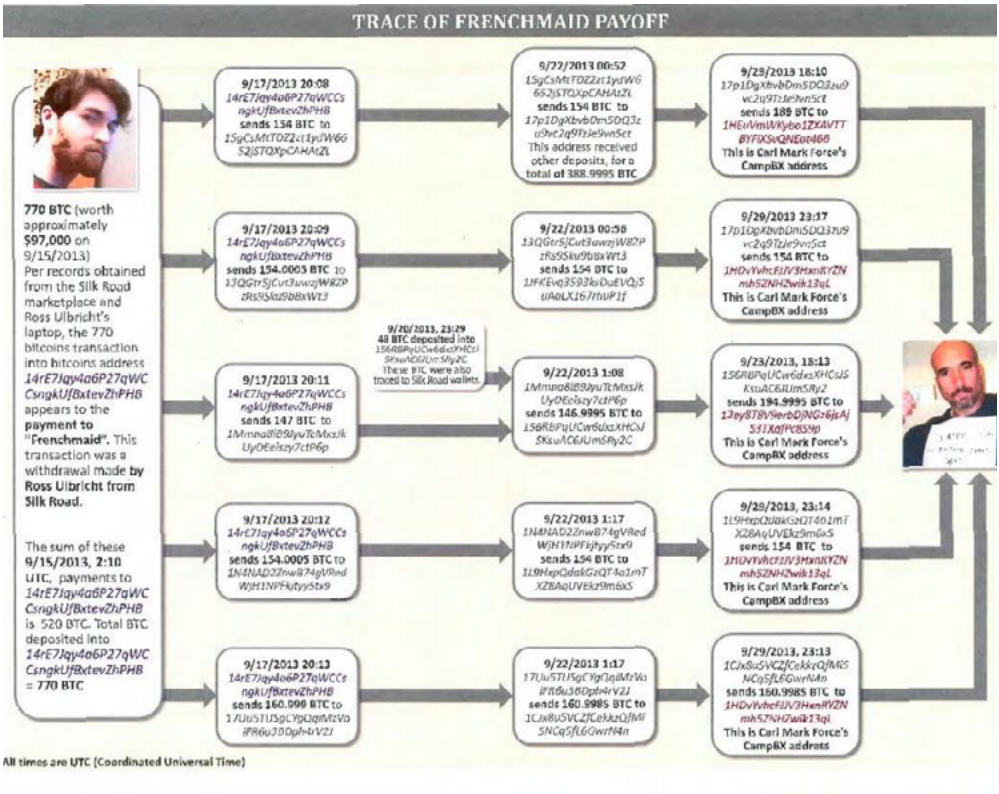
Em meados de fevereiro, Shaun Bridges, um dos agentes presos, criou uma empresa de responsabilidade limitada chamada Quantum International Investments, com uma conta na Fidelity Investments.

Os investigadores descobriram que, entre 6 de março e 7 de maio de 2013, a empresa recebeu fundos exclusivamente do Mt. Gox. Tudo isso é uma causa provável de atividade ilegal alegadamente realizada pela Bridges.

Por meio de constantes erros dos agentes, como o uso de softwares de criptografia ultrapassados, o uso do mesmo celular para chantagear o dono do Silk Road e várias men-

14 Mercado negro que operava via Rede TOR na DarkWeb e vendia produtos ilícitos, como drogas e armas.

sagens suspeitas trocadas entre os envolvidos, os dois agentes da polícia americana foram presos em abril de 2015.



Fonte: Disponível em: <http://www.bitcoinforensics.it/2015/04/bitcoin-forensics-silk-road/>.

9 O caso do *ransonware*[15] Wannacry[16]

Gallagher (2017), editor da Ars Technica, explica que os bitcoins acumulados pelo ataque do *ransonware* Wannacry foram parcialmente resgatados pelos desenvolvedores do vírus.

O Wannacry foi responsável pela onda de infecções em maio de 2017, exigindo o pagamento de bitcoins pelas vítimas, para obter o acesso aos seus arquivos. Esse golpe

15 Tipo de malware que sequestra dados de um computador e comumente pede o resgate em bitcoins.

16 Software malicioso que atacou equipamentos com Windows e pediu resgate em bitcoins para devolver o acesso aos documentos pessoais da vítima.

coletou cerca de 70 mil BTC que foram rastreados com a ajuda de um "*bot*[17]" desenvolvido por Quarts Keith Collins.

Para retirar esses valores, os criminosos utilizaram um "mixer bitcoin", ou seja, um serviço de lavagem de bitcoins para tentar esconder rastros das transações.

No processo de investigação, as autoridades tiveram a colaboração da corretora de bitcoins ShapeShift e da empresa de rastreamento Elliptic, que informou que boa parte dos bitcoins estão sendo transformados na moeda monero[18], mais difícil de ser rastreada.

Ainda de acordo com Khandewal (2017), mais de 95% de todos os pagamentos da bitcoin para *ransomware* foram transferidos via BTC-e, um serviço de lavagem de dinheiro que teve seu criador preso recentemente.

10 *Blockchain* não é só bitcoin

Qualquer aplicação que dependa de processos de monitoramento e localização podem tirar partido da tecnologia *blockchain*.

A arquitetura distribuída assegura a qualidade das transações, o armazenamento e o carimbo de data e hora para qualquer tipo de dado. Além dessas características, soma-se a inviolabilidade dos registros que garantem segurança para aplicações da indústria e do mercado.

Conforme explica o Computerworld (2016), podemos identificar as seguintes aplicações para o *blockchain*:

* ***Pagamentos***: além das tradicionais criptomoedas, os próprios bancos já enxergam a tecnologia como parceira, garantindo que os seus parceiros possuam a capacidade de cumprimento e permitindo a concretização das transações em tempo reduzido. Bancos como o UBS, o Santander e o Santander Chartered investem no projeto "Utility Settlement Coin", que lhes permite fazer transferências, em diversas moedas, para bancos como o Deutsche Bank, o BNY Mellon, entre outros.

17 Diminutivo de robô, é um aplicativo que simula ações humanas.

18 É uma criptomoeda sem órgão centralizador, que promete mais privacidade que o Bitcoin.

São os primeiros testes para uma futura solução que concorra com as transferências interbancárias como o Swift[19].

Identificar dispositivos: localizar equipamentos na internet passa a ser um desafio quando fabricantes precisam localizar seus equipamentos na rede. A tecnologia IOT (Internet das Coisas) precisa identificar versões, atualizações, além de controlar episódios de segurança e concessões de acesso. O Departamento de Segurança Interna norte-americano desenvolveu o projecto "*Factom*" para criar um registro temporal desse tipo de equipamento e evitar falsificações e alteração de registros por meio de acessos indevidos.

Certificar certificados: do mesmo jeito que dispositivos podem ser falsificados, qualificações de pessoas, como currículos, precisam ser autenticados. A *Learning Machine* e o *MIT Media Lab* trabalham no projeto "Blockcerts", que tem como objetivo validar diplomas sem necessidade de contatar a universidade.

Contratos inteligentes: alguns pesquisadores já começam a testar a execução automática de cláusulas contratuais via *blockchain*. A indústria musical pode registrar uma faixa de música nessa rede, e a cada execução receber o pagamento instantâneo de direitos autorais.

11 Conclusão

Se não bastassem as inúmeras dificuldades enfrentadas pelas autoridades no combate aos crimes cibernéticos, o surgimento das criptomoedas chama a atenção e se torna um novo desafio de crime que envolve a alta tecnologia.

A moeda virtual passa a ser um artifício para operações de fraude, extorsão, tráfico de drogas e lavagem de dinheiro, oferecendo um mínimo de anonimato e segurança para os criminosos.

Se os criminosos se utilizam de técnicas não legalizadas de lavagem de bitcoins, incluindo esse serviço de maneira nativa, como em moedas como Dash, Zerocoin e Coakcoin, por outro lado existem meios de rastrear utilizados pelas autoridades.

19 Sistema internacional que controla a transferência de fundos entre bancos.

Ferramentas como o "*Wallet Explorer", Reactor, Elliptic e ChainAnalysys* analisam a estrutura do *blockchain*, permitem localizar movimentos suspeitos e localizar rastros de criminosos. Equipamentos apreendidos acionam a ciência forense, como na ferramenta *Bitminer*, que recuperou informações sobre a mineração de moedas e até mesmo sobre aplicações de carteira virtual. Sem deixar de listar a *Multibit*, *o Bitcoin-QT, o Encase 6.19.7, Tableau, Internet Evidence Finder e Winen.exe* para coletas de memória.

As mesmas técnicas para rastrear imagens criminosas, notadamente de pornografia infantil, criadas para rastrear as redes P2P, já foram migradas para as redes de *blockchain*, permitindo monitorar e conhecer os hábitos de usuários de criptomoedas[20].

Da mesma maneira que provar a propriedade de bitcoins desafia investigadores, a descoberta de uma identidade de um criminoso cibernético pode revelar não só o crime foco daquela investigação, mas todo o seu histórico de delitos. O *blockchain* não diferencia transações legais das ilícitas, tudo está registrado em seu extenso livro de registros digital.

A tecnologia sempre trabalha para os dois lados, cada novo problema requer forças para evoluir o sistema, tanto do lado das autoridades quanto dos criminosos. E sempre podemos contar com o erro humano, principalmente no lado do criminoso.

Criar estruturas que garantam nossa privacidade, mas que também façam a proteção dos crimes digitais é o desafio da nossa geração.

Referências

ALECRIM, Emerson. **Agora temos o Bitcoin e a o Bitcoin CASH**. Disponível em: <https://tecnoblog.net/220271/bitcoin-cash-bcc-oficial/>. Acesso em: 19 set. 2017.

ANTONOPOULOS, Andreas M. **Mastering Bitcoin** – unlocking digital cryptocurrencies. O'Reilly Media, 2015.

BACK, A. **Hashcash**: a denial of service counter-measure. 2002.

BUNTINX, J. P. **Bitcoin Hot Wallet vc Cold Wallet**. Disponível em: <https://themerkle.com/bitcoin-hot-wallet-vs-cold-wallet/>. Acesso em: 22 set. 2017.

COMPUTERWORLD. **5 atuais aplicações empresariais do blockchain**. Disponível em: <https://www.computerworld.com.pt/2016/12/15/5-actuais-aplicacoes-empresariais-de-blockchain/>. Acesso em: 10 set. 2017.

CRAWFORD, Douglas. **Buying Bitcoins to pay for VPN anonymously, a step by step guide. 2013**. Disponível em: <https://www.bestvpn.com/buying-bitcoins-pay-vpn-anonymously-step-step-guide-part-4-bitcoin-mixers-optional/>. Acesso em: 10 set. 2017.

CRYPTOCOINSNEWS. **How a Bitcoin Transaction Works**. Disponível em: <https://www.cryptocoinsnews.com/bitcoin-transaction-really-works/>. Acesso em: 10 set. 2017.

20 Disponível em: <https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf>.

DEEPDOTWEB. **Introducing Grams Helix**: Bitcoins Cleaner. Disponível em: <https://www.deepdotweb.com/2014/06/22/introducing-grams-helix-bitcoins-cleaner/>. Acesso em: 10 set. 2017.

GALLAGHER, Sean. **WannaCry operator empties Bitcoin wallets connected to ransomware**. Disponível em: <https://arstechnica.com/gadgets/2017/08/wannacry-operator-empties-bitcoin-wallets-connected-to-ransomware/>. Acesso em: 1º set. 2017.

HEILMAN, Ethan et al. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In: USENIX SECURITY SYMPOSIUM, 24., 2015, Boston. **Proceedings**... Boston University, 2015, p. 129-144.

KHANDELWAL, Swati. **How Hackers Cash Out Thousands of Bitcoins Received in Ransomware Attacks**. 2017. Disponível em: <http://thehackernews.com/2017/07/cashout-bitcoin-ransomware.html>. Acesso em: 20 ago. 2017.

NOVETTA, White. **Survey of Bitcoin Mixing Services**: tracing anonymous bitcoins. 2015. Disponível em: <http://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WPW_9182015.pdf>. Acesso em: 22 set. 2017.

STEPHENS, Lea Stella. **Cold Wallet Vs. Hot Wallet**: what´s the difference. Disponível em: <https://medium.com/dash-for-newbies/cold-wallet-vs-hot-wallet-whats-the-difference-a00d872aa6b1>. Acesso em: 21 set. 2017.

SAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer eletronic cash system. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 14 set. 2017.

SOFTPEDIA. **Federal Agents Accused of Stealing Silk Road Bitcoins. 2015**. <http://news.softpedia.com/news/Federal-Agents-Accused-of-Stealing-Silk-Road-Bitcoins-477166.shtml>. Acesso em: 10 set. 2017.

WIKIPÉDIA. Disponível em: <https://pt.wikipedia.org/wiki/Minera%C3%A7%C3%A3o_de_Bitcoin>. Acesso em: 1º set. 2017.

CRIMES CIBERNÉTICOS

4 AGENTE INFILTRADO VIRTUAL

Jaqueline Ana Buffon[1]

Resumo: A cibercriminalidade trouxe a necessidade de adaptação dos ordenamentos jurídicos, com a inovação progressiva na legislação relativa aos instrumentos e mecanismos adequados de investigação para fazer frente aos novos meios de cometimento de determinados delitos e de inovadoras condutas delituosas que surgem com o mundo cibernético. O agente infiltrado virtual é uma dessas formas de investigação fundamentais à identificação e apuração no cibercrime. A ação do policial infiltrado será delimitada pela decisão judicial que a autorizar. Importante destacar a diferença das ações de ciberpatrulha em redes abertas e em relação ao agente infiltrado propriamente dito, que ocorre em redes fechadas, e que necessita de autorização do Juízo, que exclui a culpabilidade dos ilícitos cometidos, atendidos seus limites.

Palavras-chave: Agente infiltrado virtual. Cibercrime. Prova digital. Evidências Digitais. Ciberespaço. Policial infiltrado. Investigação criminal no mundo digital. Agente provocador. Ação controlada. Infiltração virtual. Infiltração de agentes.

Abstract : *Cybercrime has created the need of adapting the legal system, since a progressive innovation in procedures concerning proper investigation tools and mechanisms is necessary in order to face the new means of committing criminal offenses and the new criminal behaviours that have appeared in the cybernetic environment. The Virtual Undercover Agent is one of those key investigation procedures to identify and investigate cybercrimes. The actions of the undercover police agent will be authorized and delimited by a court order. It is important to highlight the difference between cyberpatrols' actions in open networks, and the actions of the undercover agent itself in restricted networks, since the latter need to have a Court permission that will remove the guilt in illicit acts commited, within the limits defined.*

Keywords: Virtual undercover agent. Cybercrime. Digital evidence. Cyberspace. Undercover agent. Criminal investigation in cyberspace. Agent provocateur. Sting operation. Intelligence gathering in open sources. Controleed action.

1 Jaqueline Ana Buffon é bacharel em Direito pela Universidade Federal do Rio Grande do Sul, procuradora da República e membro do Grupo de Apoio sobre Criminalidade Cibernética (Gacc), da 2ª Câmara de Coordenação e Revisão do Ministério Público Federal.

1 Introdução - Necessidade de novas ferramentas de investigação diante do uso da internet como meio ou fim para cometimento de delitos

Atualmente a internet constitui um dos modos mais comuns de praticar condutas delitivas. Essa realidade decorre das características do meio cibernético que acabam resultando em dificuldades na investigação, motivando os delinquentes a fazerem uso de novo meio para executar seus objetivos delitivos. Dentre essas características pode-se destacar:

a. *anonimato* – o uso sofisticado do ciberespaço e das Tecnologias de Informação e Comunicação (TICs) muitas vezes possibilita um anonimato que resulta em maiores dificuldades de investigação, especialmente quando se utilizam da *Dark Web*[2], por meio da ferramenta *The Onion Router*[3] ou outras.
b. *âmbito geográfico* – necessidade de uma eficaz cooperação internacional para se obter êxito nas investigações, considerando a diversidade de locais entre a execução da ação ilícita e (o)s resultado(s), além da utilização de servidores em locais que podem ser considerados "paraísos virtuais";
c. *custo/benefício do meio empregado* – a comunicação imediata que o meio proporciona, não existindo fronteiras físicas para a execução. O alcance e a propagação ocorrem num tempo extraordinário por um custo mínimo.

Com esse novo quadro, novas técnicas de investigação passaram a ser necessárias. Os tradicionais métodos são insuficientes e, muitas vezes, ineficazes para o enfrentamento do cibercrime. Diante das novas formas de delinquência e dos novos meios de cometer também aqueles crimes que já existiam, *o agente infiltrado virtual passa a ser uma ferramenta fundamental para o êxito na persecução da delinquência que faz uso da tecnologia.*

2 Conceito de agente infiltrado virtual

Nossa legislação não apresenta um conceito exato para o agente infiltrado virtual. Assim, faz-se aqui uma breve análise de outros ordenamentos jurídicos quanto ao tema, a fim de se chegar à definição dessa ferramenta de investigação.

2 É uma rede mais privativa e anônima da Deep Web ou internet profunda.

3 SILVA, Ângelo Roberto Ilha da et al. (Org.). **Crimes cibernéticos:** racismo, cyberbullying, deep web, pedofilia e ponografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017, p. 258.

2.1 Um pequeno histórico

2.1.1 Internacionalmente

Inicialmente, verifica-se que o Parlamento Europeu e o Conselho 158 dispõem na Diretiva 2014/41/UE[4], em seu art. 29, sobre as investigações realizadas por agentes infiltrados ou com uma identidade falsa.

Na Espanha, inicialmente, no art. 282 bis, da Lei Orgânica nº 5/1999, modificado com a LO nº 15/2003[5], eram necessários dois requisitos para o uso de agente infiltrado: a) investigação estar relacionada com atividades da delinquência organizada; e b) que esses crimes estivessem na lista taxativa constante no item 4 daquele artigo.

Entretanto, diante do uso das novas tecnologias para o cometimento de delitos, houve uma grande evolução na legislação espanhola, com a entrada em vigor da Lei nº 13/2015[6], que permite, atualmente, utilizar agente infiltrado em investigações de crimes não cometidos por organização criminosa e estendendo a muitos outros delitos, não somente entre aqueles que estavam lá nominados.

Assim, com a Lei nº 13/2015, a legislação espanhola trouxe dois novos parágrafos ao art. 282 bis, possibilitando uma melhor ação para as novas demandas no enfrentamento aos crimes cibernéticos, quando acrescenta dois novos tópicos:

> 6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.
>
> El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

4 EUROPA. **Diretiva 2014/41/UE**. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2014.130.01.0001.01.POR&toc=OJ:L:2014:130:TOC>. Acesso em: 24 out. 2017.

5 ESPANHA. **Ley Orgánica 15/2003**. Disponível em: <https://www.boe.es/buscar/doc.php?id=BOE-A-2003-21538>. Acesso em: 24 out. 2017.

6 ESPANHA. **Ley Orgánica 13/2015**. Disponível em: <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725>. Acesso em: 24 out. 2017.

> 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.

Na legislação argentina, com o advento da Lei nº 24.424/1995,[7] o agente infiltrado já podia ser usado nas investigações, desde que atendendo a alguns limites, como o de não existirem outros meios para atingir a finalidade da investigação. Além disso, a exclusão da culpabilidade não abarcava a ação do agente infiltrado que resultasse em crime provocador de grave risco à vida ou à integridade física de indivíduo ou que causasse grave sofrimento físico ou moral a outras pessoas.

Após analisar a legislação de vários países quanto ao tema, constata-se que há um consenso quanto a algumas condições referentes à utilização da figura do agente infiltrado[8]:

a. a infiltração ocorre em uma rede de delinquentes;
b. há a ocultação da verdadeira identidade do agente infiltrado; e
c. na maioria dos países existe a condição de agente estatal do indivíduo que se infiltra.

2.1.2 No Brasil

Em nosso país, a infiltração policial, inicialmente, aplicava-se somente a questões relativas a entorpecentes, quadrilha ou bando, associação ou organização criminosa, conforme a Lei nº 11.343/2006 e anteriores[9].

Com a Lei nº 12.850/2013, novos crimes passaram a abarcar a ferramenta para a busca da autoria e materialidade delitiva, quais sejam: (a) organizações criminosas enumeradas no art. 1º, § 1º; e (b) as situações previstas no § 2º, ambos da mesma lei.

7 ARGENTINA. **Ley 24.424**. Disponível em: <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/800/norma.htm>. Acesso em: 18 jan. 2018.

8 ZARAGOZA, Tejada. El agente encubierto online: la última frontera de la investigación penal. **Revista Aranzadi Doctrinal**, n. 1/2017, parte Tribuna; Editorial Aranzadi, S.A.U., Cizur Menor. 2017.

9 Anteriormente, Lei nº 10.217/2001 e Lei nº 10. 217/2001 tratavam do tema.

O § 2º[10] permitiu a realização de investigações no mundo virtual, em escala internacional, especialmente quanto aos crimes relacionados à pornografia infantil[11], quando acrescentou:

> I - às infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
> II - às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos.[12]

A grande inovação dessa lei é a não exigência da existência de organização criminosa para permitir o uso da infiltração policial, desde que se referissem aos delitos tratados no § 2º. Fundamental essa abertura legal, já que no mundo virtual muitos delinquentes costumam usar o mesmo ambiente, como um Fórum, por exemplo, o que não significa, necessariamente, que estão agindo sob organização. Inúmeras vezes, como em crimes de compartilhamento de imagens com pornografia infantil, os usuários infratores agem individualmente, por sua conta e risco, sem qualquer combinação entre si.

Em maio de 2017, surge a Lei nº 13.441/2017, que acrescenta a Seção V-A à Lei nº 8.069/1990 – Estatuto da Criança e Adolescente –, a qual trata especificamente de infiltração virtual de agentes policiais.

A Lei nº 13.441/2017 enumera taxativamente a quais crimes se refere, quais sejam, arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A, e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

Cabe ter bem claro, no entanto, que a *infiltração virtual*, diante dos regramentos anteriores, possuía albergado seu uso no Brasil muito antes da última lei publicada[13], na qual, pela primeira vez, houve referência expressa à aplicação no mundo digital.

10 BRASIL. 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. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 5 ago. 2013. Edição Extra. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm>. Acesso em: 22 out. 2017.

11 Operação Darknet que deflagou a primeira fase em 2014 e segunda, em 2016.

12 A redação do inciso II restou assim alterada com a Lei nº 13.260/2016.

13 BRASIL. Lei nº 13.441, de 08 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 9 maio 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm>. Acesso em: 22 out. 2017.

Apesar da referência em *numerus clausus* feita na legislação de 2017, ressalta-se que continuam aplicáveis as Leis nº 11.343/2006 e nº 12.850/2013, nos crimes que lá se referem, com exceção dos crimes contra a dignidade sexual da criança e de adolescente, já que existe a nova lei específica para tais crimes.

Para a análise das legislações acima e suas implicações em nossas investigações virtuais, passa-se a abordar alguns aspectos fundamentais.

3 Atuações Investigativas no Mundo Digital

3.1 *Ciberpatrulha*[14]: em comunidades abertas

Com a chegada das novas Tecnologias de Informação e Comunicação (TICs) houve grande mudança na vida das pessoas. A agilidade e demais facilidades provocaram – e continuam provocando – novos hábitos e rotinas que melhoraram a vida das pessoas. Por outro lado, a falta de cuidados no uso da internet e as vulnerabilidades do meio cibernético permitem também que os mal-intencionados busquem suas vítimas de forma mais fácil e rápida.

Surge assim a necessidade de cada usuário do mundo digital conhecer meios de se precaver e aplicar tais conhecimentos.

O Estado, da mesma forma, necessita fazer a prevenção do delito no meio virtual como existe no meio físico. Emerge, então, a possibilidade da *ciberpatrulha*, que consiste na averiguação dos crimes em locais virtuais públicos. O agente que faz investigações ou buscas em redes abertas, que podem ser feitas diretamente, de forma autônoma, ou com o uso de procedimentos mecânicos, não necessita de autorização judicial[15]. Obviamente que essa *ciberpatrulha* não permite ações por parte do agente, o que poderá ser feito, num segundo momento, após análise e decisão do Juízo em relação ao agente infiltrado, suas características, permissões e exclusões de culpabilidade.

14 TEJADA, Javier Ignacio Zaragoza Tejada. El agente encubierto online: la última frontera de la investigación penal. **Revista Aranzadi Doctrinal**, n.1/2017, parte Tribuna. Editorial Aranzadi, S.A.U., Cizur Menor. 2017.

15 REALPE, Germán. **Fuentes abiertas:** herramientas para hacer inteligencia em la red. Disponível em: <http://www.enter.co/chips-bits/seguridad/herramienta-inteligencia-internet/>. Acesso em: 19 jan 2018.

Na Espanha, muito antes das alterações legislativas ocorridas em 2015, no art. 282 *bis*[16], já era aceita essa possibilidade, como se constata na decisão do Tribunal Supremo 767/2007[17], de 3 de outubro:

> Efectivamente, lo cierto es que los agentes de la autoridad, cuando realizan las labores habituales de vigilancia para prevenir la delincuencia informática tuvieron noticia casual de la existencia de un posible delito de difusión de pornografía infantil. Realizaron las investigaciones oportunas y, sólo cuando tuvieron la convicción de estar efectivamente en presencia de hechos presuntamente delictivos, confeccionaron el oportuno atestado que remitieron a la Fiscalía de la Audiencia Provincial donde se instruyeron las pertinentes diligencias informativas y, acto seguido,tras la denuncia en el Juzgado de Instrucción, las Diligencias Previas. Tal método de proceder es absolutamente correcto y ninguna objeción puede merecer.

Para o êxito de uma investigação, na maioria das vezes, é necessário o uso concomitante dos dois ambientes a fim de obter a autoria e materialidade dos delitos. O cruzamento de informações entre redes abertas e fechadas, inclusive com informações obtidas na rede TOR[18], pode ser decisivo no esclarecimento dos delitos que ocorrem no mundo virtual. Portanto, é possível ser necessária a devida decisão judicial para o uso do meio da infiltração policial propriamente dita, após a descoberta, em ação de *ciber-patrulha*, de indícios de materialidade e autoria, que necessitem de acessos em redes fechadas, para esclarecimento e alcance dos fatos e delimitação dos responsáveis pela atividade ilícita.

Diante do art. 190-C, da Lei nº 13.441/2017, alguns podem ter dúvidas em relação à necessidade de autorização judicial quando o investigador se utiliza de pseudônimos ou *nicks* de fantasia em averiguações em redes abertas. Contudo, não há qualquer empecilho diante das características daquele meio na internet.

Ao analisar sob outro ângulo, apenas por usar um nome fantasia, em ambientes virtuais que não necessitem de aceitação para ingresso, por parte de outro(s) usuário(s) anterior(es)

16 ESPANHA. **Ley de Enjuiciamiento Criminal.** Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em: 24 out. 2017.

17 ESPANHA. Tribunal Supremo. **Sentencia nº 767/2007** de TS, Sala 2ª, de lo Penal, 3 de Octubre de 2007. Disponível em: <https://supremo.vlex.es/vid/facilitacion-pornografia-infantil-p-31969904>. Acesso em: 22 out. 2017.

18 SILVA, Ângelo Roberto Ilha da et al. (Org.). **Crimes cibernéticos:** racismo, cyberbullying, deep web, pedofilia e ponografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017, p. 258.

daquele espaço, não há que se falar em necessidade de autorização do juiz, pelo simples fato de que quem usa o mundo digital já está ciente de que não pode ter certeza de quem está do outro lado. A *contrario sensu*, seria exigido um requisito ao investigador que não o é aos demais usuários. Portanto, a regulamentação do agente infiltrado veio tratar das redes fechadas.

3.2 Agente infiltrado virtual: redes fechadas

As redes fechadas passaram a ser um ambiente muito atraente aos criminosos, já que o desenvolvimento das tecnologias propicia soluções que facilitam o cometimento dos delitos.

O Serviço Europeu de Polícia (Europol)[19] menciona situações que, certamente, ocorrem em inúmeros lugares do mundo, a todo o momento, quando trata de exploração sexual infantil:

> Peer-to-peer (P2P) networks and anonymised access like Darknet networks (e.g. Tor). These computer environments remain the main platform to access child abuse material and the principal means for non-commercial distribution. These are invariably attractive for offenders and easy to use. The greater level of anonymity and the strong networking possibilities offered by hidden internet that exists beneath the "surface web" appear to make criminals more comfortable in offending and discussing their sexual interests.
> Live-streaming of child sexual abuse. Facilitated by new technology, one trend concerns the profit-driven abuse of children overseas, live in front of a camera at the request of westerners.
> To a lesser degree, there is also some evidence that forms of commercial child sexual exploitation such as on-demand live streaming of abuse is also contributing to the rise of the amount of CSEM online.

No Brasil houve uma grande investigação pela primeira vez realizada na *deep web*, utilizando-se de ferramenta inédita criada pela Polícia Federal, chamada Operação Darknet[20], em que foram identificados centenas de usuários compartilhando vídeos e fotos de pornografia infantil.

19 EUROPA. **Child Sexual Exploitation.** Disponível em: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>. Acesso em: 18 jan. 2018.

20 Disponível em: <http://www.mpf.mp.br/rs/sala-de-imprensa/noticias-rs/mpf-rs-atua-na-segunda-fase-da-darknet-no-combate-a-pornografia-infantil-e-juvenil>. Acesso em: 19 jan. 2018.

Ao acessar redes fechadas, é necessário um convite e/ou a conquista da confiança por parte dos usuários daquele ambiente virtual. Assim, resta demonstrada a importância do agente infiltrado on-line, o qual deverá estar atento à observância de todos os limites que a lei impõe, para se obter uma prova válida. Um dos grandes motivos para tal exigência são as peculiaridades relativas aos direitos da privacidade de comunicação que devem ser sopesados pelas autoridades competentes, no espaço cibernético de redes fechadas, como bem menciona o membro do Ministério Público Espanhol Javier Ignacio Zaragoza Tejada (2017, p. 8) que:

> [...] el agente encubierto informático va más allá. Tiene por objeto actuar em canales cerrados de comunicación, es decir, en foros privados de internet en los que intervienen una pluralidad de internautas intercambiando expresiones, opiniones o archivos ya sean de carácter lícito o ilícito. Es decir, supone, en sí mismo, la infiltración de un agente de las fuerzas y cuerpos de seguridad del estado en un foro de carácter privado, donde va a proceder a observar las comunicaciones mantenidas entre los diferentes miembros del mismo lo que conlleva una actuación intromisiva en el derecho al secreto de comunicaciones. Por eso mismo, a diferencia de agente encubierto convencional que cuando en el curso de una actuación de investigación desarrollada bajo dicha figura, se consideraba necesario acordar una medida de intervención de comunicaciones era exigible una resolució judicial independiente, no ocurriría lo mismo con el agente encubierto informático en el que la propia naturaleza del mismo llevaría implícita la posibilidad de que se lleven a cabo acciones vulneradoras del derecho al secreto de comunicaciones reconocido en el artículo 18 de nuestro texto constitucional siempre y cuando estas se refirieran, claro está, a las comunicaciones mantenidas en abierto dentro de dicho canal cerrado de comunicación y no, como es obvio, respecto a las conversaciones privadas mantenidas entre los miembros de dichos canales ya sea dentro o fuera del mismo. (TEJADA, 2017, p. 8)

Muitos desses ambientes têm por objetivo não só o cometimento de infrações penais mas também a troca de ensinamentos aos demais criminosos de como devem agir em suas ações para que possam obter êxito em suas empreitadas criminosas. Esses verdadeiros "manuais do crime" geralmente encontram-se na *deep web*, pelo caráter de proteção que o anonimato daquele meio digital proporciona aos seus usuários.

Nesse sentido, também verifica-se constatação da Europol quando menciona a existência de troca de experiência entre os delinquentes: "Networking and forensic awareness of offenders. Offenders learn from the mistakes of those that have been apprehended by law enforcement."[21]

3.3 Requisitos para uso do agente infiltrado virtual (AI)

Como já mencionado anteriormente, a ampliação do uso das novas tecnologias e os seus benefícios trouxeram consigo a necessidade de serem adotadas novas medidas na luta contra o crime, já que os métodos tradicionais não mais se prestavam para esclarecimento dos fatos ilícitos. No Brasil, ainda são lentas e tímidas as inovações legislativas na área, considerando a realidade virtual que vivemos e os passos já dados por outros países, mais preocupados com a temática.

Inicialmente serão tratados os seguintes requisitos gerais aplicáveis ao agente infiltrado (AI), independentemente de qual das três legislações mencionadas acima (item 2.1.2) seja o fundamento legal para obtenção da autorização judicial: (a) indícios de crime, os quais podem ser identificados, inclusive, em redes abertas; e (b) inexistência de outro meio possível à obtenção das provas necessárias.

Quando se trata de crimes cometidos na *Dark Web*, é praticamente impossível a identificação por outro meio que não utilize de AI. Segundo Adriana Shimabukuro e Melissa Garcia Blagitz de Abreu e Silva (2017, p. 256-258), *"Essas páginas só podem ser acessadas com softwares específicos para navegação em ambientes criptografad os e anônimos, como TOR, invisible Internet Projetct (i2p) e FreeNet."*

Destaca-se, também, que o anonimato oferecido por essas redes prejudica por demais a investigação e é o que motiva a grande quantidade de novos usuários.

Importante aqui, portanto, tratar do funcionamento da rede The Onion Router (TOR), ferramenta gratuita, a qual provoca enorme dificuldade na identificação dos autores que a utilizam para o cometimento de crimes.

De acordo com Adriana Shimabukuro e Melissa Garcia Blagitz de Abreu e Silva (2017, p. 258):

21 EUROPA. **Child Sexual Exploitation.** Disponível em: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>. Acesso em: 18 jan. 2018.

> A mensagem original é criptografada e segue para o destino "através de uma sequência de proxies (roteadores cebola), que reencaminham as mensagens por um caminho imprevisível", passando por ao menos 3 servidores diferentes. (Carvalho, 2010).
>
> Os milhões de nós disponíveis na Internet são localizados pelo aplicativo TOR aleatoriamente, o que dificulta a espionagem, garante uma conexão privada e não deixa rastro, porque nenhum dos nós sabe da origem ou do destino da solicitação.
>
> A criptografia impede que algum atacante espione o conteúdo da mensagem. Uma das vantagens do *union routing* é que não é necessário confiar em cada roteador da rede: mesmo que um ou mais equipamento sejam violados, ainda é possível a comunicação segura, pois cada roteador da TOR aceita as mensagens, recriptografa-as e as transmite para o próximo ponto sem poder modificá-las ou acessar seu conteúdo.
>
> Apenas o primeiro e o último nós da comunicação não são criptografados: todos os nós no meio da cadeia são criptografados e recebem informações apenas do nó imediatamente anterior e encaminham o conteúdo para o nó imediatamente posterior, sem ter conhecimento da verdadeira origem e destino da mensagem. (SHIMABUKURO; ABREU E SILVA, 2017, p. 258)

Também para a análise do requisito mencionado no item (b) acima, devem estar demostradas, no requerimento do Ministério Público ou do delegado de Polícia, as circunstâncias que demostrem a inexistência de outro meio possível, ou seja, a imprescindibilidade de tal via para a identificação da autoria e/ou materialidade, bem como que restará infrutífera a continuidade das investigações sem o uso do AI.

3.4 Limites das ações do agente infiltrado virtual

O art. 190-A, I, da Lei nº 8.069/1990, introduzido pela Lei nº 13.441/1990, estabelece que a decisão judicial estabelecerá os limites para obtenção da prova, após ouvir o Ministério Público.

Esses limites estabelecidos na decisão judicial serão fundamentais para a fiscalização, por parte do juiz e do Ministério Público, quanto às ações realizadas pelo AI, no meio digital, a fim de estabelecer: (a) a legalidade da prova obtida; e (b) a verificação das ações do AI abrangidas pela excludente de culpabilidade.

O compartilhamento de material contendo pornografia infantil não está explícito na lei. No entanto, não há como se excluir tal possibilidade diante das características do meio virtual em que os delinquentes mais agem, ou seja, as redes fechadas, local em que se sentem mais protegidos. Maior ainda essa necessidade quando os criminosos estão agindo na *Dark Web*, considerando as enormes dificuldades de investigação trazidas pelo elevado grau de anonimato.

Bem menciona o membro do Ministério Público espanhol Luis Lafont Nicuesa (2015, p. 9), ao tratar desse tema:

> La posible utilización por el AE informático de material pornográfico en que aparecen menores resulta necesaria para que el agente pueda desplegar su actividad investigadora con eficacia.
> Como expone URIARTE VALIENTE (8) para acceder a un foro privado «se precisa ser previamente invitado lo que únicamente se consigue demostrando el consumo o adicción a dicho material debiendo aportarse previamente pornografía infantil. Además-prosigue el autor …una vez dentro de estos grupos, la actividad de cada miembro es controlada por el grupo, exigiéndole una actitud activa para poder continuar en el mismo, como suele ser el intercambio periódico de pornografía infantil. (NICUESA, 2015, p. 9)

O objetivo desses usuários de redes fechadas é exatamente a preservação de suas identidades e de suas atividades, evitando que investigadores lá ingressem. Como diz o membro do Ministério Público Espanhol Javier Ignacio Zaragoza Tejada (2017, p. 9), "[...] *este compartilhamento é dito pelos delinquentes como uma pessoal implicação na atividade ilícita que nesse espaço é levado a efeito.*"

Assim, quando ocorre o envio dos arquivos ilícitos, por razões de seu conteúdo, gera uma confiança do(s) delinquente(s) em relação ao AI, o que permite a continuidade das atividades criminosas que já se perpetuavam naquele ambiente virtual, muito antes do ingresso do investigador.

Salutar, no entanto, alguns *cuidados fundamentais que se deve ter ao escolher o vídeo ou imagem a ser compartilhada, a fim de restar atendido o objetivo da norma e princípio da necessidade e proporcionalidade*, tais como: (a) observância da idade da vítima, excluindo materiais que contenham crianças de faixas etárias menores e que contenham cenas sexualmente explícitas; (b) usar, se possível, filtros que transformem em imagens gráficas ou projetadas por computador que diminuam a exposição ao mínimo; (c) além desses já cita-

dos, ter a cautela de que o arquivo já estava sendo usado na internet para tais objetivos, não resultando em novidade no mundo digital.[22]

Assim, considerando a gravidade das atividades que serão desenvolvidas pelo AI nos grupos fechados, reiteramos a necessidade de estarem bem demonstrados os princípios da necessidade e proporcionalidade para o uso de tão extrema medida. Conforme Javier Ignacio Zaragoza Tejada (2017, p. 9):

> En ocasiones, para lograr la infiltración en determinados canales privados de comunicación de carácter delictivo no basta con que un agente estatal se inscriba o de alta en el mismo actuando bajo una identidad diferente a la verdadera o bajo un determinado nick o pseudonimo de fantasía. La gravedad de las actividades delictivas que se desarrollan en dichos foros, unidas al interés de sus usuarios en preservar su verdadera identidad frente a las actuaciones de rastreo o de investigación realizada por las fuerzas policiales, hace que se adopten algunas medidas adicionales de seguridad a fin de prevenir, precisamente, la infiltración de los mismos. Así, por ejemplo, es habitual que em determinados foros de pornografía infantil, de ciberyihadismo, o aquellos relacionados con la planificación y ejecución de ataques a sistemas informáticos se condicione el acceso al mismo a la previa invitación de alguno de sus miembros e incluso a la aportación de material ilícito (material pedófilo, de apología del terrorismo etc.) como expresión de una personal implicación en la actividad ilícita que en ese espacio se lleva a efecto.

3.5 Especificidades da ação controlada durante a infiltração policial

Para o AI obter a identificação de autoria e materialidade dos usuários delinquentes, possivelmente será necessário um tempo considerável, a fim de, em momento posterior, serem executados mandados de busca e apreensão, preferencialmente, no mesmo dia em todo país, não frustrando o trabalho, já que a comunicação na internet é instantânea e pode gerar comprometimento em obter a mídia que irá fortalecer a prova dos crimes detectados. Durante esse tempo em que forem colhidas as provas, haverá um período de ação controlada, quando se retarda a intervenção policial ou administrativa, mas em acompanhamento

22 NICUESA, Luis Lafont. El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal. **Diario La Ley**, n. 8580, 2015, Sección Doctrina, Editorial LA LEY 10 jul. 2015. Ref. D-278, ISSN 1989-6913.

constante para que a prova seja buscada no tempo mais adequado para o sucesso das investigações.[23]

Quando se estiver diante de investigações relativas aos crimes de pornografia infantil, os cuidados terão que ser redobrados. Isso porque a análise das imagens e diálogos deverá ser constante e muito cuidadosa, já que podem surgir notícias de possíveis ou reais abusos sexuais com ou sem produção de imagens para posse ou compartilhamento. Nessas situações, apesar da continuação da ação controlada, a fim de se atingir o objetivo proposto, o ideal é a imediata retirada desse(s) alvo(s), com sua remessa ao competente Juízo do local de ocorrência dos delitos, diante do grave perigo à criança ou ao adolescente. Ainda, para não prejudicar o êxito da investigação virtual e a ação controlada consequente, conveniente é um contato direto com as autoridades competentes que receberão o material referente ao(s) investigado(s), explicando a origem e o motivo de não se aguardar o final da ação controlada para a execução do mandado de busca e apreensão em relação àqueles possíveis agressores de menores.

O art. 190-A, § 1º, trata dos relatórios parciais que poderão ser requisitados pela autoridade judicial e pelo Ministério Público durante o período da infiltração virtual. Verifica-se de suma importância a realização desses relatórios parciais, tanto para acompanhar a existência de eventual situação de vulnerabilidade que possa exigir providências urgentes e imediatas, mesmo não se estando ao final da investigação, a exemplo do acima mencionado, como para averiguar se as ações do AI estão atendendo aos limites da decisão judicial. Essa análise contínua é de extrema importância para que se tenha prova lícita. Um trabalho árduo, mas necessário.

3.6 Diferença entre agente infiltrado (AI) e agente provocador (AP)

Há grandes diferenças nas ações do agente infiltrado e do agente provocador. O primeiro está albergado pela lei e com os limites bem determinados pela decisão judicial, enquanto que as ações decorrentes do agente provocador tornarão a prova inválida.

Enumeram-se aqui as principais diferenças entre ambos, quais sejam:

23 BRASIL. Lei nº 12.850, de 2 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. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 5 ago. 2013. Edição Extra. Art. 8º e seguintes. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm>. Acesso em: 22 out. 2017.

3.6.1 Agente Infiltrado:

- objetiva coletar informações – aa observação de um ambiente fechado virtual é essencial para a busca de dados que podem esclarecer ou identificar autoria e/ou materialidade delitiva. A análise de relações entre pessoas e/ou empresas pode ser essencial para o esclarecimento de crimes que usam o meio digital como fim ou como meio para realização de seus fins;

- postura passiva – a ação do agente infiltrado não terá o objetivo de levar o investigado a cometer crimes. Exatamente o oposto. No entanto, importante se ter bem presente que isso não exclui a possibilidade de esse mesmo agente estatal cometer algum ato que se caracterize infração penal, mas tão somente nos limites estabelecidos na decisão judicial;

- obtém a confiança do suspeito – os criminosos possuem muita cautela para permitir o ingresso de um novo integrante em suas redes fechadas. O receio de que seja um investigador faz parte dessa precaução. Decorre, assim, a necessidade de o agente infiltrado ter de ultrapassar tal limite para que possa fazer parte daquele círculo, a fim de coletar as informações necessárias.

- possui participação acessória – como dito acima, o domínio do fato criminoso é uma atividade exclusiva do delinquente. O agente infiltrado deve estar atento às suas funções no ambiente que examina, colhendo as provas e agindo exatamente nos ditames dispostos pelo Juízo.

3.6.2 Agente Provocador:

Diferentemente do agente infiltrado, para se caraterizar o agente provocador são necessárias ações muito diversas, quais sejam:

a. **instigar ou induzir o investigado a executar o crime**[24] - ocorre quando o criminoso não possui motivação própria;
b. **agir com postura ativa**- *agente estatal deflagra o mecanismo causal da infração delituosa*;[25]
c. **possuir o agente policial o domínio final do fato** – ocorre quando o investigador é ator fundamental para a execução do crime.

24 KNIJNIK, Danilo. O "agente infiltrado", "encoberto" e "provocador": recepção, no direito brasileiro, das defesas do entrapment e "da conduta estatal ultrajante" como meio de "interpretação conforme": da Lei 9.034/1995. **Revista dos Tribunais**, ano 93, v. 826, p. 413-427, ago. 2004.

25 BRASIL. Supremo Tribunal Federal. **HC 109703 SP**, Relator: Min. Celso de Mello, Data de Julgamento: 6 abr. 2015, Data de Publicação: Dje-065 8 abr. 2015. Disponível em: <https://stf.jusbrasil.com.br/jurisprudencia/180436138/habeas-corpus-hc-109703-sp-sao-paulo-9952673-1420111000000>. Acesso em: 19 jan. 2018.

As ações do agente provocador terão como consequência a impossibilidade da consumação do delito, exatamente o oposto do resultado obtido pelo agente infiltrado, o qual não interfere na prática do crime. Para haver a nulidade dessa prova, também, há a necessidade, concomitantemente, de o agente provocador ter tomado todas as providências necessárias capazes de tornar impossível o crime.

Constata-se, portanto, que o uso do agente infiltrado é atividade lícita, totalmente albergada pela nossa legislação e pela Constituição brasileira.

4 Conclusão

Apesar de termos no Brasil a ferramenta do agente infiltrado, constata-se ainda muito tímido nosso arcabouço jurídico nesse aspecto.

A realidade mundial tem mostrado a necessidade de conscientização dos órgãos competentes para o estudo, aprofundamento e ampliação das formas de enfrentamento aos crimes cibernéticos, área muito demandada com a abrangência do uso das TICs.

Nosso país carece, com urgência, de melhorar a legislação em relação ao tema. Um dos aspectos é a extensão do uso do agente infiltrado a muitos outros crimes igualmente graves.

A preocupação quanto à cibersegurança e à cibercriminalidade é mundial. A comissão Europeia, *"em 13 de setembro de 2017, propôs um pacote de reforma da cibersegurança"*, pois *"A "Internet das coisas" é já uma realidade, esperando-se que, até 2020, haja dezenas de milhares de milhões de dispositivos digitais conectados."*[26]

Existem muitos comportamentos criminosos no mundo digital que necessitam ser detectados e investigados, portanto, as redes abertas e as redes fechadas devem ser objeto de análise, a fim de possibilitar um resultado eficaz na identificação de materialidade e autoria delitiva, bem como devem-se utilizar outras formas de investigação. No entanto, destaca-se que cada ambiente on-line possui características que devem, necessariamente, ser observadas para que haja a devida autorização judicial nos casos necessários, observando os princípios da proporcionalidade e necessidade a fim de se obter uma prova lícita.

Reflexões são necessárias, com as devidas e urgentes reformas. O país teve alguns avanços, mas ainda em passos muito lentos.

26 EUROPA. **Reforma da cibersegurança na Europa**. Disponível em: <http://www.consilium.europa.eu/pt/policies/cyber-security/>. Acesso em: 24 out. 2017.

Referências

BRASIL. Lei nº 12.850, de 2 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. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 5 ago. 2013. Edição Extra. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12850.htm>. Acesso em: 22 out. 2017.

_____. Lei nº 13.441, de 8 de maio de 2017. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 9 maio 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13441.htm>. Acesso em: 22 out. 2017.

BRASIL. Supremo Tribunal Federal. **HC 109703 SP**. Relator: Min. Celso de Mello,Data de Julgamento: 6 abr. 2015, Data de Publicação: Dje-065 8 abr. 2015. Disponível em: <https://stf.jusbrasil.com.br/jurisprudencia/180436138/habeas-corpus-hc-109703-sp-sao-paulo-9952673-1420111000000>. Acesso em: 19 jan. 2018.

ESPANHA. **Ley de Enjuiciamiento Criminal**. Disponível em: <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em: 24 out. 2017.

_____. **Ley Orgánica 15/2003**. Disponível em: <https://www.boe.es/buscar/doc.php?id=BOE-A-2003-21538>. Acesso em: 24 out. 2017.

_____. Tribunal Supremo. **Sentencia nº 767/2007** de TS, Sala 2ª, de lo Penal, 3 de Octubre de 2007. Disponível em: <https://supremo.vlex.es/vid/facilitacion-pornografia-infantil-p-31969904>. Acesso em: 22 out. 2017.

_____. **Ley Orgánica 13/2015**. Disponível em: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725>. Acesso em: 24 out. 2017.

EUROPA. **Child Sexual Exploitation**. Disponível em: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation>. Acesso em: 18. jan. 2018.

_____. **Diretiva 2014/41/UE**. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2014.130.01.0001.01.POR&toc=OJ:L:2014:130:TOC>. Acesso em: 24 out. 201

_____. **Reforma da cibersegurança na Europa**. Disponível em: <http://www.consilium.europa.eu/pt/policies/cyber-security/>. Acesso em: 24 out. 2017.

KNIJNIK, Danilo. O "agente infiltrado", "encoberto" e "provocador": recepção, no direito brasileiro, das defesas do entrapment e "da conduta estatal ultrajante" como meio de "interpretação conforme": da Lei 9.034/1995. **Revistas dos Tribunais**, ano 93, v. 826, p. 413-427, ago. 2004.

NICUESA, Luis Lafont. El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal. **Diario La Ley**, n. 8580, 2015, Sección Doctrina, Editorial LA LEY 10 jul. 2015. Ref. D-278, ISSN 1989-6913.

PACELLI, Eugênio. FISCHER, Douglas. **Comentários ao Código de Processo Penal e sua Jurisprudência**. 9. ed. [S.l: s.n], 2017.

SILVA, Ângelo Roberto Ilha da et al. (Org.). **Crimes cibernéticos:** racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017.

SHIMABUKURO, Adriana; ABREU, Melissa Garcia Blagitz de. Internet, Deep web e Dark web.In: SILVA, Ângelo Roberto Ilha da et al. (Org.). **Crimes cibernéticos:** racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2017.

TEJADA, Javier Ignacio Zaragoza. **El agente encubierto online: la última frontera de la investigación penal.** n.1/2017 Parte Tribuna, Editorial Aranzadi, S.A.U., Cizur Menor. 2017.

5 ASPECTOS JURÍDICOS NO COMBATE E PREVENÇÃO AO *RANSOMWARE*

Fábio Lucena de Araujo[1]

Resumo: A evolução tecnológica fez surgir novos crimes cibernéticos, entre eles o ataque por "*ransomware*". Prática cada vez mais recorrente, em que o criminoso por meio de criptografia, impossibilita o acesso à máquina infectada, cobrando um valor em dinheiro (geralmente em moeda virtual) para liberar o acesso ao usuário. Nesse contexto, o presente artigo tem como objetivo analisar a prevenção e a atuação da polícia judiciária no combate ao "ransomware", discorrendo sobre seus limites jurídicos e observando os mecanismos de cooperação internacional, utilizando-se da pesquisa bibliográfica, bem como da exegese dos diplomas legais.

Palavras-chave: Aspectos jurídicos. Combate e Prevenção. *Ransomware*.

Abstract: *Technological evolution has given rise to new cybercrimes, including the "ransomware attack". Increasingly recurring practice, where the criminal through encryption, makes it impossible to access the infected machine, charging a cash value (usually in virtual currency) to release access to the user. In this context, this article aims to analyze the prevention and action of the judicial police in the fight against "ransomware", discussing its legal limits and observing the mechanisms of international cooperation, using bibliographical research, as well as the exegesis of legal diplomas.*

Keywords: Legal aspects. Combat and Prevention. Ransomware.

1 Introdução

O acesso às novas tecnologias em um mundo cada vez mais conectado têm garantido diversos avanços nas relações sociais e econômicas. Entretanto, toda essa tecnologia também pode ser utilizada para a prática de crimes. Os crimes cibernéticos são uma realidade, várias espécies de crimes se originaram e outros já conhecidos ganharam uma nova roupagem diante do avanço tecnológico.

Neste artigo, trataremos do tema "*ransomware*", chamado popularmente de "sequestro digital" ou "sequestro de dados". Em síntese, trata-se de uma espécie de vírus de computador, em que o cibercriminoso, após conseguir infectar a máquina desejada, por

1 Advogado – graduado em Direito pela Universidade Estácio de Sá (Unesa). Tecnólogo em Gravação e Produção Fonográfica pela Universidade Estácio de Sá (Unesa).

meio de criptografia, impossibilita o acesso à máquina já infectada, cobrando um valor em dinheiro (geralmente em moeda virtual) para liberar o acesso ao usuário.

É de especial relevância o estudo do tema, tendo em vista os prejuízos políticos, econômicos e sociais oriundos de um ataque virtual nesse sentido. O mundo tem assistido ultimamente a uma ameaça crescente desses ataques, o que nos leva a um questionamento imediato. A legislação pátria e as ferramentas de informação são eficientes na prevenção e combate ao *ransomware*?

Nessa esteira, busca-se, com o presente artigo, dissecar o tema, analisando a prevenção e a investigação da polícia judiciária no combate ao *ransomware*, discorrendo sobre seus limites jurídicos e observando os mecanismos de cooperação internacional, bem como na especial exegese da Lei n° 12.737, de 30 de novembro de 2012.

Os ataques dos cibercriminosos têm se expandido dos usuários particulares para as grandes corporações e até mesmo governos. Por meio de diversas táticas, eles têm conseguido grande percentual de sucesso, gerando lucros exorbitantes para essas organizações criminosas. Por consequência, essas ações geram graves reflexos nos campos social, econômico e governamental.

Indubitável a necessidade de uma análise criteriosa sobre o tema, discorrendo sobre a legislação pertinente e a cooperação internacional na busca da prevenção e combate a essa ameaça que põe em risco o mundo inteiro em ataques cada vez mais danosos.

2 *Ransomware*

Chamado comumente de *ransomware*, esse vírus faz parte de uma classe específica de *malwares*[2] que são utilizados nas chamadas "extorsões digitais", pois obrigam suas vítimas a pagarem determinado valor em troca do completo controle de seus dados. Essencialmente, existem duas classes: a *Locker*, que impede que a vítima acesse o equipamento infectado, praticamente inutilizando-o, e a *Crypto*, que bloqueia o acesso aos dados armazenados no equipamento infectado, utilizando criptografia.

2 *Malware* – é a combinação das palavras inglesas malicious e software, ou seja, programas maliciosos. São programas e comandos feitos para diferentes propósitos: apenas infiltrar um computador ou sistema, causar danos e apagar dados, roubar informações, divulgar serviços etc.

Sua origem tem início em 1989, com o nome de "AIDS", criado por Joseph L. Popp, um biólogo com PhD em Harvard. À época, bem menos danoso do que o próprio vírus cujo nome se originou. Esse malware mantinha em seus ataques uma contagem específica de reinicializações do sistema, para posteriormente ocultar todos os diretórios. Entretanto, por conter uma criptografia básica, ele era facilmente removido.

Após um breve período de hibernação, em meados da década de 2000, diante dos novos avanços tecnológicos, da capacidade cada vez maior de processamento dos computadores e diante de formas mais complexas de criptografia, voltaram a aparecer ataques cada vez mais elaborados e diversas variantes de *ransomware*.

Hodiernamente, esses ataques têm se tornado cada vez mais frequentes e tendo como vítimas não só o usuário particular, mas também pessoas jurídicas de direito privado e de direito público. Os cibercriminosos têm expressivo sucesso nesses ataques, conseguindo quantias vultuosas, chegando ao ponto de terceirizar seus vírus na *deep web*[3], no serviço chamado de (RaaS – *Ransomware as a Service*) ou seja: "*Ransomware* como um Serviço", cobrando um percentual sobre os ataques bem-sucedidos. Essas empreitadas se espalham tanto pelos computadores pessoais quanto para os das grandes corporações, seus servidores e até os dispositivos móveis.

Em maio de 2017, o mundo presenciou um dos maiores ataques cibernéticos, o vírus chamado "*WannaCry*", que afetou mais de 150 países fazendo aproximadamente 200.000 vítimas[4]. A maioria dos ataques foram contra empresas, acendendo uma luz de alerta ao mundo sobre a vulnerabilidade dos nossos sistemas. Torna-se deveras preocupante a quantidade de dados confidenciais a que essas organizações criminosas conseguiram ter acesso. E esse é apenas um dos milhares de *malwares* espalhados pela rede.

3 Dinâmica dos ataques

A análise sistemática dos ataques cibernéticos é de extrema importância para o desenvolvimento de mecanismos de defesa, bem como para o aperfeiçoamento legislativo no sentido de combater tais práticas. Percebe-se que o comportamento dos crimi-

3 Deep Web – é o nome dado para uma zona da internet que não pode ser detectada facilmente pelos tradicionais motores de busca, garantindo "em tese" privacidade e anonimato para os seus navegantes.

4 CEBRIÁN, Belén Dominguez. Cibertaque: o vírus WannaCry e a ameaça de uma nova onda de infecções. **El País**, Madri. 15 maio 2017. Disponível em: <http://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html> Acesso em: 20 maio 2017.

nosos tende a mudar de acordo com o alvo escolhido. Existem ataques mais simples e outros mais complexos, estes ocorrem quando existe um alvo específico, seja pessoa física, seja pessoa jurídica de direito privado ou até mesmo pessoa de direito público. As abordagens se desenvolvem de diversas formas – explorando as falhas dos sistemas ou também por meio de engenharia social, explorando as nossas vulnerabilidades sociais. Diante do exposto, trataremos tais etapas como: Implantação; Instalação; Comando e Controle; Destruição e Extorsão, conforme classificação elencada por Allan Liska e Timothy Gallo[5].

3.1 A Implantação do *Malware*

Num primeiro momento, há necessidade de o cibercriminoso ter acesso à máquina-alvo, com o fito de adicionar as partes integrantes do *malware*. Nessa etapa, eles se utilizam dos chamados *download drive-by*[6]. Exemplificando: ao visitar páginas da internet já infectadas e aproveitando-se das falhas de segurança da máquina-alvo, quando o usuário final acessa um desses sites, *downloads* automáticos são efetuados pela máquina sem que esse usuário perceba. Diante de diversas técnicas, os componentes do *malware* são instalados sem que o antivírus da máquina perceba. Outra forma de ataque complexo é o *watering hole attack*[7]. Esse procedimento consiste na busca de diversas informações sobre a vítima, como os sites que ela visita, as permissões que ela tem de autorizar em sua navegação, os aplicativos necessários para acessar determinado local, os tipos de e-mails que podem ser trocados, entre outras formas. Assim, os cibercriminosos podem executar um ataque específico. Trata-se de um ataque personalizado.

3.2 A Instalação do *Malware*

Em um ataque bem-sucedido, o qual pode ter se efetivado pelas diversas ferramentas utilizadas para esse propósito, uma parte do *malware* acessa a máquina. Nesse momento inicial, o programa é executado no sentido de fazer o *download* do *ransomware* completo. Após esse estágio, ocorrerá uma gradativa dependência da máquina em relação ao criminoso, o qual passa literalmente a "varrer" a máquina na busca de suas prin-

5 Cf. LISKA, Allan; GALLO, Timothy. **Ransomware (Defendendo-se da Extorsão Digital)**. São Paulo: Novatec Editora Ltda., 2017, p. 19.

6 Qualquer *download* que acontece sem o conhecimento da pessoa, geralmente um vírus de computador, um *spyware* ou um *malware*.

7 Temos diversas analogias esquisitas no mundo da informática, *Watering Hole Attack* é mais uma delas. Nesse caso *Watering Hole* seria uma analogia a uma fonte d´agua na África, onde os animais param para beber água e ficam vulneráveis aos predadores que ficam à espreita, no aguardo de uma presa fácil.

cipais diretrizes de comando. Essa conexão entre criminoso e máquina infectada passa a trazer diversos riscos, não só para essa máquina, mas para toda a estrutura a qual eventualmente ela esteja conectada.

As palavras de Allan Liska e Timothy Gallo[8] são cristalinas em definir essa etapa:

> Em um ataque com alvo específico, as técnicas para instalar, ofuscar, compactar o código e explorar falhas podem ser mais nefastas na tentativa de maximizar o resgate (ransom). O ransomware pode usar essa instalação inicial para se espalhar lentamente pela rede afetada, instalando-se em vários sistemas e abrindo compartilhamentos de arquivos que, por sua vez, serão simultaneamente criptografados quando instruções forem enviadas na próxima fase. (LISKA; GALLO, 2017, p. 19)

Após essa varredura, o vírus passará a desabilitar todo e qualquer procedimento que permita ao usuário tentar reverter a situação atual, como funcionalidades padrão, recuperação do sistema, logins e antivírus. Vencida esta etapa, haverá a necessidade de se estabelecer uma nova troca de informações entre criminoso e máquina infectada para o comando e controle.

3.3 O Controle da máquina

A partir da execução, o vírus passará a buscar na máquina diversas informações importantes, como sistemas instalados, protocolo de internet (IP), tipos de antivírus, navegadores, entre outras informações, para ter a ciência se a máquina infectada é realmente importante para os criminosos ou não, continuando, assim, com as outras fases do ataque.

3.4 Destruição de dados e "extorsão" das vítimas

De posse de tais informações, os arquivos serão criptografados ou bloqueados, tendo em vista que estes já foram identificados pela fase anterior. Normalmente os arquivos mais procurados são os arquivos de texto, planilhas, arquivos de programas de imagens,

8 Cf. LISKA, Allan; GALLO, Timothy. **Ransomware (Defendendo-se da Extorsão Digital)**. São Paulo: Novatec Editora Ltda., 2017, p. 22.

de áudio e vídeo. Exemplo de extensões desses arquivos: *pdf, mp3, rtf, txt, bmp, zip, jpg, xls, exe, ppt, gif, docx, avi, html, mpeg, avi, jpeg*, entre outros.

O processo de criptografia desses arquivos utiliza chaves simétricas ou assimétricas, as quais movem e embaralham esses arquivos. Entretanto, diante do rápido desenvolvimento desses vírus, os ataques têm cada vez mais utilizado as duas técnicas. A chave simétrica é uma chave única que serve para criptografar, bem como para descriptografar os dados da máquina. Em sua funcionalidade, ela usa menos recursos do sistema da máquina infectada, podendo criptografar de forma mais rápida, mesmo quando o computador estiver *off-line*. Entretanto, o criminoso somente terá as informações sobre a conclusão do ataque quando a máquina se reconectar à internet. É também chamada de "criptografia de chave secreta".

Quanto à chave assimétrica, esta traz uma criptografia mais complexa, tendo o invasor uma chave pública, que serve para criptografar os arquivos, e uma chave privada, que será usada no processo de descriptografia. A criptografia assimétrica necessita de maior processamento da máquina, mas garante maior segurança no ataque, tendo em vista que apenas a chave pública transita entre o criminoso e a máquina-vítima. Após essa etapa, a vítima terá seu acesso limitado ou não terá nenhum acesso ao computador, o qual apresentará uma tela com instruções para o pagamento do resgate de seus dados.

O pedido de pagamento ocorre nesse momento, diante da máquina infectada, a vítima não terá acesso aos seus dados e será compelida a pagar um valor, que aumentará com o passar do tempo, dependendo do tipo de ataque. Um usuário particular não é tão importante para os cibercriminosos quanto governos ou grandes corporações. Normalmente os valores são cobrados em moeda virtual (geralmente o *bitcoin*[9]).

A partir de uma infecção, pagar ou não o valor pedido pelos criminosos?

A orientação dos órgãos de segurança é não pagar. Entretanto, cabe fazermos uma análise sobre a extensão do dano sofrido. Se a vítima possui dados importantes que venham a trazer altos prejuízos tanto a si quanto a terceiros, talvez a melhor opção seja pagar o resgate. Mas é importante frisar que o pagamento desses valores não será a garantia de que o criminoso enviará a chave que irá descriptografar os arquivos.

9 Bitcoin é uma tecnologia digital que permite reproduzir em pagamentos eletrônicos a eficiência dos pagamentos com cédulas descrita acima. Pagamentos com bitcoins são rápidos, baratos e sem intermediários. Além disso, eles podem ser feitos para qualquer pessoa, que esteja em qualquer lugar do planeta, sem limite mínimo ou máximo de valor.

4 A criptomoeda

Normalmente os cibercriminosos têm utilizado o *bitcoin* (criptomoeda) para o pagamento dos resgates por dificultar o rastreamento das transações. O *bitcoin* trata-se de uma moeda digital descentralizada, ou seja, ela não depende de um emissor central e pode ser transacionada para qualquer pessoa em qualquer parte do planeta sem intermediários, e, inclusive, sem limite de valor. Sem muito aprofundamento, para utilizá-la cada usuário terá de criar uma "carteira" (um programa). Ela serve para acumular os seus endereços *bitcoin*. Assim, ao criar uma carteira, o usuário receberá duas chaves: uma chave criptografada pública e outra privada. A chave pública é aquela em que o usuário informará aos outros e utilizará para efetuar suas transações e a chave privada é como se fosse a "senha" da chave pública. Como as chaves públicas são muito extensas, utiliza-se muito nessas transações o chamado "QR Code"[10], que é a representação da chave pública em forma de imagem.

Quando ocorrem essas transações, é gerada uma corrente de blocos (*blockchain*[11]), que é basicamente um banco de dados. Cria-se, então, um bloco inicial que a cada 10 minutos é ampliado e um novo bloco é gerado, de modo que cada bloco posterior possui informações de seu antecessor. Assim ocorre até o final da transação.

Como forma de proteção, cada transação efetuada é impressa na rede *bitcoin*, de modo que não há possibilidade de tentar gastar aquela moeda em mais de uma transação. As transações são públicas, mas ninguém sabe quem são as pessoas que estão por trás dos pontos de início e fim, em tese, garantindo o anonimato. Por óbvio que usuários comuns, podem deixar outros rastros em suas transações, como seu número de IP. Sabemos que os criminosos facilmente podem mascarar seu IP original. Por tais fatores, os cibercriminosos preferem essa moeda em suas empreitadas.

5 Prevenção

Um dos principais fatores de sucesso dos ciberataques é a exploração das vulnerabilidades do usuário final. Os usuários particulares ainda não se deram conta das ameaças

10 Código QR (sigla do inglês *Quick Response*) é um código de barras bidimensional que pode ser facilmente escaneado usando a maioria dos telefones celulares equipados com câmera. Esse código é convertido em texto (interativo), um endereço de internet, um número de telefone, uma localização georreferenciada, um e-mail, um contato ou um SMS.

11 A cadeia de blocos, ou *blockchain*, é o sistema de registros que garante a segurança das operações realizadas por criptomoedas – as bitcoins.

que se escondem por trás de uma simples visita à internet. As empresas e os governos devem investir pesado em campanhas de conscientização de seus funcionários para a execução de uma navegação segura. Visando à prevenção e à minimização dos danos, é de extrema importância fazer uma cópia periódica (*backup*) de todos os dados das máquinas em mídia física externa. Noutro ponto, outras medidas simples, porém não menos importantes, como a ativação da extensão dos arquivos, bem como o monitoramento dos anexos dos e-mails, para evitar que um arquivo executável malicioso seja ativado.

Manter os programas sempre atualizados, porque estes estão sempre em desenvolvimento de proteção para novas ameaças. Importante baixar aplicativos apenas de fontes confiáveis, verificando se as permissões de instalação e execução são coerentes e desabilitar a autoexecução de mídias removíveis e de arquivos que estejam anexados. Algumas empresas de cibersegurança também desenvolvem ferramentas gratuitas para descriptografar dados infectados por *ransomware*, tendo como exemplo o site <www.nomoreransom.org>.

As equipes de segurança da informação também utilizam a chamada "*sandbox*" (caixa de areia), que é uma ferramenta capaz de executar os programas suspeitos de forma isolada, num ambiente virtual dentro da própria máquina, possibilitando ao usuário analisar seus procedimentos de forma segura, num perímetro limitado e sem afetar a máquina. Outro procedimento utilizado é o chamado método "*honeyfile*" ou "*honeypot*"" ("arquivo de mel" ou "pote de mel"), em que se apresenta um sistema exposto como uma isca para um ataque. Diante desse ataque, a equipe de segurança da informação poderá estudá-lo, podendo desenvolver novos mecanismos de defesa para novos vírus.

Por óbvio que os procedimentos de prevenção não se esgotam aqui, diversos procedimentos técnicos são utilizados, mas não caberia maior aprofundamento, tendo em vista correr o risco de desviarmos da análise jurídica do presente estudo.

6 Principais mecanismos de investigação

O combate aos diversos crimes praticados na grande rede mundial de computadores deve observar diversos fatores, entre eles o aspecto jurídico, quanto à eventual necessidade de autorização judicial, e o técnico, no que tange aos equipamentos e à capacitação dos profissionais envolvidos nesse mister. A Polícia Federal mantém em suas superintendências Grupos de Repressão a Crimes Cibernéticos (GRCC), e em âmbito

estadual, particularmente no Rio de Janeiro, a Polícia Civil possui a especializada Delegacia de Repressão aos Crimes de Informática (DRCI).

Cumpre observar que nesse tipo de crime as evidências apresentam características diversas, possuindo diversos formatos, pois podem se tratar de imagens, vídeo, áudio, planilhas, documentos, seja de forma isolada ou em conjunto. Essas evidências, por serem facilmente destruídas ou alteradas, devem ser de pronto preservadas. Elas estão misturadas a outros dados, obrigando os investigadores e técnicos a fazer uma análise mais apurada durante a sua obtenção.

Na apuração desses crimes, cada área tem seus procedimentos específicos, por exemplo: análise dos dados registrados nos servidores; análise dos pacotes de dados contidos na transferência de informações dentro da rede; quanto à investigação relacionada a *websites*, é necessária a guarda de todos os seus componentes, e para isso existem programas específicos como: *HTTrack, Express WebPictures, Grab-a-Site, WebLooper e WebReaper*.

Além disso, há necessidade da descoberta do servidor que faz a hospedagem desses *websites*, e para isso é importante saber se o *website* em questão é nacional ou não. Por meio da ferramenta *whois*[12], bem como no site (www.registro.br), o qual é o responsável pelo registro dos domínios das páginas no Brasil, é possível ter acesso ao nome do responsável administrativo pelo domínio; o contato de incidentes de segurança (responsável pelo Setor de Tecnologia de Informação); e o provedor de *backbone*[13] (empresa que detém blocos de endereços IPs). Caso o domínio seja estrangeiro, ainda há possibilidade de obtermos essas informações por outros serviços de whois, tais como: <http://www.internic.net/whois.html>; <http://lacnic.net/>; <http://www.arin.net/> e <http://www.networksolutions.com>.

Em que pese o fato de os crimes cibernéticos deixarem rastros, sabemos que os cibercriminosos também utilizam ferramentas para buscar o anonimato em suas ações. Um exemplo disso é o navegador TOR[14], um dos mais utilizados para acessar a *deep web* para a prática de crimes. Ele mascara o IP original e a localização, embaralhando as informa-

12 A ferramenta Whois é utilizada para se obter informações sobre um determinado domínio. Por meio do Whois pode-se obter informações sobre os servidores DNS, estado do domínio (ativo, expirado etc.), informações sobre a empresa de hospedagem de sites, entre outros dados.

13 O *backbone*, tradução de "espinha dorsal", é uma rede principal por onde passam os dados dos clientes da internet. Todas essas vias [ou pequenas redes] estão conectadas à estrada principal [backbone]".

14 TOR (*The Onion Router*) é uma rede de túneis virtuais que dificulta e embaralha a identificação dos equipamentos ao acessarem determinado conteúdo na rede.

ções e dificultando a identificação. Isso ocorre por causa de seu complexo mecanismo, que utiliza uma rede de transmissão de dados baseada em múltiplas máquinas. Assim, ao enviar uma mensagem, ela passa não por apenas uma, mas por inúmeras máquinas até chegar ao destinatário. O objetivo é dificultar o acesso indevido ao computador, confundindo quem tenta invadir a sua privacidade para ter acesso às suas informações.

Ressalte-se que não há crime perfeito, pois ainda que esteja anônimo, quem navega pela *deep web* e troca mensagens produz pacotes (unidades de dados), e ao monitorar a rede esses dados podem dar aos agentes indícios de atividades ilícitas, por meio da análise do tempo dos dados transmitidos. Registre-se que a Polícia Federal desenvolveu uma tecnologia inédita na América Latina que possibilitou efetuar o monitoramento da *deep web*, o que resultou na operação Darknet em 2014, segundo o professor Rafael de Souza, em matéria publicada na Associação Nacional dos Delegados da Polícia Federal[15]:

> Uma das formas de se investigar a rede secreta, segundo o professor, é estudando o tráfego da internet. Embora com IP escondido, quem troca mensagens pela *deep web* ainda produz pacotes (como são chamadas as unidades de dados) visíveis. Um dos indícios de que existiria uma atividade ilícita seria a troca de pacotes entre um pequeno grupo de usuários sem localização de IP definida.
> Tráfego de dados constante entre computadores ocultos é um sinal mais do que suspeito.
> Quem monitora esse trânsito consegue, também, verificar o formato das mensagens partilhadas.
> Geralmente, grupos de pedofilia na *deep web*, por exemplo, trocam fotos, identificadas pelo formato, que pode ser jpg., jpge, entre outros.

A partir de nossa pesquisa sobre o *ransomware*, percebemos que parte relevante do sucesso nos ataques está na falta de informação/cuidado do usuário final na administração de seus e-mails pessoais e profissionais. Portanto, a abordagem a seguir trata do mecanismo de investigação no que tange aos e-mails.

Quando um e-mail é enviado, aparece o endereço do remetente e do destinatário no chamado "cabeçalho" da mensagem (os navegadores dispõem essa função, geralmente na aba opções). O objetivo é ter acesso a todos os códigos da mensagem para descobrir a

15 GUIMARÃES, Fabiane. A internet que ninguém via. Metro. **Associação Nacional dos Delegados de Polícia Federal**. 30 dez. 2014. Disponível em: <http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia _codigo=7235&tit=A-internet-que-ninguem-via#.WVsS6YjyvIV> Acesso em: 3 jul. 2017.

numeração do IP, a data e a hora da mensagem. Numa primeira análise de conteúdo, busca-se a palavra *received* (recebido), essa palavra aparece em ordem decrescente e indica por quantas estações (servidores) a mensagem passou antes de chegar ao destinatário final. Assim, na última palavra "*received*" podemos encontrar quem foi o remetente.

Ao localizar o IP, a autoridade interessada deverá efetuar a pesquisa nos mecanismos *whois* para ter acesso aos dados do provedor de acesso e, a partir daí, a pedido dela, o juiz oficiará esse provedor no sentido de quebrar o sigilo dos dados telemáticos com a finalidade de acessar as informações do usuário vinculado ao IP em determinada data e horário. Caso não consiga localizar o número do IP, a partir do e-mail do remetente pode-se requerer judicialmente a quebra do sigilo de dados telemáticos ao provedor desse e-mail, para que ele informe o número do IP da máquina que autenticou a conta, na data e horário do e-mail enviado.

Outro procedimento é o monitoramento de e-mail de alvos suspeitos (mediante autorização judicial). Dessa forma, o juiz pode determinar que o provedor responsável pela conta desvie as mensagens enviadas ou recebidas para uma conta de monitoramento, possibilitando que as mensagens sejam analisadas. Assim será possível saber com quem o alvo se corresponde e de onde realiza os acessos.

7 Mecanismos de cooperação internacional

O Estado brasileiro é signatário de diversos tratados internacionais, e diante das conexões político-econômicas, a República Federativa do Brasil se comporta nas relações internacionais na forma do art. 4° da Constituição Federal, sendo regida pelos seguintes princípios *in verbis*:

> Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios:
> 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;
> X – concessão de asilo político.
> Parágrafo único. A República Federativa do Brasil buscará a integração econômica, política, social e cultural dos povos da América Latina, visando à formação de uma comunidade latino-americana de nações.

A dificuldade encontrada pelas autoridades na apuração dos crimes cibernéticos está na característica transnacional destes, havendo grande obstáculo na obtenção de provas ou indícios, tendo em vista não haver uma legislação unificada, considerando-se a soberania dos países. Diante da inexistência de poder coercitivo na esfera internacional, os países estabelecem tratados internacionais e acordos de cooperação. Nessa atuação, há necessidade de uma combinação entre os tratados, os princípios do direito internacional e a legislação que regulamenta as empresas privadas que atuam na internet.

Importante instrumento em âmbito global no combate aos crimes cibernéticos é a Convenção de Budapeste (Convenção sobre o Cibercrime), firmada pelo Conselho Europeu em 23 de novembro de 2001, na Hungria. Em seus quarenta e oito artigos, acreditando que uma luta efetiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal, rápida e eficaz, ela disciplina procedimentos como: medidas legislativas a serem tomadas em âmbito nacional entre os membros; a manutenção dos dados informáticos; a interceptação e o recolhimento em tempo real dos dados de tráfego; estabelece os princípios gerais relativos ao auxílio mútuo, entre outros.

Ao tomar como exemplo o fato de que a maioria das empresas privadas que atuam na internet possuem suas sedes nos Estados Unidos da América e que existe acordo de cooperação internacional entre Brasil e EUA, discorreremos sobre os principais procedimentos utilizados na investigação de crimes transnacionais em relação aos dois países. Numa investigação nesse sentido, a Constituição Federal em seu art. 144, § 1° e § 4° c/c o art. 2° da Lei n° 12.830/2013, confere aos delegados de polícia federal e delegados de Polícia Civil dos estados a competência para requerer esses dados. O Ministério Público, amparado pelo art. 8° da Lei Complementar n° 75/1993 c/c o art. 62 da Lei n° 8.625/1993 c/c Resolução n° 13/2006 CNMP e diante do entendimento do STF, no julgamento do RE 593727/MG em 2015, também é autoridade competente nesse sentido. No entanto, ressaltamos que diante desses pedidos, o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça (DRCI/MJ) é o órgão competente para auxiliar essas autoridades nesse mister, conforme o art. 10, V do Decreto n° 8.668, de 11 de fevereiro de 2016. Essas autoridades atuam em conjunto com outros países e com instituições como a Interpol, Europol, Ameripol, FBI, entre outras.

O Marco Civil da Internet (Lei n° 12.965/2014), no § 2° do art. 11, estabelece que a legislação brasileira deverá ser aplicada às empresas estrangeiras sediadas no exterior, desde que estas ofertem serviços ao público brasileiro ou que pelo menos um integrante do mesmo grupo econômico possua estabelecimento no Brasil. Noutro ponto, também estabelece que se aplica a lei brasileira aos dados coletados em território nacional desde que pelo menos um dos terminais esteja localizado no Brasil. No entanto, diante das dificuldades na obtenção desses dados, em investigações sobre cibercrimes de ordem transnacional, o Ministério Público Federal (MPF) defende o entendimento do Marco Civil, que não exige o MLAT (*Mutual Legal Assistance Treaty*) quando a empresa presta serviços no Brasil. O governo do Brasil e o dos Estados Unidos da América firmaram esse acordo de assistência judiciária em matéria penal em outubro de 1997 e está representado em nosso ordenamento pelo Decreto nº 3.810/2001.

Para a obtenção dos dados não amparados pelo manto constitucional, as autoridades lançam mão do documento chamado "*Subpoena*", que, parafraseando José Augusto Campos Versiani[16], tem como tradução literal "intimação", mas que pode ser entendido como uma requisição que deve ser preenchida em inglês, assinada, digitalizada e encaminhada à empresa detentora da informação. No que tange aos dados protegidos, as autoridades valem-se do MLAT, devendo também observar o princípio da dupla incriminação.

O acordo de cooperação internacional deve obedecer a requisitos de ordem formal e material, partindo-se de uma base legal como uma convenção, um acordo internacional e o princípio da reciprocidade, devendo passar obrigatoriamente pela autoridade central designada para esse fim. Ressalte-se, que serve tanto para a cooperação ativa ou passiva e que, em nosso caso, é o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça (DRCI/MJ)[17]. As solicitações devem ser produzidas em duas vias, tomando como exemplo investigações originadas aqui no Brasil, a primeira via será original na língua portuguesa e a segunda via traduzida para o idioma do Estado requerido.

No que tange aos requisitos materiais, obrigatoriamente a autoridade requerente deverá endereçar o pedido ao correto destinatário da solicitação, que em nosso exemplo é

16 VERSIANI, José Augusto Campos et al. **Combate ao Crime Cibernético**. Cooperação Internacional na Investigação de Crimes Cibernéticos. Rio de Janeiro: M. Mallet Editora Ltda., 2016, p. 156.

17 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). 3. ed. Brasília: Ministério da Justiça, 2014. p. 56.

o Departamento de Justiça dos Estados Unidos da América. Noutro ponto, é importante indicar o órgão e a autoridade competente responsável pelo inquérito policial ou qualquer outro procedimento de investigação criminal, ou, ainda, pela ação penal em curso, informando o número do inquérito ou ação penal, o cargo e o nome completo das autoridades, bem como os dados de contato, tais como e-mails ou telefone.

Não menos importante é a descrição narrativa completa, clara e objetiva dos fatos, discorrendo sobre os elementos essenciais dos acontecimentos, as circunstâncias sobre o lugar, a data e a maneira pela qual a infração foi cometida, esclarecendo detalhadamente o nexo causal entre a investigação ou processo em curso, seus suspeitos ou réus e a assistência jurídica solicitada.

7.1 Territorialidade

A necessidade de combate aos cibercrimes, em especial ao *ransomware*, invariavelmente transita pelo assunto da territorialidade/extraterritorialidade. Em que pese o fato de existirem diversos mecanismos de investigação, inclusive com colaborações em tempo real, como é o caso do Sistema Mundial de Informação (I-24/7)[18] da Interpol, o qual funciona 24 horas nos 7 dias da semana, sabemos que os cibercriminosos utilizam ferramentas que camuflam sua identidade, dificultando a análise de seus rastros, conforme já ventilado em tópicos anteriores.

Exemplo importante de toda essa complexidade é o fato de que um criminoso em um determinado país pode infectar uma máquina em um outro, utilizando-se de um servidor que se encontra em um terceiro país. Em outra forma de ataque, criminosos também podem infectar determinada máquina, valendo-se de outra máquina (zumbi)[19], situada em qualquer outro país.

Nesse contexto, salientamos o *status* residual da competência da justiça estadual em relação à justiça federal em seu art. 109, IV e V, da Constituição Federal. Diante da controversa doutrina, imaginemos um cibercrime: um ataque de *ransomware* ocorrido

18 BLAT, Erick Ferreira et al. **Combate ao Crime Cibernético**. Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal. Rio de Janeiro: M. Mallet Editora Ltda., 2016, p. 78.

19 Computador zumbi é um termo empregado para classificar computadores utilizados para envio de *spam* e ataque a sites, sem que o dono do computador saiba de tal atividade. Para que isso aconteça, o invasor precisa instalar um programa no computador-alvo, normalmente por meio de e-mails, redes ponto a ponto (*peer-to-peer*), ou mesmo de sites com links em que o invasor disfarça o programa para que o usuário não saiba de que se trata. Após a instalação do programa, o invasor passa a utilizar esse computador (com todos os outros computadores infectados) para enviar e-mails em série (spam) com diversas finalidades, ou mesmo para atacar sites, com intuito de criar danos ao site ou de deixá-lo lento.

em território brasileiro, porém em estados diferentes, o chamado "crime plurilocal". Tomando como exemplo, um criminoso situado no estado do Rio de Janeiro infecta um computador de um usuário residente no estado de São Paulo, passando a exigir que este deposite certa quantia em moeda virtual para liberar o acesso à máquina infectada, conduta tipificada no art. 154-A do Código Penal.

Numa primeira análise, percebemos que tal crime possui pena de até 2 anos, submetendo-se à Lei n° 9.099/1995 (Juizado Especial Criminal), a qual adota em seu art. 63 a teoria da ubiquidade, competindo ao órgão judicial do lugar em que foi praticada a infração penal julgá-la (Justiça Estadual do Rio de Janeiro). Em uma análise prática, percebe-se que ao adotar tal teoria, em alguns casos, ela atentaria contra os próprios princípios norteadores da Lei n° 9.099/1995, em seu art. 2°: a economia processual e a celeridade, posto que obrigaria a vítima a se deslocar até outro estado (art. 154-B), podendo inviabilizar a prestação jurisdicional.

Ressalte-se que a depender do caso concreto, tal conduta poderá ultrapassar os 2 anos, não mais enquadrando-se como de menor potencial ofensivo, submetendo-se à Vara Criminal. Nesse sentido a competência será determinada pelo lugar em que se consumou a infração, com fulcro no art. 70 do Código de Processo Penal, consagrando a teoria do resultado.

Ponto importante é a análise da redação contida no art. 5° do Código Penal, que dispõe aplicar-se a lei brasileira, sem prejuízo das convenções, tratados e regras de Direito Internacional ao crime praticado no território nacional, adotando, assim, a teoria da territorialidade temperada, em que o Brasil abre uma lacuna à sua exclusividade em prol da cooperação internacional.

Diante dessa abordagem, quanto aos crimes à distância que se iniciam em um país e terminam em outro, tratando-se da aplicação da norma penal no espaço, a aplicabilidade do art. 6° do Código Penal se vislumbra a mais adequada. Ele considera praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado, adotando assim a teoria da ubiquidade.

8 Análise legislativa (Lei n° 12.737/2012)

A evolução das relações econômicas e tecnológicas condicionou a sociedade a depender cada vez mais da internet, e hoje em dia nos grandes centros é praticamente im-

possível haver pessoas físicas ou jurídicas que não possuam um computador, um *tablet* ou um celular que lhes auxilie nas relações de trabalho ou simplesmente de lazer. Diante desse crescente fluxo de dados, a tecnologia da informação se mostra de extrema importância para nos auxiliar nessa nova realidade, seja na melhora da produtividade, dando mais eficiência às relações, seja na proteção estratégica de informações pessoais, empresariais e/ou governamentais.

Nesse contexto, os crimes praticados pela internet cresceram e disseminou-se uma silenciosa guerra por importantes informações sigilosas. Entre outros projetos que tramitavam no Poder Legislativo, em 30 de novembro de 2012 foi sancionada a Lei n° 12.737/2012[20] (Projeto de Lei n° 2.793/2011).

Apelidada de "Lei Carolina Dieckmann", ela entra no ordenamento jurídico de forma muito rápida e leva esse apelido por manter relação com o episódio do furto de fotos íntimas do computador da supracitada atriz, a qual teve tais fotos divulgadas na internet[21]. Entre outros tipos penais criados pela lei, consta o art. 154-A que altera o Código Penal com o *nomen iuris* de "invasão de dispositivo informático", o qual tipifica a conduta apresentada no presente estudo. Com o fito de analisarmos o aludido artigo, é necessário transcrevê-lo a seguir:

> 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.

Os cibercriminosos que se utilizam do *ransomware* praticam a conduta prevista no referido artigo, mas para melhor examinarmos é importante fracioná-lo: *invadir / dispositivo informático alheio / conectado ou não à rede de computadores / mediante violação indevida de mecanismo de segurança / 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.*

20 BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em: 30 jul. 2017.

21 Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera "justiça". **G1**, São Paulo. 14 maio 2012. Disponível em: <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em: 30 jul. 2017.

Em análise, conforme já ventilado no tópico 4 (Dinâmica dos Ataques) do presente estudo, os criminosos invadem dispositivo informático alheio, normalmente conectado à internet, assim considerados os (*smartphones*, computadores, *tablets, ipads, ipods* etc.). Importante observarmos o termo "*mediante violação indevida de mecanismo de segurança*", e por mecanismo de segurança podem ser considerados (*antimalware*[22], backups, login/senha, certificado digital[23], firewall[24], entre outros).

Sabemos que existem diversas possibilidades de invadir e infectar a máquina, e a título de exemplo, ainda que o usuário execute um *malware* "camuflado" anexado ao seu e-mail (prática descrita como *phishing*) ainda se configurará o crime, visto que existirá um vício de vontade (dolo) que faz o criminoso enganar o usuário, e o *malware* após instalado ainda irá burlar os mecanismos de segurança da máquina.

Outro ponto é o especial objetivo de agir descrito no tipo penal: "*com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo*". Perceba que no crime em comento, a conduta dos criminosos subsume-se ao tipo penal, tendo em vista que o ransomware em sua silenciosa atuação, ao criptografar os arquivos, altera os dados, embaralhando as informações, obtendo-as em seus servidores de controle e comando, podendo também destruí-las, se assim quiser o criminoso.

Ao final do tipo penal, "*ou instalar vulnerabilidades para obter vantagem ilícita*" trata-se de mero exaurimento, mas ainda assim constitui uma finalidade específica de um ataque por *ransomware*. Uma das etapas é a instalação do programa, o qual irá modificar e explorar as vulnerabilidades do sistema para na etapa final, forçar a vítima a pagar um valor visando obter novamente o controle de seu sistema.

> § 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.

22 Ferramentas *antimalware* são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, *antispyware*, *antirootkit* e *antitrojan* são exemplos de ferramentas desse tipo.

23 Certificado Digital – é um arquivo eletrônico que funciona como se fosse uma assinatura digital, com validade jurídica, e que garante proteção às transações eletrônicas e outros serviços via internet, de maneira que pessoas (físicas e jurídicas) se identifiquem e assinem digitalmente, de qualquer lugar do mundo, com mais segurança e agilidade.

24 Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a internet (ou entre a rede onde seu computador está instalado e a internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados.

No parágrafo primeiro, temos a figura da equiparação, o que demonstra que o legislador estava atento, pois se ajusta perfeitamente à figura das organizações de cibercriminosos que disponibilizam os códigos maliciosos em fóruns de internet, terceirizando os ataques e cobrando um percentual sobre o valor recebido.

> § 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.

Temos no parágrafo terceiro a modalidade qualificada, dobrando a pena estipulada no primeiro parágrafo. Ciberataques vinculados à espionagem industrial e governamental são uma realidade[25], os ataques de *ransomware* geram grandes prejuízos[26], afetando a economia dos países. Uma questão gira em torno do que significa "informações sigilosas". Discorrendo sobre o assunto, Rogério Grego[27] traz à baila o conceito de informação sigilosa para a Administração Pública, disposto no inciso III do art. 4° da Lei n° 12.527/2011 (Lei de Acesso à Informação), in verbis:

> Art. 4° – Para os efeitos desta lei, considera-se:
> [...]
> III – informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

Ponto relevante é se organizações criminosas em ciberataques conseguirem informações sigilosas sobre o Estado brasileiro. Nesse caso, aplicaremos o §3° do art. 154-A do Código Penal ou tal conduta se ajusta ao crime tipificado no parágrafo único, inciso IV do art. 13 da Lei n° 7.170/1983 (Lei de Segurança Nacional), *in verbis*:

25 GROSSMANN, Luís Oswaldo. Symantec identifica ciberataques em 16 países com malware da CIA. **Convergência Digital**. 10 abr. 2017. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44938&sid=18>. Acesso em: 6 ago. 2017.

26 SANTANA, Felipe. 60% das pequenas empresas atingidas por vírus nos EUA vão à falência. **G1**, Nova Iorque, EUA. 13 maio 2017. Disponível em: <http://g1.globo.com/mundo/blog/direto-de-nova-york/post/60-das-pequenas-empresas-atingidas-por-virus-nos-eua-vao-falencia.html>. Acesso em: 6 ago. 2017.

27 GRECO, Rogério. **Código Penal Comentado**. 7.ed. Niterói, RJ: Impetus, 2013, p.447.

> Art. 13. Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.
> Pena: reclusão, de 3 a 15 anos.
> Parágrafo único – Incorre na mesma pena quem:
> [...]
> IV – obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo.

O art. 154-A protege a intimidade, a liberdade individual e a segurança da informação. Em estudo, sob o prisma do princípio da especialidade, percebe-se que sua redação traz diversos elementos que podem ser utilizados para a prática do delito. Entretanto, importante observarmos a expressão em seu § 3º: "**se a conduta não constitui crime mais grave**".

Nessa esteira, trazemos à baila a Lei de Segurança Nacional (Lei n° 7.170/1983), que, no parágrafo único, inciso IV, do art. 13, traz condutas que também se enquadram aos ataques por *ransomware*, punindo-as com reclusão de 3 a 15 anos. A referida lei tutela os interesses do Estado brasileiro no que tange à independência, segurança e integridade de seus órgãos supremos.

Não se pode olvidar que algumas agências de inteligência governamentais exploram e armazenam as vulnerabilidades dos sistemas operacionais utilizados na internet, criando *exploits*[28] para monitoramento em massa. Essas ferramentas podem ser utilizadas tanto pelos governos como por cibercriminosos[29] em ataques com motivações políticas, religiosas ou econômicas. Dessa feita, em um ataque por *ransomware*, dados sigilosos que são importantes para nosso país podem chegar às mãos dos criminosos

28 Um *exploit* geralmente é uma sequência de comandos, dados ou uma parte de um software elaborados por *hackers* que conseguem tirar proveito de um defeito ou vulnerabilidade.

29 HIGA, Paulo. Microsoft reclama de governos que "colecionam" falhas de segurança do Windows. WannaCry surgiu de uma vulnerabilidade descoberta pela agência de segurança dos EUA (e que foi vazada por hackers). **Tecnoblog**. 15 maio 2017. Disponível em: <https://tecnoblog.net/214665/microsoft-nsa-cia-vulnerabilidades-windows-wannacry/>. Acesso em: 7 ago. 2017.

por meio dos servidores de comando e controle que se comunicam com a(s) máquina(s) infectada(s).

Em remate, no que tange à supracitada indagação, salientamos que em que pese o fato de o art. 154-A do Código Penal trazer condutas mais específicas e adequadas à nova realidade social, amparado pela parte final da sanção prevista no § 3° do aludido artigo, entendemos ser perfeitamente aplicável o parágrafo único, inciso IV, do art. 13 da pretérita Lei n° 7.170/1983, tendo em vista a maior abrangência do bem jurídico tutelado por esta.

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

Nos aludidos parágrafos, temos as causas especiais de aumento de pena, e em relação ao § 2°, este apenas terá relação com o *caput* e o § 1º do art. 154-A, devendo ser aplicado na forma do art. 68 do Código Penal. Quanto aos §§ 4° e 5°, estes são autoexplicativos. Os crimes do art. 154-A se procedem mediante representação, salvo se o crime for cometido contra a Administração Pública direta ou indireta de qualquer dos Poderes da União, estados, Distrito Federal ou municípios ou empresas concessionárias de serviços públicos. Fator importante na referida lei é que a conduta em estudo trata-se de um crime de menor potencial ofensivo. No entanto, diante da gravidade da conduta, há entendimento no sentido da aplicabilidade do crime de extorsão (art. 158 do CP)[30], com a devida vênia, não conjugamos com tal entendimento por considerarmos que o art. 154-A

30 CRESPO, Marcelo. Ransonware e sua tipificação no Brasil. **Canal Ciências Criminais**. 28 out. 2015. Disponível em: <http://canalcienciascriminais.com.br/ransonware-e-sua-tipificacao-no-brasil/>. Acesso em: 7 ago. 2017.

é mais específico, tutelando bens jurídicos direcionados e seria forçoso entender que há grave ameaça na estudada conduta.

Apesar de a Lei n° 12.737/2012 ter adentrado em nosso ordenamento jurídico, temos assistido a ataques cada vez mais complexos, trazendo resultados desastrosos em diversos países, sem a devida identificação e punição desses cibercriminosos. O problema é global e a constante evolução tecnológica trará novos desafios aos países, a conexão entre *ransomware* e IOT[31] (internet das coisas) ampliará o espectro criminal dessas organizações. A título de exemplo, citamos o ataque ao metrô de São Francisco, nos Estados Unidos, em 2016, em que criminosos invadiram o sistema, liberando as catracas e também furtando dados[32]. No mesmo ano, um hospital em Kansas (EUA) sofreu dois ataques que impediram os funcionários de terem acesso aos arquivos, prontuários médicos e arquivos financeiros do hospital[33]. No início de 2017, um hotel na Áustria sofreu um ataque que invadiu o sistema de fechaduras eletrônicas, impedindo os clientes de entrarem ou saírem de seus quartos[34].

Em análise, percebemos que o tipo penal do art. 154-A descrito na Lei n° 12.737/2012 não alcança a realidade fática, visto que traz penas inexpressivas, em completa discrepância em relação aos danos causados. Noutro giro, percebe-se que o legislador pátrio ainda não se ateve à problemática em comento, pois em que pese ter criado no anteprojeto do novo Código Penal (PLS nº 236/2014) uma parte especial para os crimes cibernéticos (Título IV), o anteprojeto ainda se mostra desproporcional ao tamanho dos lucros auferidos e dos danos causados por um ataque de *ransomware*.

31 A Internet das Coisas (do inglês, *Internet of Things*) é uma revolução tecnológica a fim de conectar dispositivos eletrônicos utilizados no dia a dia (como aparelhos eletrodomésticos, eletroportáteis, máquinas industriais, meios de transporte etc.) à Internet, cujo desenvolvimento depende da inovação técnica dinâmica em campos tão importantes como os sensores *wireless*, a inteligência artificial e a nanotecnologia.

32 ROHR, Altieres. Metrô de São Francisco libera catracas após ataque por vírus de resgate. **G1**. 28 nov. 2016. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/ post/metro-de-sao-francisco-libera-catracas-apos-ataque-por-virus-de-resgate.html>. Acesso em: 7 ago. 2017.

33 HOSPITAL de Kansas atingido por *ransomware*, extorquido duas vezes. **Blog Trend Micro**. 30 maio 2016. Disponível em: <http://blog.trendmicro.com.br/hospital-de-kansas-atingido-por-ransomware-extorquido-duas-vezes/>. Acesso em: 7 ago. 2017.

34 DEMARTINI, Marina. Hackers trancam quartos de hotel e exigem resgate em bitcoin. **Revista Exame**. São Paulo. 1 fev. 2017. Disponível em: <http://exame.abril.com.br/tecnologia/ hackers-trancam-hospedes-em-hotel-e-exigem-resgate-em-bitcoin/>. Acesso em: 7 ago. 2017.

9 Conclusão

No presente estudo, pôde-se discorrer sobre a complexidade dos avanços tecnológicos, seus reflexos na vida social atual e como isso propiciou o aparecimento de novas condutas criminosas, bem como de velhos tipos penais que ganharam novas roupagens. Aproveitando-se da rapidez tecnológica e da lentidão burocrática dos órgãos repressivos governamentais, organizações de cibercriminosos se estruturaram e passaram a movimentar vultuosos valores com a conduta perpetrada no presente estudo.

Hodiernamente, ataques globais põem em risco todos os países em uma guerra silenciosa, e não obstante os ataques aos usuários privados, dados importantes de empresas e governos são coletados para os mais diversos fins. Percebeu-se que diversos mecanismos que propiciam o anonimato e a falta de informação dos usuários finais contribuem para o maior sucesso dos ataques por *ransomware*.

Noutro ponto, os tratados e acordos de cooperação internacional conjugados aos métodos de investigação das polícias judiciárias são importantes vetores no combate ao crime cibernético. No entanto, diferente do que ocorre com outros crimes cibernéticos como a injúria racial praticada pela internet e a pornografia infantil, a prática do *ransomware* ainda não resultou em importantes condenações em nosso país.

Em análise, concluiu-se que a tipificação do ataque por *ransomware*, disposta na Lei n° 12.737/2012, não se mostrou eficaz em combater o referido crime. Percebeu-se que o legislador pátrio ainda não está afinado com as transformações tecnológicas e suas implicações dentro do cibercrime. Ainda que o legislador tenha disponibilizado um título para os crimes cibernéticos no anteprojeto do novo Código Penal, as penas aplicáveis à estudada conduta são mínimas e não correspondem à gravidade dos danos causados, tanto às pessoas físicas e jurídicas, quanto à segurança político-econômica do país.

Referências

BLAT, Erick Ferreira et al. **Combate ao Crime Cibernético**. Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal. Rio de Janeiro: M. Mallet Editora Ltda., 2016.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde**: Segurança cibernética no Brasil. Organização por Claudia Canongia e Raphael Mandarino Junior. Brasília, 2010.

_____. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 3 dez. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 30 jul. 2017.

_____. 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). 3. ed. Brasília: Ministério da Justiça, 2014.

CAROLINA Dieckmann fala pela 1ª vez sobre fotos e diz que espera "justiça". **G1**, São Paulo, 14 maio 2012. Disponível em: <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em: 30 jul. 2017.

CEBRIÁN, Belén Dominguez. Cibertaque: o vírus WannaCry e a ameaça de uma nova onda de infecções. **El País**, Madri, 15 maio 2017. Disponível em: <http://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html>. Acesso em: 20 maio 2017.

CRESPO, Marcelo. Ransonware e sua tipificação no Brasil. **Canal Ciências Criminais**, 28 out. 2015. Disponível em: <http://canalcienciascriminais.com.br/ ransonware-e-sua-tipificacao-no-brasil/>. Acesso em: 7 ago. 2017.

DAMÁSIO, Jesus de; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Editora Saraiva, 2016.

DEMARTINI, Marina. Hackers trancam quartos de hotel e exigem resgate em bitcoin. **Revista Exame**, São Paulo. 1 fev. 2017. Disponível em: <http://exame.abril.com.br/tecnologia/hackers-trancam-hospedes-em-hotel-e-exigem-resgate-em-bitcoin/>. Acesso em: 7 ago. 2017.

GONÇALVES BARRETO, Alessandro; WENDT, Emerson; CASELLI, Guilherme. **Investigação digital em fontes abertas**. Rio de Janeiro: Brasport Editora., 2017.

GRECO, Rogério. **Código Penal Comentado**. 7.ed. Niterói, RJ: Impetus, 2013.

GROSSMANN, Luís Oswaldo. Symantec identifica ciberataques em 16 países com malware da CIA. **Convergência Digital**, 10 abr. 2017. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44938&sid=18>. Acesso em: 6 ago. 2017.

GUIMARÃES, Fabiane. A internet que ninguém via. Metro. **Associação Nacional dos Delegados de Polícia Federal**. 30 dez. 2014. Disponível em: <http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia_codigo=7235&tit=A-internet-que-ninguem-via#.WVsS6YjyvIV>. Acesso em: 3 jul. 2017.

HIGA, Paulo. Microsoft reclama de governos que "colecionam" falhas de segurança do Windows. WannaCry surgiu de uma vulnerabilidade descoberta pela agência de segurança dos EUA (e que foi vazada por hackers). **Tecnoblog**, 15 maio 2017. Disponível em: <https://tecnoblog.net/214665/ microsoft-nsa-cia-vulnerabilidades-windows-wannacry/>. Acesso em: 7 ago. 2017.

HOSPITAL de Kansas atingido por ransomware, extorquido duas vezes. **Blog Trend Micro**, 30 maio 2016. Disponível em: <http://blog.trendmicro.com.br/hospital-de-kansas-atingido-por-ransomware-extorquido-duas-vezes/>. Acesso em: 7 ago. 2017.

LISKA, Allan; GALLO, Timothy. **Ransomware** (Defendendo-se da Extorsão Digital). São Paulo: Novatec Editora Ltda., 2017.

ROHR, Altieres. Metrô de São Francisco libera catracas após ataque por vírus de resgate. **G1**, 28 nov. 2016. Disponível em: <http://g1.globo.com/ tecnologia/blog/seguranca-digital/post/metro-de-sao-francisco-libera-catracas-apos-ataque-por-virus-de-resgate.html>. Acesso em: 7 ago. 2017.

SANTANA, Felipe. 60% das pequenas empresas atingidas por vírus nos EUA vão à falência. **G1**, Nova Iorque, EUA. 13 maio 2017. Disponível em: <http://g1.globo.com/mundo/blog/direto-de-nova-york/post/60-das-pequenas-empresas-atingidas-por-virus-nos-eua-vao-falencia.html>. Acesso em: 6 ago. 2017.

VERSIANI, José Augusto Campos et al. **Combate ao Crime Cibernético**. Cooperação Internacional na Investigação de Crimes Cibernéticos. Rio de Janeiro: M. Mallet Editora Ltda., 2016.

6 RACISMO CIBERNÉTICO E OS DIREITOS DA TERCEIRA DIMENSÃO

Pedro de Vilhena Panazzolo[1]

Resumo: O presente artigo explora aspectos dos crimes cibernéticos, em especial o crime de racismo praticado pela internet, em comunhão com os princípios da terceira dimensão de direitos fundamentais e a proteção dos bens jurídicos inerentes aos direitos dessa dimensão. Num primeiro tópico, analisa os crimes cibernéticos, notadamente a sua conceituação. Passo avante, analisa o crime de racismo. Em seguida, adentra no exame da teoria das dimensões dos direitos fundamentais. Por fim, explora a junção dos direitos da terceira dimensão e o racismo praticado no campo cibernético, sempre em apreço aos direitos humanos e fundamentais, abordando a jurisprudência, a doutrina e a legislação vigentes no Brasil, bem como os tratados internacionais.

Palavras-chave: Racismo. Crimes Cibernéticos. Direitos Fundamentais. Direitos da Terceira Dimensão.

Abstract: *This article explores aspects of cybercrime, in particular the crime of racism practiced through the Internet, in accordance with the third dimension principles of fundamental rights and the protection of legal rights inherent in the rights of this dimension. In a first topic, it analyzes cybercrime, in particular, its conceptualization. In the following it analyzes the crime of racism. After entering the examination of the theory of the dimensions of fundamental rights. Finally, it enters into the junction of the rights of the third dimension and the racism practiced in the cybernetic field, always in appreciation of human and fundamental rights.*

Keywords: Racism. Cybercrime. Fundamental rights. Third dimension principles.

1 Introdução

Com o avanço tecnológico modificam-se também os costumes sociais e hábitos em geral dos indivíduos. Da mesma forma o Direito precisa acompanhar o caminho evolutivo da sociedade, merecendo profundo estudo das novas formas de interação das pessoas e as consequências jurídicas desse novo agir.

Logicamente, assim também caminha o Direito Penal, acompanhando o desenvolvimento dos modos de atuar e pensar do ser humano. Geralmente não com a mesma

1 Bacharel em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul. Especialista em Direito do Estado pela Universidade Federal do Rio Grande do Sul. Advogado.

velocidade e compreensão. Entretanto, é necessária uma contínua observância desses avanços, pois a forma como se apresentam os delitos e as agressões aos bens jurídicos protegidos por essa seara do direito, consequentemente, também vão se alterando.

Mudam-se os meios, os instrumentos, as maneiras de agir para a prática de infrações penais, o que demanda um olhar atento para a legislação vigente em compasso com a doutrina especializada e as decisões judiciais, com o fito de ser mantida a proteção dos direitos fundamentais consagrados pela Constituição Federal.

De outra banda, estamos em um tempo em que não se respeitam mais as diferenças e muitos querem impor a sua verdade como se fosse a única existente ou possível. A ideia da supremacia racial, étnica, religiosa, de classe social, origem nacional, gênero, orientação sexual está presente na sociedade e cada dia se avulta mais nos meios de comunicação.

É nessa toada que se mostra imperiosa a análise dos crimes cibernéticos como nova forma de práticas criminosas e novo instrumento do delito, em especial o crime de racismo praticado pela internet, em paralelo com os direitos fundamentais da terceira dimensão, ou seja, os direitos ligados ao princípio da fraternidade.

O presente artigo tem como escopo fazer um exame das expressões racistas publicadas no mundo virtual e suas consequências jurídico-penais em análise conjunta com os direitos da terceira dimensão, colacionando o arcabouço legislativo nacional e tratados internacionais atrelados à matéria, bem como a visão doutrinária e a jurisprudência.

2 Os Crimes Cibernéticos

O elemento central no estudo dos crimes ou da teoria do delito é a conduta, a qual pode ser comissiva ou omissiva, dolosa ou culposa. No campo da conduta, o Direito Penal pátrio adotou a teoria finalista da ação, elaborada por Welzel. Para essa teoria, a conduta é o comportamento humano voluntário dirigido a um fim.

A conduta deve estar definida em lei como crime anteriormente à sua prática para que possa ser punida pelo Estado, atendendo-se ao princípio da legalidade insculpido no inciso XXXIX, do art. 5º, da Constituição Federal, segundo o qual *não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*. Tal princípio também está presente no art. 1º do Código Penal Brasileiro.

A conduta pode ser praticada de vários modos e meios. Com o avanço da tecnologia, novos instrumentos são utilizados para a prática de delitos tipificados no ordenamento jurídico-penal. Entre esses novos instrumentos estão o computador e os demais dispositivos eletrônicos. Quando esses meios são utilizados para a prática de um delito, podemos nomeá-los, segundo Carla Rodrigues Araújo de Castro, como crimes de informática.

A citada autora conceitua o crime de informática como sendo (CASTRO, 2003):

> aquele praticado contra o sistema de informática ou através deste, compreendendo os crimes praticados contra o computador e seus acessórios e os perpetrados através do computador. Inclui-se neste conceito os delitos praticados através da internet, pois pressuposto para acessar a rede é a utilização de um computador.
>
> Ainda, quando o crime é praticado através da internet, seja por computador ou por outro dispositivo conectado à rede de comunicação, intitula-se também de crime cibernético. (CASTRO, 2003)

Nesse viés, Roberto Antônio Darós Malaquias classifica os crimes cibernéticos em duas categorias: próprios e impróprios. E assim define cada uma delas (DARÓS MALAQUIAS, 2015):

> Crime cibernético próprio: é aquele que necessita do espaço virtual para ser praticado, ou seja, está diretamente relacionado com a utilização da tecnologia da informação e comunicação. Para facilitar a compreensão, têm-se como exemplos enquadrados neste grupo, a criação e disseminação de vírus e outros códigos maliciosos, a negação de serviços, a invasão e a destruição de bancos de dados (público ou privado) e tantos outros atos ilícitos;
>
> Crime cibernético impróprio: é aquele em que o computador ou a estação de trabalho transforma-se em instrumento para a prática do delito. Nesse grupo estão inseridos, a título de exemplo, os tipos penais comuns como a calúnia, a injúria, a difamação, o furto, o estelionato, a produção, a divulgação e a publicação de fotografias ou imagens contendo pornografia ou cenas de sexo explícito envolvendo crianças ou adolescentes e todos os demais delitos preceituados no Código Penal e nas leis especiais, possíveis de serem praticados com a utilização dessa citada ferramenta e das novas tecnologias. (DARÓS MALAQUIAS, 2015)

Portanto, os crimes cibernéticos são as condutas praticadas por meio de dispositivos conectados à rede mundial de computadores, seja com a finalidade de consumar atos que atinjam bens jurídicos ligados à informática propriamente dita ou a outras categorias protegidas pelo Direito.

No plano nacional há dispositivos legais penais voltados especialmente para a proteção de dados informáticos, como é o caso do *caput* do art. 154-A do Código Penal, acrescentado pela Lei nº 12.737, de 30 de novembro de 2012 (Lei Carolina Dieckmann), o qual tipifica a conduta de 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, punindo tal conduta com a pena de detenção de três meses a um ano e multa. O referido artigo ainda descreve nos seus parágrafos algumas hipóteses qualificadoras e causas de aumento de pena.

A mencionada lei de 2012 também incluiu na redação do art. 266 do Código Penal um parágrafo primeiro para tipificar a conduta de interromper serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar-lhe o restabelecimento, atribuindo uma pena de detenção de um a três anos e multa.

No que tange ao Direito Internacional Público, no território europeu foi elaborada no ano de 2001 a Convenção de Budapeste ou Convenção sobre o Cibercrime (*Budapest Convention on Cybercrime*), no bojo do Conselho da Europa, a qual tem por objetivo tratar da estruturação do combate aos crimes cibernéticos, aspectos processuais, cooperação internacional, recomendações legislativas, competência jurisdicional, troca de informações, extradição, entre outros assuntos relacionados.

Concluindo, cumpre registrar que esse documento internacional ainda não foi assinado pelo Brasil, sendo que no arcabouço de tratados do sistema interamericano de direitos humanos não há ainda nenhuma convenção que trate da matéria, tornando-se a Convenção de Budapeste uma diretriz a ser seguida pelos blocos regionais e por toda a comunidade global para o combate ao *cibercrime*.

3 O Crime de Racismo

O dicionário define racismo como a doutrina que sustenta a superioridade de certas raças (FERREIRA, 1993).

A Constituição Federal de 1988 estipula como um dos objetivos fundamentais da República Federativa do Brasil promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (art. 3º, IV). Outrossim, estipula como um dos princípios regentes das relações internacionais do Brasil o repúdio ao racismo (art. 4º, VIII).

Passo avante, a CF/88 determina no rol de direitos e garantias fundamentais do art. 5º, em seu inciso XLII, que a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei. Ou seja, a Lei Fundamental Brasileira prescreve um mandado de criminalização acerca da conduta consistente no racismo.

Portanto, nota-se pelo teor dos preceitos contidos na Constituição Federal que o repúdio ao racismo é verdadeiro princípio a ser seguido pelo legislador e por toda a sociedade brasileira, devendo ser previsto no ordenamento jurídico como crime a prática de atos de racismo.

Concretizando a ordem constitucional, foi editada a Lei nº 7.716, de 5 de janeiro de 1989 (Lei de Racismo), que define os crimes resultantes de preconceito de raça ou de cor. O art. 1º dessa lei determina que serão punidos os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, o que deixa claro que o racismo, para essa expressão legislativa, não se restringe ao preconceito ligado somente à cor ou raça, mas também ao que se refere à etnia, religião ou origem nacional.

Uma série de condutas penalmente puníveis são descritas na lei acima mencionada, em especial, no art. 20 em que restam tipificadas as condutas de praticar, induzir ou incitar a discriminação ou o preconceito de raça, cor, etnia, religião ou procedência nacional, cominando-lhe uma pena de reclusão de um a três anos e multa. E no seu parágrafo primeiro estão tipificadas as condutas de fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo, estipulando-se uma pena de reclusão dois a cinco anos e multa.

Os bens jurídicos protegidos são o direito à igualdade, bem como a dignidade da pessoa humana. É a pretensão ao respeito à personalidade humana, a própria dignidade da pessoa, considerada não só individualmente, como coletivamente (BALTAZAR JÚNIOR, 2017).

O Código Penal também possui dispositivo que tipifica conduta relacionada à discriminação ou ao preconceito ligado à raça, cor, etnia, religião, origem ou à condição de pessoa idosa ou portadora de deficiência, qual seja, o § 3º do art. 140, consistente na injúria em virtude das características pessoais acima expostas, determinando como conduta qualificada a injúria racial, diversa do crime de injúria previsto no *caput*, cominando-lhe pena de reclusão de um a três anos e multa.

Na esfera internacional, o Brasil é signatário no âmbito da ONU de um tratado que se refere ao combate ao racismo, a Convenção sobre a Eliminação de Todas as Formas de Discriminação Racial, assinada pelo Brasil em 7 de março de 1966, ratificada em 27 de março de 1968 e promulgada pelo Decreto nº 65.810, de 8 de dezembro de 1969.

No seu Artigo I, 1, a referida Convenção, ratificada e promulgada pelo Brasil por meio do Decreto acima, define discriminação racial como sendo:

> Qualquer distinção, exclusão, restrição ou preferência fundadas na raça, cor, descendência ou origem nacional ou étnica que tem por fim ou efeito anular ou comprometer o reconhecimento, o gozo ou o exercício, em igualdade de condições, dos direitos humanos e das liberdades fundamentais nos domínios político, econômico, social, cultural ou em qualquer outro domínio da vida pública.

Observa-se, portanto, que o arcabouço jurídico que visa proteger a igualdade e a dignidade da pessoa humana, no que tange ao combate à discriminação e ao preconceito, é vasto, estando presente na CF/88 tanto como objetivo da República, quanto como princípio regente das relações internacionais e como mandado de criminalização disposto com caráter de direito fundamental.

Ainda antes da Constituição, mas recepcionado por esta, o Brasil já havia assinado tratado internacional contra a discriminação racial, conforme acima mencionado.

Atendendo a tais mandamentos e evitando a proteção deficiente dos bens jurídicos tutelados pela Constituição, foram elaboradas normas penais que visam garantir os

direitos de igualdade e dignidade da pessoa humana a todos os indivíduos, utilizando como instrumento para o alcance dessa meta o direito criminal.

4 As dimensões de direitos fundamentais

A teoria das dimensões ou gerações de direitos trata-se de uma sistematização dogmática dos direitos fundamentais. A doutrina classifica os direitos em dimensões ou gerações de acordo com a natureza do princípio, em especial os princípios da liberdade, igualdade e fraternidade, dividindo-se, portanto, em três dimensões segundo a fase evolutiva constitucional.

O centro do Constitucionalismo a partir do advento da Constituição dos Estados Unidos da América e da Revolução Francesa são os direitos fundamentais. Direitos estes que se confundem com os direitos humanos protegidos nacional e internacionalmente.

Editada a Constituição dos Estados Unidos da América e a Declaração dos Direitos do Homem na França, ao final do século XVIII, ali estavam presentes direitos de caráter individual que visavam garantir, primordialmente, a liberdade do ser humano em face do Estado, com base nos ideais iluministas. Assim aconteceu com as demais constituições na fase moderna do constitucionalismo. Tais direitos são considerados pela doutrina como a primeira dimensão ou geração dos direitos fundamentais.

Com a revolução industrial e a exploração do homem pelo homem na esfera privada, uma nova necessidade surgiu: a defesa da igualdade. Com isso passaram a ser prescritos nas Constituições princípios e normas que buscavam garantir direitos sociais, tendo como marcos iniciais dessa fase a Carta Fundamental do México de 1917 e a Constituição Alemã de Weimar de 1919. A dogmática jurídica categorizou esses direitos como sendo da segunda dimensão.

Em um terceiro momento, após a Segunda Guerra Mundial, novos direitos passaram a ser necessários para a verdadeira concretização dos ideais do constitucionalismo. Entrava-se, portanto, nos direitos da terceira dimensão, que se ligam ao princípio da fraternidade.

André de Carvalho Ramos explica de forma clara a teoria das dimensões ou gerações de direitos (RAMOS, 2016):

> A teoria das gerações dos direitos humanos foi lançada pelo jurista francês de origem checa, Karel Vasak, que, em conferência proferida no Instituto Internacional de Direitos Humanos de Estrasburgo (França), no ano de 1979, classificou os direitos humanos em três gerações, cada uma com características próprias. [...]. Cada geração foi associada a um dos componentes do dístico da Revolução Francesa: *liberte, egalité et fraternité* (liberdade, igualdade e fraternidade). [...] A primeira geração engloba os chamados direitos de liberdade, que são direitos às prestações negativas, nas quais o Estado deve proteger a esfera de autonomia do indivíduo. São denominadas também "direitos de defesa", pois protegem o indivíduo contra intervenções indevidas do Estado, possuindo caráter de distribuição de competências (limitação) entre o Estado e o ser humano. [...] A segunda geração de direitos humanos representa a modificação do papel do Estado, exigindo-lhe um vigoroso papel ativo, além do mero fiscal das regras jurídicas. [...] O direitos sociais são também titularizados pelo indivíduo e oponíveis ao Estado. São reconhecidos o direito à saúde, educação, previdência social, habitação, entre outros, que demandam prestações positivas do Estado para seu atendimento e são denominados direitos de igualdade por garantirem, justamente às camadas mais miseráveis da sociedade, a concretização das liberdades abstratas reconhecidas nas primeiras declarações de direitos. [...]. Já os direitos de terceira geração são aqueles de titularidade da comunidade, como o direito ao desenvolvimento, direito à paz, direito à autodeterminação e, em especial, o direito ao meio ambiente equilibrado. (RAMOS, 2016)

O Supremo Tribunal Federal sustenta suas decisões com base na teoria das gerações ou dimensões dos direitos fundamentais, conforme se toma como exemplo trecho da decisão a seguir colacionada:

> [...] A questão do direito ao meio ambiente ecologicamente equilibrado – direito de terceira geração – princípio da solidariedade. O direito a integridade do meio ambiente – típico direito de terceira geração – constitui prerrogativa jurídica de titularidade coletiva, refletindo dentro do processo de afirmação dos direitos humanos, a expressão significativa de um poder atribuído, não ao indivíduo identificado em sua singularidade, mas, num sentido verdadeiramente mais abrangente, a própria coletividade social. Enquanto os direitos de primeira geração (direitos civis e políticos) – que compreendem as liberdades clássicas, negativas ou formais – realçam o

> princípio da liberdade e os direitos da segunda geração (direitos econômicos, sociais e culturais) – que se identifica com as liberdades positivas, reais ou concretas – acentuam o princípio da igualdade, os direitos de terceira geração, que materializam poderes de titularidade coletiva atribuídos genericamente a todas as formações sociais, consagram o princípio da solidariedade e constituem um momento importante no processo de desenvolvimento, expansão e reconhecimento dos direitos humanos, caracterizados, enquanto valores fundamentais indisponíveis, pela nota de uma essencial inexauribilidade. (MS 22164, Relator: Min. Celso de Mello, Tribunal Pleno, julgado em 30/10/1995).

Dessarte, a teoria das dimensões dos direitos é uma forma de classificação dos direitos fundamentais, conforme a evolução individual, social, cultural e econômica da sociedade em paralelo com o advento das constituições nacionais, local onde atualmente se abrange o teor dos tratados internacionais de direitos humanos firmados em plano global ou regional, visando ao atendimento dos valores e princípios garantidores de direitos naturais historicamente conquistados e/ou almejados pelo ser humano.

5 O racismo cibernético e os direitos de terceira dimensão

A Constituição Federal tem como vetores principais a dignidade da pessoa humana e a busca pela igualdade material (Preâmbulo, art. 1º, III e art. 5º, *caput*). Além disso, assevera como princípio o pluralismo de ideias e de concepções pedagógicas, estando esse termo presente no art. 206 como um dos princípios do ensino e, é claro, trata-se de uma vertente dos princípios da igualdade e da dignidade da pessoa humana.

O texto do art. 216 da CF/88 demonstra de forma implícita que o pluralismo deve ser buscado pelo ordenamento jurídico e pela sociedade como um todo, elencando um rol de bens materiais e imateriais que constituem o patrimônio cultural brasileiro:

> Art. 216. Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:
> I – as formas de expressão;
> II – os modos de criar, fazer e viver;

> III – as criações científicas, artísticas e tecnológicas;
> IV – as obras, objetos, documentos, edificações e demais espaços destinados às manifestações artístico culturais;
> V – os conjuntos urbanos e sítios de valor histórico, paisagístico, artístico, arqueológico, paleontológico, ecológico e científico.

Assim, nota-se a importância de se proteger as diferenças entre os indivíduos, punindo condutas que emanem discriminação e preconceito. Nessa toada, o Direito Penal surge como importante instrumento de atendimento ao fim buscado pela Constituição no que se refere à igualdade, à dignidade da pessoa humana e ao pluralismo, sob pena de o Estado incorrer na proteção deficiente desses bens jurídicos.

Farias destaca que:

> A fim de solucionar a tão presente problemática da discriminação racial, alguns países, como é o caso do Brasil, por exemplo, vê no Direito Penal, através da criminalização das condutas dessa natureza, a melhor forma de coibir a discriminação racial e corrigir as injustiças causadas pelas suas terríveis consequências à sociedade como um todo. (FARIAS, 2015)

A partir daí se manifesta a produção legislativa com o advento da Lei nº 7.716/1989 e o previsto no § 3º do art. 140 do Código Penal, punindo condutas que disseminem a discriminação e o preconceito em virtude de raça, cor, etnia, religião ou procedência nacional.

Importante destacar que a conduta visada pelo tipo do art. 140, § 2º, do Código Penal é aquela direcionada a alguém individualmente, ou seja, um ato de injúria racial praticado contra uma vítima individualizada. Diferentemente, a conduta objetivada pelo tipo contido no art. 20 da Lei nº 7.716/1989 (crime de racismo) é aquela que atinge uma coletividade ou grupo.

Ainda, o § 2º do art. 20 da Lei nº 7.716/1989 qualifica a conduta tipificada no *caput* quando cometida por intermédio dos meios de comunicação social ou publicação de qualquer natureza, cominando-lhe a pena de reclusão de dois a cinco anos e multa.

Ao mesmo tempo a liberdade de expressão é também um direito fundamental consagrado pela Constituição Federal em seu art. 5º, IX, prevendo que *é livre a expressão da atividade intelectual, artística, científica e de comunicação*.

Frisa-se que o Supremo Tribunal Federal já considerou a liberdade de expressão como sendo um direito preferencial *prima facie* e de elevado valor, sendo necessária uma carga argumentativa muito forte para que outro direito se sobreponha a ele em uma ponderação de princípios, como se observa no julgamento da ADI 4815/DF, de relatoria da ministra Cármen Lúcia, no qual o Plenário do STF julgou procedente a ação para declarar inexigível a autorização prévia para publicação de biografias (ADI 4815/DF – Biografias não autorizadas – Rel. Min. Cármen Lúcia).

Por outro lado, a Corte Suprema já decidiu que a liberdade de expressão comporta limitações, não estando em sua esfera de abrangência o *hate speech* ou discurso de ódio, devendo ser punidas as condutas de discriminação e preconceito publicamente proferidas, não podendo ser reconhecida como livre a expressão de posições claramente racistas. Além disso, o STF definiu que raça e racismo não se tratam de termos ligados meramente à cor ou etnia, mas sim de critérios sociais e históricos. Assim decidiu a Corte no paradigmático caso Ellwanger:

> HABEAS-CORPUS. PUBLICAÇÃO DE LIVROS: ANTI-SEMITISMO. RACISMO. CRIME IMPRESCRITÍVEL. CONCEITUAÇÃO. ABRANGÊNCIA CONSTITUCIONAL. LIBERDADE DE EXPRESSÃO. LIMITES. ORDEM DENEGADA. 1. Escrever, editar, divulgar e comerciar livros "fazendo apologia de idéias preconceituosas e discriminatórias" contra a comunidade judaica (Lei 7716/89, artigo 20, na redação dada pela Lei 8081/90) constitui crime de racismo sujeito às cláusulas de inafiançabilidade e imprescritibilidade (CF, artigo 5º, XLII). 2. Aplicação do princípio da prescritibilidade geral dos crimes: se os judeus não são uma raça, segue-se que contra eles não pode haver discriminação capaz de ensejar a exceção constitucional de imprescritibilidade. Inconsistência da premissa. 3. Raça humana. Subdivisão. Inexistência. Com a definição e o mapeamento do genoma humano, cientificamente não existem distinções entre os homens, seja pela segmentação da pele, formato dos olhos, altura, pêlos ou por quaisquer outras características físicas, visto que todos se qualificam como espécie humana. Não há diferenças biológicas entre os seres humanos. Na essência são todos iguais. 4. Raça e racismo. A divisão dos seres humanos em raças resulta de um processo de conteúdo meramente político-social. Desse pressuposto origina-se o racismo que, por sua vez, gera a discriminação e o preconceito segregacionista. 5. Fundamento do núcleo do pensamento do nacional-socialismo de que os judeus e os arianos formam raças distintas. Os primeiros seriam raça inferior, nefasta e infecta, características suficientes para justificar a segregação e

o extermínio: inconciabilidade com os padrões éticos e morais definidos na Carta Política do Brasil e do mundo contemporâneo, sob os quais se ergue e se harmoniza o estado democrático. Estigmas que por si só evidenciam crime de racismo. Concepção atentatória dos princípios nos quais se erige e se organiza a sociedade humana, baseada na respeitabilidade e dignidade do ser humano e de sua pacífica convivência no meio social. Condutas e evocações aéticas e imorais que implicam repulsiva ação estatal por se revestirem de densa intolerabilidade, de sorte a afrontar o ordenamento infraconstitucional e constitucional do País. 6. Adesão do Brasil a tratados e acordos multilaterais, que energicamente repudiam quaisquer discriminações raciais, aí compreendidas as distinções entre os homens por restrições ou preferências oriundas de raça, cor, credo, descendência ou origem nacional ou étnica, inspiradas na pretensa superioridade de um povo sobre outro, de que são exemplos a xenofobia, "negrofobia", "islamafobia" e o anti-semitismo. 7. A Constituição Federal de 1988 impôs aos agentes de delitos dessa natureza, pela gravidade e repulsividade da ofensa, a cláusula de imprescritibilidade, para que fique, ad perpetuam rei memoriam, verberado o repúdio e a abjeção da sociedade nacional à sua prática. 8. Racismo. Abrangência. Compatibilização dos conceitos etimológicos, etnológicos, sociológicos, antropológicos ou biológicos, de modo a construir a definição jurídico-constitucional do termo. Interpretação teleológica e sistêmica da Constituição Federal, conjugando fatores e circunstâncias históricas, políticas e sociais que regeram sua formação e aplicação, a fim de obter-se o real sentido e alcance da norma. 9. Direito comparado. A exemplo do Brasil as legislações de países organizados sob a égide do estado moderno de direito democrático igualmente adotam em seu ordenamento legal punições para delitos que estimulem e propaguem segregação racial. Manifestações da Suprema Corte Norte-Americana, da Câmara dos Lordes da Inglaterra e da Corte de Apelação da Califórnia nos Estados Unidos que consagraram entendimento que aplicam sanções àqueles que transgridem as regras de boa convivência social com grupos humanos que simbolizem a prática de racismo. 10. A edição e publicação de obras escritas veiculando idéias anti-semitas, que buscam resgatar e dar credibilidade à concepção racial definida pelo regime nazista, negadoras e subversoras de fatos históricos incontroversos como o holocausto, consubstanciadas na pretensa inferioridade e desqualificação do povo judeu, equivalem à incitação ao discrímen com acentuado conteúdo racista, reforçadas pelas conseqüências históricas dos atos em que se baseiam. 11. Explícita conduta do agente respon-

> sável pelo agravo revelador de manifesto dolo, baseada na equivocada premissa de que os judeus não só são uma raça, mas, mais do que isso, um segmento racial atávica e geneticamente menor e pernicioso. 12. Discriminação que, no caso, se evidencia como deliberada e dirigida especificamente aos judeus, que configura ato ilícito de prática de racismo, com as conseqüências gravosas que o acompanham. 13. Liberdade de expressão. Garantia constitucional que não se tem como absoluta. Limites morais e jurídicos. O direito à livre expressão não pode abrigar, em sua abrangência, manifestações de conteúdo imoral que implicam ilicitude penal. 14. As liberdades públicas não são incondicionais, por isso devem ser exercidas de maneira harmônica, observados os limites definidos na própria Constituição Federal (CF, artigo 5º, § 2º, primeira parte). O preceito fundamental de liberdade de expressão não consagra o "direito à incitação ao racismo", dado que um direito individual não pode constituir-se em salvaguarda de condutas ilícitas, como sucede com os delitos contra a honra. Prevalência dos princípios da dignidade da pessoa humana e da igualdade jurídica. 15. "Existe um nexo estreito entre a imprescritibilidade, este tempo jurídico que se escoa sem encontrar termo, e a memória, apelo do passado à disposição dos vivos, triunfo da lembrança sobre o esquecimento". No estado de direito democrático devem ser intransigentemente respeitados os princípios que garantem a prevalência dos direitos humanos. Jamais podem se apagar da memória dos povos que se pretendam justos os atos repulsivos do passado que permitiram e incentivaram o ódio entre iguais por motivos raciais de torpeza inominável. 16. A ausência de prescrição nos crimes de racismo justifica-se como alerta grave para as gerações de hoje e de amanhã, para que se impeça a reinstauração de velhos e ultrapassados conceitos que a consciência jurídica e histórica não mais admitem. Ordem denegada. (HC 82424, Relator(a): Min. MOREIRA ALVES, Relator(a) p/ Acórdão: Min. MAURÍCIO CORRÊA, Tribunal Pleno, julgado em 17/09/2003, DJ 19-03-2004 PP-00017 EMENT VOL-02144-03 PP-00524).

Portanto, atitudes racistas devem ser punidas mesmo que proferidas como divulgação de ideias. E, nos dias de hoje, o local mais apropriado e fácil para a divulgação de ideias e/ou ideais é o ambiente virtual, a internet, surgindo esta como instrumento para a prática de condutas que podem ser categorizadas como racismo.

É nesse momento que se interligam os direitos da terceira dimensão e a proteção do pluralismo, considerando que a comunicação e a liberdade de expressão são meios para a consecução da liberdade de forma ampla e da igualdade em suas várias vertentes.

Nesse sentido, vejamos as lições de Paulo Bonavides acerca dos direitos fundamentais da terceira geração:

> Com efeito, um novo polo jurídico de alforria do homem se acrescenta historicamente aos da liberdade e da igualdade. Dotados de altíssimo teor de humanismo e universalidade, os direitos da terceira geração tendem a cristalizar-se no fim do século XX enquanto direitos que não se destinam especificamente à proteção dos interesses de um indivíduo, de um grupo ou de um determinado Estado. Têm primeiro por destinatário o gênero humano mesmo, num momento expressivo de sua afirmação como valor supremo em termos de existencialidade concreta. [...] Emergiram eles da reflexão sobre temas referentes ao desenvolvimento, à paz, ao meio ambiente, à *comunicação* e ao patrimônio comum da humanidade. (BONAVIDES, 2013)

Podemos destacar, dos direitos da terceira dimensão, a comunicação, o desenvolvimento, a paz e o patrimônio comum da humanidade como de tênue ligação com a "realidade cibernética", a qual tem um caráter nitidamente transindividual e difuso, referente à tecnologia e evolução da humanidade, estando presente em todas as esferas de atuação humana.

Nesse diapasão, Sarlet leciona acerca dos direitos da terceira dimensão referindo que

> Cuida-se, na verdade, do resultado de novas reivindicações fundamentais do ser humano, geradas dentre outros fatores, pelo impacto tecnológico, pelo estado crônico de beligerância, bem como pelo processo de descolonização do segundo pós-guerra e suas contundentes consequências, acarretando profundos reflexos na esfera dos direitos fundamentais. [...] Para outros, por sua vez, os direitos fundamentais da terceira dimensão, como leciona Pérez Luño, podem ser considerados uma resposta ao fenômeno denominado de *poluição das liberdades*, que caracteriza o processo de erosão e degradação sofrido pelos direitos e liberdades fundamentais, principalmente em face do uso de *novas tecnologias*. Nesta perspectiva, assumem especial relevância o direito ao meio ambiente e à qualidade de vida, bem como o *direito de informática (ou liberdade de informática)*, cujo

> reconhecimento é postulado justamente em virtude do controle cada vez maior sobre a liberdade e intimidade individual mediante bancos de dados pessoais, meios de comunicação, etc. [...] (SARLET, 2011)

São inúmeros os meios de comunicação via internet atualmente disponíveis (computador, *smatphone*, *tablet*, smartTV), bem como os espaços virtuais, como as redes sociais (Facebook, Twitter, Linkedin, Instagram) e demais páginas da internet onde se publicam conteúdos que passam a ser acessíveis a todos que estejam conectados. Portanto, fácil é a difusão de ideias via internet e rápido o alcance a um número cada vez maior de pessoas. Dessarte, devida e necessária a proteção contra as palavras, imagens e vídeos racistas publicados no campo virtual.

Realçando a importância do tema, houve um caso notório na mídia nacional em que a apresentadora negra Maria Júlia Coutinho, do Jornal Nacional, da Rede Globo de televisão, sofreu inúmeras ofensas em virtude de sua cor em rede social (Facebook), dando azo à discussão nos meios de comunicação.

Tal caso, conforme nosso entendimento, caracterizou injúria racial, conduta insculpida no tipo do art. 140, § 3º, do Código Penal, muito embora haja interpretações de que também havia se caracterizado o crime de racismo.

Na seara do Direito Internacional, inclusive, a própria Convenção de Budapeste sobre o Cibercrime, de acordo com o disposto no seu Protocolo Adicional Relativo à Incriminação de Atos de Natureza Racista e Xenófoba Praticados Através de Sistemas Informáticos, adotado em 28 de janeiro de 2003 e com entrada em vigor na ordem internacional em 1º de março de 2006, orienta os Estados signatários a tipificar criminalmente infrações relacionadas aos conteúdos de racismo e xenofobia praticados por meio da internet, a distribuição, ou outras formas de disponibilização ao público, mediante um sistema informático, de material racista e xenófobo (art. 3º); a ameaça, por meio de um sistema informático, de cometer uma infração penal grave nos termos do seu direito interno contra: i) um indivíduo por força da sua pertença a um grupo identificado pela raça, cor, ascendência, origem nacional ou étnica e religião, se for utilizada como pretexto para qualquer um destes elementos; ii) um grupo de indivíduos identificado por qualquer uma dessas características (art. 4º); o insulto em público, mediante um sistema informático: i) dirigido a um indivíduo por força da sua pertença a um grupo identificado pela raça, cor, ascendência, origem nacional ou étnica e religião, se for utilizado como pretexto para qualquer um desses elementos; ii) dirigido a um grupo de indivíduos identi-

ficado por qualquer uma dessas características (art. 5º); a distribuição, ou outras formas de disponibilização ao público, por intermédio de um sistema informático, de material que negue, grosseiramente minimize, aprove ou justifique atos constitutivos de crimes de genocídio ou de crimes contra a humanidade, tal como definidos no direito internacional [...] (art. 6º).

O Estatuto de Roma do Tribunal Penal Internacional, convenção assinada pelo Brasil e promulgada pelo Decreto nº 4.388, de 25 de setembro de 2002, dispõe em seu art. 6º sobre o crime de genocídio, definindo este como qualquer prática com intenção de destruir, no todo ou em parte, um grupo nacional, étnico, racial ou religioso, por meio de atos definidos em suas alíneas tais como as ofensas graves à integridade física ou mental de membros do grupo (alínea b).

No mesmo sentido, a Lei nº 2.889, de 1º de outubro de 1956, que tipifica a conduta de genocídio no Brasil, descreve que: pratica esse crime quem, com a intenção de destruir, no todo ou em parte, grupo nacional, étnico, racial ou religioso, causar lesão grave à integridade mental de membros do grupo, entre as ações previstas nas alíneas do seu art. 1º.

Ou seja, são inúmeras as condutas tipificadas como crime e é extenso o arcabouço jurídico-penal, nacional e internacional, que visa proteger os direitos à diversidade cultural, racial, econômica, étnica, religiosa e demais diferenças que são asseguradas pela Constituição Federal de 1988, aproximando-se do fim visado pelo ordenamento fundamental, qual seja, a dignidade da pessoa humana.

Tais condutas racistas também, quando praticadas no âmbito do mundo digital, merecem ser severamente combatidas, vez que elementos legais e jurídicos para tanto já existem no ordenamento jurídico brasileiro, e, muito embora o Brasil não tenha ainda assinado a Convenção de Budapeste, fato é que seus princípios e orientações de combate ao racismo e à xenofobia são seguidos pela nossa legislação.

Outrossim, como acima exposto, o Supremo Tribunal Federal já se manifestou no sentido de que as ofensas proferidas publicamente com caráter racista não estão protegidas pelo manto do direito fundamental à liberdade de expressão, sofrendo, portanto, limitação e alcance do Direito Penal com possibilidade de punição estatal.

6 Conclusão

Os direitos da terceira dimensão francamente ligados ao princípio da fraternidade permeiam todo o ordenamento jurídico pátrio, não podendo ser diferente com o Direito Penal. Entre os direitos elencados como sendo da terceira dimensão estão a paz, a proteção ao meio ambiente, a autodeterminação, a proteção do patrimônio comum, o desenvolvimento, os direitos da comunicação e os direitos informáticos.

A Constituição Federal determina no seu Preâmbulo a busca por uma sociedade fraterna e no seu corpo estipula uma série de direitos ligados a esse princípio, tendo como vértice axiológico a dignidade da pessoa humana.

Assim, o Direito Penal aparece como instrumento de proteção social desses bens jurídicos e num mundo hoje digital, assegurar esses direitos no âmbito cibernético é uma necessidade premente, em especial, quando se está em jogo a diversidade, o pluralismo e a igualdade, devendo ser penalmente punidas as condutas racistas praticadas por meio da internet, conforme se observa da legislação e jurisprudência supramencionada, sob pena de proteção deficiente dos direitos da terceira dimensão.

Busca-se, afinal, liberdade, igualdade, *fraternidade, tecnologia!*

Referências

BALTAZAR JUNIOR, José Paulo. **Crimes Federais**. 11. ed. São Paulo: Saraiva, 2017.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 28. ed. São Paulo: Malheiro Editores, 2013.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

DARÓS MALAQUIAS, Roberto Antônio. **Crime cibernético e prova**: a investigação criminal em busca da verdade. 2 ed. Curitiba: Juruá, 2015.

FARIAS, Vilson. **Racismo à luz do Direito Criminal (com incursão no Direito Comparado)** – aspectos materiais, processuais e sociológicos. Pelotas: Livraria Mundial, 2015.

FERREIRA, Aurélio Buarque de Holanda. **Minidicionário da língua portuguesa**. 3. ed. Rio de Janeiro: Nova Fronteira, 1993.

RAMOS, André de Carvalho. **Curso de Direitos Humanos**. 3. ed. São Paulo: Saraiva, 2016.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 10. ed. Porto Alegre: Livraria do Advogado, 2011.

7 CIBERESPIONAGEM: ENTRAVES NA APURAÇÃO DE PROVAS E RESPONSABILIZAÇÃO PENAL

André Luís Woloszyn[1]

Resumo: O presente artigo se propõe a analisar a ciberespionagem internacional, classificada como delito contra a segurança do Estado, sob a égide da legislação nacional e internacional, com viés na prática perpetuada por governos contra outros governos, voltados à obtenção de segredos comerciais, industriais e governamentais, bem como seus impactos na sociedade e na governabilidade. Identifica os diferentes entraves na apuração de autores, provas e responsabilização penal. Conclui que os mecanismos tecnológicos e legais à disposição do país não são suficientes para assegurar uma proteção adequada às informações sensíveis de caráter governamental. Sugere, como alternativas, a adoção de políticas públicas de educação digital somada a investimentos em pesquisa e desenvolvimento de uma tecnologia cibernética nacional que dê suporte técnico à legislação de combate aos crimes cibernéticos.

Palavras-chave: Crimes cibernéticos. Legislação. Ciberespionagem. Segurança nacional. Impactos. Entraves na apuração.

Abstract: *This paper aims to analyze the international cyber-spying, classified as a crime against State security, under the aegis of national and international legislation, with bias in perpetuated practice by governments against other governments, aimed at obtaining industrial and governamental trade secrets, as well as its impacts on society and governance. It identifies the different obstacles in the investigation of authors, evidence and criminal responsibility. The conclusion is that the technological and legal mechanisms available to the country are not sufficient to ensure adequate protection of sensitive information of governmental kind. It suggests, as alternatives, the adoption of public policies of digital education combined with investments in research and development of a national cyber technology that provides technical support to legislation to combat cybercrime.*

Keywords: Cybercrimes. Legislation. Cyber-spying. National security. Impacts. Obstacles in the investigation.

1 Mestre em Direito pela UniRitter – Laureate International Universities, especialista em Ciências Penais pela Universidade Federal do Rio Grande do Sul, diplomado em Inteligência Estratégica pela Escola Superior de Guerra e assessor de Segurança Institucional do Ministério Público Federal, Procuradoria da República no Rio Grande do Sul.

1 Introdução

O tema da ciberespionagem é paradoxal. Isso porque, enquanto os países da comunidade internacional condenam sua prática, considerando-a um crime de natureza grave contra a segurança do Estado em suas legislações internas, ao mesmo tempo fomentam e desenvolvem tecnologias avançadas para sua utilização sistemática contra outros governos na busca por segredos de Estado, envolvendo todas as expressões do poder nacional, quer industriais, tecnológicas, econômicas, diplomáticas ou militares.

Uma primeira pesquisa etimológica revela que ciberespionagem tem sua raiz na expressão espionar, ação que remonta à Antiguidade, revelada por clássicos de estratégia como a Arte da Guerra, de Sun Tzu, escrita por volta do século IV a.C, e na obra de mesmo título escrita por Nicolas Maquiavel, em meados do século XV.

Da Antiguidade até o período em que Manual Castell classificou como a era da informação, referindo-se à segunda metade do séc. XIX, alcançada com o desenvolvimento da internet e das tecnologias eletrônicas e digitais, era realizada exclusivamente por fontes humanas, por meio de técnicas de observação, memorização e descrição. Tratava-se de um instrumento direcionado a manter e ampliar o poder de governos, em questões diplomáticas e em conflitos bélicos.

Espionagem, na definição de Cepik[2], é a atividade de coleta de informações sem o consentimento e cooperação de parte dos alvos da ação. Para Volkman[3], significa o ato de obter informações secretas militares, políticas, econômicas e outras de uma nação-estado, por meio do uso de espiões, monitoramento ou outros meios.

De outro giro, a criação da internet, na década de 1960, durante a Guerra Fria e sua massificação, promovida na década de 1990, somadas, paulatinamente, ao fenômeno da globalização econômica, caracterizado por mercados em alta competitividade, oportunizou novas perspectivas para governos, empresas e profissionais explorarem a espionagem no meio digital.

Com efeito, a lição de Fiorillo e Conte assim manifesta:

2 CEPIK, Marco. Inteligência e políticas públicas: dinâmicas operacionais e condições de legitimação. **Security and Defense Studies Review**, v. 2, p. 249, winter, 2002-2003.

3 VOLKMAN, Ernest. **A história da espionagem**. Tradução Ciro Mioranza e Antônio Carlos Braga, São Paulo: Ed. Escala, 2013, p. 7.

> […] O problema da internet passou a ser identificado quando a tecnologia começou a interferir nas relações sociais pacíficas e controladas, assim como possibilitou algumas práticas socialmente desagradáveis, como sua utilização para a perpetuação de delitos e criação de novos contatos que colocam em risco bens que ainda não tiveram sua relevância reconhecida pelo direito[4].

Na mesma linha argumentativa, Alvin Toffler, ainda na década de 1980, advertia que o desenvolvimento de todo esse processo tecnológico acarretaria, paralelamente, para a sociedade sérios efeitos colaterais. Referindo-se à espionagem, no contexto da era da informação, assevera:

> […] o agente espião é uma das mais poderosas metáforas do nosso tempo pois vem equipado com a última e mais exótica tecnologia: microfones eletrônicos, bancos de computadores, câmeras infravermelhas, [...] pois o negócio básico da espionagem é a informação. E a informação, tornou-se talvez o negócio mais importante e o que mais cresce no mundo. O espião é um símbolo vivo da revolução que hoje invade a infosfera[5].

O fenômeno recrudesce, com a dependência irreversível e cada vez mais acentuada da sociedade internacional em sistemas e redes digitais. Como profetizou Castell[6], com seu conceito de sociedade em rede e o desvirtuamento do ciberespaço para outras finalidades que iriam além da democratização do conhecimento.

Surgiram, assim, os chamados crimes cibernéticos e a ciberespionagem, definida como a invasão a sistemas informáticos e digitais na busca por informações sensíveis, protegidas por grau de sigilo.

Como asseveram Falcão Júnior e Buffon, referindo-se ao ciberterrorismo como um conceito polêmico por oscilar entre a criminalidade de condutas civis e democrática e a punição de atos qualificados como guerra[7], na ciberespionagem a oscilação se dá entre

4 FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013, p. 14.

5 TOFFLER, Alvin. **A terceira onda**. Tradução de João Távora. Rio de Janeiro: Record, 1980. p. 161-162.

6 CASTELLS, Manuel. **A sociedade em rede**: a era da informação, economia, sociedade e cultura. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999, v. 1. p. 69.

7 SILVA, Ângelo Roberto Ilha da; SHIMABUKURO, Angela (Org.). Crimes Cibernéticos.: In: FALCÃO JÚNIOR, Alfredo Carlos G.; BUFFON, Jaqueline Ana. **Ciberterrorismo**: entre a prevenção e o combate. Porto Alegre: Livraria do Advogado, 2017, p.155.

condutas adotadas por agentes governamentais sob proteção legal e a punição de atos qualificados como segurança do Estado.

Devido à relevância do tema e os reflexos nefastos que acarretam o desenvolvimento e o progresso de uma nação, este artigo se propõe a analisar a ciberespionagem sob a égide da legislação nacional e internacional, com viés na prática perpetuada por governos contra outros governos, voltados à obtenção de segredos comerciais, industriais e governamentais, considerados informações estratégicas[8] e seus impactos na sociedade e na governabilidade. Por fim, conclui que os mecanismos tecnológicos e legais à disposição não são suficientes para assegurar uma proteção adequada às informações sensíveis de caráter governamental.

2 Aspectos gerais da ciberespionagem

O crime de ciberespionagem se reveste de alta complexidade, uma vez que necessita do domínio da tecnologia digital, passando ao longe da espionagem tradicional. Trata-se não somente da invasão de sistemas digitais para subtração de documentos sensíveis, mas, sobretudo, da inserção de programas de *malwares* configurados especificamente para tal finalidade.

Nela, a proteção contra riscos, ameaças e vulnerabilidades é direcionada para o sistema informático que tem como bem jurídico tutelado pela norma a informação sensível de natureza estratégica para o país. O emblemático nesse contexto é que quando é identificada uma invasão, a *priori*, pelo decurso de tempo, os danos já são irreparáveis.

Woloszyn[9] assevera que entre suas características principais estão a possibilidade de ser praticada fora do território nacional, dificuldades em identificar a fonte, facilidade de encobrimento por rastros e perfis falsos no intuito de confundir as investigações ou, ainda, de atribuir a responsabilidade a terceiros, além de custos relativamente baixos.

8 Os conhecimentos considerados estratégicos permitem à nação detentora o domínio tecnológico, o poderio econômico, político e militar, as vantagens nas relações comerciais, entre outros. Os países, ao perceberem tal singularidade, atribuem uma proteção especial ao conhecimento e fortes restrições de divulgação, venda e transferência de tecnologia, tendo-se em tela a manutenção do sigilo sobre este. FREITAS, Neisser Oliveira. Aspectos jurídico-históricos das Patentes de Interesse da Defesa Nacional. **Revista Brasileira de Inteligência**. Brasília, DF: Abin, n. 6, p. 60, 2005.

9 WOLOSZYN, André Luís. **Vigilância e Espionagem Digital**: a legislação internacional e o contexto brasileiro. Curitiba: Juruá, 2016. p. 62.

O problema se intensifica quando envolve governos, uma vez que as ações podem ser facilmente dissimuláveis pelos meios legais que os Estados possuem para determinar seu uso e, ao mesmo tempo, encobri-la na forma da lei.

Assim como os crimes cibernéticos praticados contra pessoas e instituições, os efeitos da ciberespionagem nas expressões do poder nacional atingem indiretamente a sociedade, como podemos observar logo a seguir:

Tabela 1 – Consequências da ciberespionagem nas expressões do poder nacional

Expressões do poder nacional	Consequências
Indústria	Queda da competitividade mercadológica e desemprego.
Ciência e tecnologia	Evasão de divisas resultante da violação de segredos industriais e tecnológicos, acarretando na perda de patentes e perdas de recursos financeiros em pesquisas.
Economia	Desequilíbrio da balança comercial, em especial, na exportação e importação de produtos, o que trará consequências diretas no Produto Interno Bruto (PIB) e na taxa de crescimento do país.
Segurança e Defesa	Avaliação das vulnerabilidades do país, suas deficiências e necessidades, visando criar oportunidades de negócios para empresas que fornecem armas e equipamentos bélicos, um dos ramos mais rentáveis do comércio internacional ou, simplesmente, medir sua capacidade de reação.
Política interna	Conhecimento sobre tendências políticas e ideológicas e a posição do país em questões de cunho internacional.
Política internacional	Perda da credibilidade internacional e a consequente redução de investimentos externos, além de constrangimentos diplomáticos.

Fonte: Woloszyn (2016, p. 63)

Pela análise das consequências descritas, ficam evidenciados os efeitos na sociedade, uma vez que reduzem o potencial econômico do país atingido. Tal redução impacta a competitividade tecnológica, industrial e mercadológica, o que traz desemprego e recessão, importando na redução de investimentos em políticas e serviços públicos.

Ainda sobre os impactos econômicos da ciberespionagem, estima-se que as perdas anuais sejam da ordem de US$ 800 milhões a US$ 1 bilhão de dólares/ano, em valores de propriedade intelectual. Em termos gerais, os números podem atingir US$ 500 bilhões/ano. Para a economia dos EUA, considerando a taxa de exportação e uma estimativa de extinção de 508 mil postos de trabalho, os prejuízos atingem entre US$ 70 e US$ 140 bilhões[10].

10 MINGST, Karen; TOFT, Ivan M. Arreguín. **Princípios das Relações Internacionais**. Tradução de Cristina de Assis Serra. Rio de Janeiro: Elsevier, 2014. p. 126.

Todavia, o despertar de uma consciência mais efetiva em relação a essa grave ameaça é recente. Sobreveio, a partir do ano de 2010, com dois acontecimentos singulares. O primeiro, ocorrido nesse mesmo ano, com a divulgação de milhares de documentos confidenciais do governo norte-americano pelo site *Wikileaks*, de Júlio Assange, acerca da diplomacia externa e das operações militares e de inteligência no Iraque e Afeganistão.

Em 2013, ocorreria o segundo episódio, envolvendo o ex-funcionário da *Central Intelligence Agency* (CIA) e da *National Security Agency* (NSA), Edward Snowden, que comprovou casos de ciberespionagem internacional cujo principal alvo eram as comunicações on-line de milhares de pessoas ao redor do mundo, sob pretexto da segurança nacional contra o terrorismo e proteção preventiva contra o uso de armas de destruição em massa por agentes não estatais. Restou comprovada, também, a ciberespionagem direcionada a autoridades governamentais de primeiro escalão em diferentes nações, incluindo a presidente Dilma Roussef e alguns de seus principais assessores, tendo esta recebido um pedido de desculpa formal do governo dos EUA.

Nessa esteira, novos episódios de espionagem governamental apareceram na mídia, como o caso da agência de espionagem britânica, a *Government Communications Headquarters*, (GCHQ) que, em conjunto com a NSA, grampeou as comunicações realizadas por cabos de fibra ótica, que inclui ligações telefônicas e mensagens via *e-mails* em todo o Reino Unido. As provas, de caráter documental, apontavam, também, para a estreita colaboração de empresas privadas no fornecimento de dados pessoais ao governo. Esses fatos demonstram a amplitude, a abrangência e a complexidade da rede de ciberespionagem estatal existente na atualidade.

Na trajetória revelada, as tecnologias cibernéticas, ao ultrapassarem as fronteiras nacionais, acabaram dificultando governos administrarem as ameaças oriundas da ciberespionagem contra seus sistemas e infraestruturas, assim como de agentes não estatais, um novo ator com a mesma capacidade tecnológica que anteriormente era privilégio exclusivamente de agências governamentais.

Um ponto que merece destaque, válido não apenas para a ciberespionagem como também para outros crimes cibernéticos, é citado na lição de Nogueira[11], quando aduz que existe um sentimento de impunidade evidente, quase absoluta, justamente pela falta de uma legislação clara acerca da questão.

11 NOGUEIRA, Sandro D'Amato. **Crimes de informática**. São Paulo: BH Editora, 2009. p. 63.

Ademais, na visão de Luke[12], as normas foram criadas para aplicação em ações e objetos com existência corpórea e uma realidade composta por coisas imateriais gera problemas que a interpretação analógica nem sempre logra resolver.

Consoante as visões anteriores, Serge Fdida[13] complementa que, nesse domínio, a legislação é inexistente ou até mesmo inaplicável, devido ao desaparecimento das fronteiras no espaço digital, onde são questionados conceitos tradicionais como territorialidade e soberania, fatores que impactam no problema da jurisdição.

Pode-se afirmar que, nessa seara, as correntes céticas sobre a possibilidade de uma legislação que permita fiscalização e controle predominam, como o pensamento de Júlio Assange:

> [...] A interceptação estratégica não pode ser restrita pela legislação. Implica em interceptar todo o mundo, independente de serem culpados ou inocentes. Precisamos lembrar, que essa é a essência do establishment que executa este tipo de vigilância. Sempre haverá falta de interesse político em expor a espionagem estatal, aliado ao fato de que a tecnologia é inerentemente tão complexa, e sua utilização, na prática, tão secreta, que não poderá haver uma supervisão democrática expressiva[14].

O sintoma dessa relativização raramente é enfrentado, tanto pelos Estados praticantes como pelos Estados alvos da ação. Os primeiros, por questões diplomáticas e razões de Estado. Os demais, para evitar constrangimentos quanto a questionamentos acerca da sua capacidade de segurança e defesa cibernética na proteção de suas informações estratégicas.

Nessa conjuntura, a evidência argumentativa direciona para o ponto crucial dos esforços a serem dispendidos pelas autoridades governamentais, manifestado na necessidade de desenvolvimento da inteligência cibernética no país.

Wendt, a define como:

12 LUKE, Victor. Seguridad informática y derecho internacional público em el siglo XXI: desafios frente a la protección de infraestructuras informáticas. **Revista de Direito Público**, Madri, v. 77, p. 415, 2013.

13 FDIDA, Serge. **Das auto-estradas da informação ao ciberespaço**. Tradução de Ana Cristina Leonardo. Lisboa (PT): Ed. Piaget, 1997. p. 112.

14 ASSANGE, Júlio. **Cypherpunks**: Liberdade e o futuro da Internet. Tradução de Cristina Yamagam. São Paulo: Boitempo, 2013. p. 63-64.

> […] um processo que leva em conta o ciberespaço, objetivando a obtenção, a análise e a capacidade de produção de conhecimentos baseados nas ameaças virtuais e com caráter prospectivo, suficientes para permitir formulações, decisões a ações de defesa e respostas imediatas visando à segurança virtual de uma empresa, organização e ou Estado[15].

Todavia, para o desenvolvimento dessa tecnologia, fator essencial é o conhecimento da infraestutura da rede, o que não está disponível em níveis avançados.

3 A legislação internacional e as discussões acerca da questão

Na legislação internacional, não há referências à ciberespionagem. Consequentemente, não figura no rol dos crimes de competência do Tribunal Penal Internacional.

Na visão de Flávia Piovesan[16], tal desiderato não poderá ocorrer enquanto não for construído um marco regulador da internet em âmbito internacional pelos países-membros da Organização das Nações Unidas.

Na mesma linha argumentativa, observa-se o pensamento de Kalmykova, que assim assevera:

> […] As tecnologias cibernéticas contemporâneas, que permitem aos serviços secretos invadir sistemas de outros países e computadores de seus cidadãos, são acessíveis para muitos Estados. Na opinião de peritos, para regularizar essas questões litigiosas, é necessário aprovar adicionalmente atas jurídicas internacionais com o objetivo de limitar tal intervenção.Contudo, ainda é duvidoso que os países aceitem tais limitações[17].

Todavia, os debates acerca da regulamentação no uso das tecnologias da comunicação, em especial da internet, ampliaram-se como estratégia de proteção jurídica de dados e informações de caráter pessoal. Paralelamente, discute-se, inclusive, a inclusão de acesso no rol dos direitos humanos, não havendo previsão legal que contemple a ci-

15 WENDT, Emerson. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. **Revista Brasileira de Inteligência**, Brasília, n. 6, p. 23, 2005.

16 PIOVESAN, Flávia. **Direitos humanos e justiça internacional**: um estudo comparativo dos sistemas regionais europeus, interamericano e africano. 5. ed., ampl. e atual. São Paulo: Saraiva, 2014, p. 87.

17 KALMYKOVA, Svetlana. **Ciberespionagem desafia direito internacional**. Disponível em: <http://portuguese.ruvr.ru/news/2014_10_22/Ciberespionagem-desafia-direito-internacional-9648>. Acesso em: 23 ago. 2014.

berespionagem quando praticada por governos contra governos, em que o objeto a ser tutelado são as informações estratégicas governamentais.

Nesse mister, pode-se afirmar que há avanços significativos na tutela de direitos fundamentais com as normas de proteção e tutela dos direitos humanos, que asseguram a inviolabilidade das comunicações e o sigilo à intimidade e à vida privada.

Basta excursionarmos pelos textos da Carta Universal dos Direitos Humanos, do Pacto Internacional dos Direitos Civis e Políticos e da Convenção Americana de Direitos Humanos, incorporados à Organização dos Estados Americanos (OEA).

Por outro lado, tratando-se de determinadas comunidades on-line descentralizadas ou quando a ciberespionagem é originada em outros países, ocorrendo na base da infraestrutura da rede, não existe uma proteção ao alcance da lei e há enormes dificuldades para precisar de que ponto do globo partiram os ataques. Nesses casos, para se atingir uma efetividade plena da legislação, seria necessária uma norma de regulação internacional que estipulasse parâmetros mínimos aceitáveis, em especial, para empresas de serviços de internet e governos.

4 A análise do ordenamento jurídico brasileiro

No plano do Direito Constitucional brasileiro, não há referências à ciberespionagem como conduta criminal. Segundo Woloszyn, tal omissão legislativa é natural, uma vez que a revolução trazida pelas novas tecnologias digitais era desconhecida ao tempo da promulgação da Constituição Federal de 1988.

No mesmo *status*, encontra-se a legislação ordinária. O Código Penal (1940), Código Penal Militar (1969), Lei de Segurança Nacional (1983), e a Lei de Responsabilidade Civil e Criminal por atos Relacionados à Atividade Nuclear (1977) se referem a atos de espionagem de menor complexidade.

Vale lembrar, por esta época, que a materialidade do crime de espionagem era identificável, pois entre as condições para a sua prática estavam o acesso de fontes humanas aos locais de interesse somado à colaboração de agentes estatais. Como crimes conexos, contemplavam-se a falsificação de documentos pessoais e o suborno a agentes estatais, situações que deixavam evidências concretas para as investigações.

Em momento diverso, já sob a influência das tecnologias digitais, foi promulgada a Lei nº 9.296, de 24 de julho de 1996[18],que trata da interceptação das comunicações telefônicas, informáticas ou telemáticas. Contudo, está direcionada à proteção e à tutela do Direito Constitucional que garante a inviolabilidade da intimidade, da privacidade e das comunicações do cidadão singular.

O texto acarretou celeumas jurídicas por conta do parágrafo único do art. 1º, que preconiza a ampliação dessa interceptação do fluxo de comunicações aos sistemas de informática e telemática, o que alguns juristas, como Greco Filho[19], defendem ser flagrantemente inconstitucional, pois, segundo o autor, a expressão "no último caso" refere-se apenas às comunicações telefônicas e não aos outros tipos de comunicação.

No seguimento, e em razão de casos de exposição digital de pessoas destacadas na sociedade brasileira, sobreveio a Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos, alterando o Código Penal pelo acréscimo de dois artigos: 154-A e 154-B. Essa norma jurídica é um significativo avanço na proteção interna de dados e informações dos usuários da rede mundial de computadores, permitindo que condutas criminosas praticadas por meio do sistema informático sejam objeto do Direito Penal.

No art. 1º, refere-se à invasão de dispositivo informático e assim o tipifica:

> 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[20].

A clareza da descrição de tais condutas é de fundamental importância. Abrange a ciberespionagem como crime cibernético, além de englobar todo tipo de ação delituosa,

18 BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03 /leis/L9296.htm>. Acesso em: 4 out. 2017.

19 GRECO FILHO, **Vicente. Interceptação telefônica**. São Paulo: Saraiva, 1996. p. 10.

20 BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737 .htm>. Acesso em: 4 out. 2017

inclusive a de inserir em equipamentos informáticos programas desenvolvidos especificamente para tal finalidade, como *spams, malwares*[21], e outras formas.

Com os casos de ciberespionagem envolvendo a figura da ex-presidente da República Dilma Roussef, e outras autoridades governamentais do Brasil e na esteira das revelações do ex-técnico da NSA, Edward Snowden, ocorridas no ano de 2013, o governo brasileiro tomou uma atitude reativa à intromissão indevida na tentativa de proteger seus dados e informações governamentais.

Além da instauração de uma Comissão Parlamentar de Inquérito (CPI) no Senado Federal em 2013 para investigar casos de espionagem ocorridos na esfera federal, foi promulgado o Decreto nº 8.135, de 4 de novembro de 2013, que dispõe sobre as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional[22].

No magistério de Veloso, essa norma desponta com a pretensão de ser a solução para ameaças reais e de noticiar os incidentes de ciberespionagem das comunicações de autoridades brasileiras e outros governos. Contudo, a norma levanta muitas críticas da comunidade especializada em segurança das informações, as quais, segundo a avaliação do autor, repousam nas seguintes questões:

> […] O Decreto não diz exatamente o que fazer e como deve ser feito. Outro ponto se refere à determinação de que os equipamentos e programas destinados às atividades de comunicações de dados devam ter características que permitam a auditoria para fins de integridade dos dados o que é praticamente impossível de ser realizada além de que o decreto apresenta um equívoco conceitual, uma vez que técnicas de auditoria não garantem os atributos da segurança da informação[23].

21 Os *malware* Flame e Stuxnet foram programas desenvolvidos especificamente para espionar e neutralizar sistemas que contivessem informações confidenciais como o programa nuclear iraniano. Outro poderoso vírus, chamado *Madi*, é direcionado à espionagem de organizações financeiras, de infraestrutura e autoridades governamentais que detenham algum tipo de conhecimento sensível.

22 BRASIL. **Decreto nº 8.135, de 4 de novembro de 2013**. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm>. Acesso em: 6 maio 2014.

23 VELOSO, Marcelo de Alencar. Ciberespionagem Global e o Decreto 8.135: uma avaliação segurança das informações do governo brasileiro. Painel 49/142. Segurança das Informações. In: CONGRESSO CONSAD DE GESTÃO PÚBLICA, 7., mar. 2014. Brasília, DF. **Anais**... Brasília: Consad, 2014, p.14. Disponível em: <http://pt.slideshare.net/mvsecurity/artigo-consad-2014-ciberespionagem-global-e-o-decreto-8135-uma-avaliao-da-segurana-das-informaes-do-governo-brasileiro>. Acesso em: 6 maio 2014.

A esse respeito, é preciso dizer que, a exemplo de outras legislações citadas, sua efetividade é relativa, uma vez que os legisladores, pela análise do parágrafo acima, dão a entender que carecem de conhecimentos mais aprofundados sobre o funcionamento do sistema de ciberespionagem global, os quais são de acesso restrito às agências de inteligência e segurança e, portanto, não disponibilizados, protegidos pelo manto do segredo ou razão de Estado[24].

Esse entendimento é flagrante na Lei Complementar nº 149, sancionada em 12 de janeiro de 2015[25], que altera a Lei Complementar nº 90, de 1º de outubro de 1997, e regula as condições de permanência e trânsito dos integrantes de forças estrangeiras em território nacional. Foi elaborado devido à nova realidade de segurança nacional, a qual também surgiu após as revelações do ex-técnico da NSA, Edward Snowden, sobre espionagem cibernética.

O relevante do texto recai no art. 2º, inciso IV da referida norma, que preceitua o dever da especificação do quantitativo, da natureza do contingente ou grupamento, bem como dos veículos e equipamentos bélicos, de comunicação, de guerra eletrônica, de reconhecimento e vigilância.

Todavia, pelo conteúdo anteriormente exposto neste estudo, pode-se afirmar que tal Lei Complementar possui efetividade relativa, uma vez que a característica principal desses equipamentos, tratando-se de ciberespaço, é a sua utilização em longas distâncias, em que as fronteiras territoriais e a presença de agentes governamentais no país são irrelevantes. Principalmente quando tais ações ocorrem no âmbito da estrutura da rede que não se encontra localizada em território nacional.

Por fim, a Lei nº 12.965, de 23 de abril de 2014[26], conhecida como o Marco Civil da Internet, foi festejada como o maior avanço nessa conjuntura, pela tutela de direitos fundamentais surgidos do uso da internet, além de pretender assegurar aspectos de soberania e da defesa nacional contra atos de ciberespionagem.

24 Bobbio esclarece que razão de Estado é um conjunto de princípios com base nos quais ações que não seriam justificadas se empreendidas por um indivíduo isolado não são apenas justificadas, mas exaltadas se cumpridas por quem exerça o poder em nome de um Estado. BOBBIO, Norberto. **Teoria geral da política**: a filosofia política e as lições de clássicos. Organização de Michelangelo Boneso. Tradução Danila Beccaccia Versiani. Rio de Janeiro: Elsevier, 2000, p.176.

25 BRASIL. **Lei Complementar nº 149, de 12 de janeiro de 2015**. Altera a Lei Complementar no 90, de 1o de outubro de 1997, que determina os casos em que forças estrangeiras possam transitar pelo território nacional ou nele permanecer temporariamente. Disponível em: <http://www.planalto.gov.br/ccivil_03 /leis/lcp/Lcp149.htm>. Acesso em: 15 fev. 2015.

26 BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 18 fev. 2015.

Quanto aos primeiros objetivos, dita norma é um avanço e possibilita a proteção a dados pessoais. Quanto aos últimos, contudo, carece de judicialização internacional, portanto, válida apenas contra o crime praticado dentro do território nacional.

Nesse sentido, o país escolheu o caminho inverso do que tradicionalmente ocorre, quando primeiro reconhece a legislação internacional como aplicável *interna corporis* para, posteriormente, criar normas infraconstitucionais regulando a matéria.

5 O *status* brasileiro frente às tecnologias digitais

Segundo a classificação de Willian Martin[27], o Brasil figura no rol dos países pobres em informação sem o domínio da tecnologia eletrônica e cibernética e o consequente conhecimento técnico especializado, possuindo limitações significativas para combater ameaças e vulnerabilidades internas e externas de maior complexidade. Isso equivale a dizer que existe uma total dependência em relação às tecnologias que são administradas pelas grandes potências mundiais, em especial, os EUA.

A falta de infraestrutura é outro problema, apontado por Coronato e Barifouse[28], os quais afirmam que mais de 80% da capacidade de transmissão por cabos de fibra ótica que conectam o Brasil ao mundo passam pelo território estadunidense, assim como todas as comunicações via internet, uma vez que o país não possui satélites de transmissão do tráfego de dados pela internet e da telefonia móvel, sendo este alugado de uma empresa mexicana para suprir tal necessidade.

Em decorrência, o país valeu-se de acordos de cooperação com outros países para capacitação e treinamento. Na maioria dos casos, solicita doações, em alguns, adquire equipamentos, sistemas e programas desenvolvidos para identificar e neutralizar ações de ciberespionagem.

O Relatório Final da Comissão Parlamentar de Inquérito, denominada CPI da Espionagem, instaurada pelo Senado Federal em 2013, apresenta um diagnóstico estar-

27 MARTIN, Willian J. apud VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sérgio Antônio Fabris Ed, 2007. p.161.

28 CORONATO, Marcos; BARIFOUSE, Rafael. Somos todos vigiados. **Revista Época**, Rio de Janeiro, n. 790. p. 25, jul. 2013. Disponível em: <http://epoca.globo.com/tempo/noticia/2013/07/somos-todos-vigiados-pelo-bgoverno-americanob.html>. Acesso em: 23 jul. 2015.

recedor sobre as fragilidades do Brasil frente à espionagem eletrônica e digital, especialmente, em relação ao estágio em que o país se encontra em termos de segurança cibernética, evidenciando graves problemas no sistema de telecomunicações brasileiro e do sistema de inteligência e defesa cibernética[29].

Quanto à cultura de segurança cibernética na esfera governamental, o documento assim expressa:

> […] Em estudo de 2010, o TCU levantou que mais da metade das instituições públicas fazia *software* de forma amadora; mais de 60% não tinham na prática uma política e estratégia para informática e segurança de informação, e 74% não tinham nem mesmo as bases de um processo de gestão de ciclo de vida de informação. Ainda, 75% não gerenciavam incidentes de segurança de informação, como invasão de sites e sistemas e perdas ou pior alteração de dados, e 83% não faziam ideia dos riscos a que a informação sob sua responsabilidade estava sujeita. O relatório aponta ainda que quase 90% dos órgãos não classificavam a informação, o que significa que a instituição está sob provável e permanente caos informacional. Em maio de 2011, o Tribunal de Contas da União informava que havia "uma total ausência de comprometimento dos altos escalões com a área de Tecnologias da Informação e Comunicação (TIC), do governo federal[30].

Diante desse contexto, o Brasil apela, tradicionalmente, para a legislação como resposta salvadora para o caos informático estabelecido. Contudo, tal iniciativa não apresenta probabilidade de sucesso na redução das ações de ciberespionagem, uma vez que não pode, de forma exclusiva, responder por problemas infraestruturais e culturais sem que existam políticas públicas para o setor. E, em especial, devido a legislação brasileira não possuir poder de judicialização internacional.

Quanto ao aspecto da rede global, aponta:

> […] Já em relação às redes globais, valem as leis de outros países Assim, uma interceptação das comunicações para fins de espionagem, além de extremamente fácil, pode ser absolutamente legal. Estima-se que mais de

29 SENADO FEDERAL. **CPI da Espionagem**: Relatório final. Disponível em: <http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em: 18 jun. 2015.

30 SENADO FEDERAL. **CPI da Espionagem**: Relatório final. Disponível em: <http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em: 18 jun. 2015.

> 70% do tráfego de dados gerado por brasileiros circule fora do Brasil. Isso ocorre porque uma das pontas da comunicação está fora do território nacional [...]. Em outros termos, uma informação originada em um ponto do território nacional com destino a outro, seja um correio eletrônico, o acesso a um *site* de notícias brasileiro ou o *download* de um aplicativo de um provedor nacional pode trafegar por equipamentos localizados no exterior, facilitando seu monitoramento por agentes externos[31].

Vale destacar que essa conjuntura torna-se válida para todos os tipos de crimes cibernéticos, notadamente, a ciberespionagem e o ciberterrorismo, quanto às dificuldades encontradas nas investigações e no alcance das normas.

Quanto a tendências e possibilidades de redução dos atos de ciberespionagem no cenário brasileiro e mundial, a CPI chegou à seguinte conclusão:

> [...] Se existe uma afirmação que pode ser feita sobre a espionagem internacional é que esta continuará e, de fato, mostrar-se-á mais intensa com o desenvolvimento de recursos tecnológicos que permitam a operação no ambiente virtual. Essa espionagem, feita por governos, empresas e organizações não pode ser objeto de qualquer regulamentação internacional, pois é atividade típica do sistema internacional anárquico. Assim, iniciativas de se propor um regime internacional para regular o recurso à espionagem por parte de governos é, na melhor das hipóteses, utópica e ingênua. O direito internacional dificilmente alcançará o ofício dos espiões[32].

Evoluindo na construção dessas concepções, fica evidenciado o poder limitado do país frente ao delito de ciberespionagem, pelo caráter pouco claro das normas existentes, pelas deficiências nas estruturas tecnológicas e pela falta de uma cultura preventiva dos usuários direcionada aos riscos no mundo digital.

Nesse sentido, importante ressaltar a iniciativa pioneira do Ministério Público Federal com seu projeto institucional de oficinas de educação digital nas escolas, que deverá despertar para uma nova consciência preventiva. Outra medida que merece destaque é

31 SENADO FEDERAL. **CPI da Espionagem**: Relatório final. Disponível em: <http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em 18 jun. 2015.

32 SENADO FEDERAL. **CPI da espionagem**: Relatório final. Disponível em: <http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em: 18 jun. 2015.

a criação do Centro de Defesa Cibernética do Exército Brasileiro (CDCiber), exercendo a proteção contra ciberataques às instalações sensíveis, dentre estes, a ciberespionagem.

6 A proteção às informações sensíveis - conhecendo a estrutura da rede

O paradigma da proteção às informações sensíveis segue alguns padrões regulamentares que nem sempre são aplicáveis, variando de país a país, em razão das diferenças nas sociedades, sua infraestrutura crítica, cultura digital e valores. Contudo, essencial se torna conhecer a infraestrutura da rede de informações para adoção de medidas profiláticas em caso de intrusão.

Recorrendo à lição de Dunn e Wigert, estes afirmam que:

> […] não é fácil entender o que é exatamente a infra-estrutura de informações. Isto é devido ao fato de não ter apenas um componente *físico* que é facilmente compreendido – como, por exemplo, redes de alta velocidade, interativas, de banda estreita e de banda larga – satélite, terrestre e de arame, menos sistemas de comunicação; e os computadores, televisores, telefones, rádios e outros produtos que as pessoas empregam para acessar a infra-estrutura, mas também um *immaterial*, às vezes muito evasiva (ciber) componente, nomeadamente a informação e o conteúdo que atravessa a infra-estrutura, o conhecimento que é criado a partir desta, e os serviços que são fornecidos[33]. (tradução nossa)

Num plano básico, existe um cardápio de medidas disponíveis destinadas à proteção da informação e dos sistemas informáticos. Incluem *firewalls*, *softwares*, sistemas de detecção e prevenção de intrusão, senhas de login e criptografia, medidas que a maioria dos países adotam com maior ou menor grau de intensidade. Contudo, o maior problema é a pronta resposta quando da ocorrência de incidentes de violação como a ciberespionagem, que envolve maior complexidade tecnológica.

33 Is not easy to understand what exactly the information infrastructure is. This is due to the fact that it has not only a physical component that is fairly easily grasped – such as high-speed, interactive, narrow-band, and broadband networks; satellite, terrestrial, and wireless communications systems; and the computers, televisions, telephones, radios, and other products that people employ to access the infrastructure – but also an equally important immaterial,sometimes very elusive (cyber) component, namely the information and content that flows through the infrastructure, the knowledge that is created from this, and the services that are provided. DUNN M. e WIGERT I. **The International CIIP Handbook 2004**: An Inventory of Protection Policies in Fourteen Countries. Zurich: Center for Security Studies. 2004, p. 19-20.

Inobstante não haver regulamentação de parte da ONU, a União Europeia encontra-se em estágio avançado nesse contexto, por meio de uma série de regulamentos visando à proteção de dados pessoais e governamentais. Possui uma Agência, a Enisa, criada em 2004, por meio do Regulamento nº 460/2004, do Parlamento Europeu, destinada a promover a segurança das redes de informação e sensibilização para todos os Estados-Membros, editando recomendações, adotando políticas de segurança e fornecendo apoio técnico e *feedback* às instituições públicas e privadas.

Outro instrumento, a Diretiva sobre Segurança de Redes e Sistemas de Informação (Diretiva NIS), em vigor desde 6 de julho de 2016, visa aperfeiçoar os níveis de segurança cibernética. Entre os requisitos da diretiva estão a adoção, por empresas públicas e privadas, de medidas técnicas que gerenciem riscos de violações à segurança cibernética e a adoção de políticas de segurança, devendo essas empresas reportar incidentes de qualquer natureza.

O Regulamento Geral de Proteção de Dados (RDPR) da UE é outra inovação significativa prevista para vigorar a partir de 25 de maio de 2018. O regulamento pretende redefinir as fronteiras geográficas do bloco no intuito de dar maior efetividade e amplitude na aplicação das normas, em especial, o tratamento de dados, independentemente do local em que esteja sendo processado.

Nos EUA, em 2012, houve um esforço político de parlamentares norte-americanos para a aprovação da Lei de Segurança Cibernética. Tal desiderato não logrou êxito no Senado, sob a alegação de que o projeto de lei acarretaria regulamentos que não seriam efetivos e trariam dificuldades as empresas. De outro giro, está em vigor, desde 2002, a Lei Federal de Gestão da Segurança da informação (Fisma) que determina para as empresas públicas e privadas a adoção de medidas de proteção à informação.

No Brasil, existe uma instituição similar, anterior à promulgação do Marco Civil da Internet. Trata-se do Comitê Gestor da Internet no Brasil (CGI.br), criado pela Portaria Interministerial nº 147, de 31 de maio de 1995, entidade privada. Entre suas atribuições está a de promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços na internet. Contudo, sua efetividade é dificultada pela falta de uma cultura digital no país.

Nessa discussão, ganha contornos inigualáveis o debate acerca da eficácia de toda a estrutura de proteção disponível na atualidade.

Mert e Bilge, especialistas internacionais em proteção da informação, em artigo intitulado *Securing Networks in the Information Age*, assim asseveram:

> [...] there is no absolute security, there is always a risk affecting the information system. The purpose should not be to eliminate this risk, which is impossible because of financial and technical difficulties. There is no technology that eliminates the risk in information system. To apply a more expensive countermeasure than the cost of asset just in order to eliminate the risk of the asset is not a rational approach. It is more of a realistic approach to live with the risk rather than try to eliminate it. In order to achieve this, a tool is required which makes comparisons, interpretations and calculations. A sample comparison is between the cost of countermeasure and the cost of the asset itself. If the cost of a countermeasure is more than the cost of damage to the asset, there is no need to apply a countermeasure. Risk management is the tool that makes all these comparisons, calculations and interpretations. The impossibility of absolute security and ubiquitous risk eliminates the view of security as a result. Today, security of information technologies is the real time risk management process. Briefly, security is not a technology concept but a business concept. Risk management is the core of this concept and it is the main decision point for the selection and development of security measures[34].

A teoria acima é compartilhada por Perrow, argumentando que as tecnologias de informação são interativas, complexas e estreitamente acopladas, sendo atingidas por incidentes que não podem ser evitados. Pela complexidade inerente, as falhas vão interagir de maneiras que não podem ser previstas por *designers*, nem compreendidas por operadores. Se o sistema estiver acoplado, as falhas rapidamente estarão fora do controle antes que alguém entenda o que está acontecendo e seja capaz de intervir[35].

Vale destacar que essas teorias fazem parte, na atualidade, do grande debate empreendido por cientistas da comunidade internacional, sobre as quais não há respostas.

34 MERT, Uneri; BILGE, Karabacak. Securing **Networks in the Information Age**. Published in cooperation with NATO public diplomacyp. Lisbon, 2006, p. 62.

35 The technological systems that are interactively complex and tightly coupled will be struck by accidents that cannot be prevented. Because of the inherent complexity, independent failures will interact in ways that can neither be foreseen by designers nor comprehended by operators. If the system is also tightly coupled, the failures will rapidly escalate beyond control before anyone understands what is happening and is able to intervene. PERROW, C.(1984). **Normal Accidents**: Living with High-Risk Technologies. New York: Basic Books, p.14.

7 Conclusão

Finalizando este trabalho, concluímos que a legislação existente no ordenamento jurídico nacional e internacional omite-se quanto à caracterização do crime de ciberespionagem. Especificamente, no contexto brasileiro, parte significativa das normas foram promulgadas entre as décadas de 1960 e 1970, referindo-se à espionagem tradicional, uma vez que não havia perspectiva de uma revolução tecnológica como a iniciada na década de 1990 e que perdura na atualidade.

Um segundo ponto, que merece atenção especial, é o fato de que o Brasil ainda dá seus primeiros passos na tecnologia cibernética, carecendo de investimentos massivos no desenvolvimento de polos tecnológicos e de pesquisas. Em consequência, não possui quadros com conhecimentos técnicos especializados que possibilitem uma investigação efetiva de delitos cibernéticos mais complexos, na dependência da importação de tecnologias desenvolvidas por outros países, assim como de seu assessoramento técnico.

Essa conjuntura permite que em alguns tipos de crimes cibernéticos, como a pornografia infantojuvenil, haja uma colaboração significativa, uma vez que, a *priori*, são crimes que fazem parte de uma rede global e, por esse motivo, são de interesse dos países que fornecem tecnologia e intercâmbio de dados e informações ao Brasil.

Todavia, com relação à ciberespionagem internacional, quando patrocinada por governos contra governos, não há nenhum tipo de colaboração, e o uso de sistemas e programas oriundos destes acarreta em maiores vulnerabilidades para um acesso indevido ou inserção de *malwares*. Muitas ações vêm à tona em razão de denúncias de especialistas, como nos casos do vazamento de informações confidenciais no *site Wikileaks* e as denúncias de Edward Snowden, com repercussão na mídia internacional. As tentativas de investigação esbarram na inexistência de uma legislação internacional, no desconhecimento técnico e na alegação de segredo de Estado, em que crimes dessa natureza encontram proteção legal.

À guisa de fundamentação dessa linha de raciocínio, observa-se que a ciberespionagem, diferentemente de outros crimes cibernéticos, está intimamente ligada a interesses estratégicos de controle e poder, direcionada à busca ou mantimento de uma hegemonia econômica, tecnológica, industrial e militar. Portanto, a vontade política de se construir uma legislação internacional é remota, assim como a possibilidade de colaboração técnica.

Resta a países como o Brasil a adoção de políticas públicas de incremento à pesquisa e desenvolvimento de uma tecnologia cibernética nacional, além da formação de quadros especializados que deem suporte técnico à legislação de combate a crimes cibernéticos, permitindo, assim, a responsabilização penal da ciberespionagem quando praticada dentro dos limites territoriais brasileiros.

A *priori*, esse tipo de delito só poderá ser combatido com a evolução da inteligência cibernética, e esse ponto é crucial para os países considerados em desenvolvimento, na busca de condições técnicas e legais para enfrentar as dinâmicas complexas e variadas trazidas pelas ameaças digitais.

Referências

ASSANGE, Júlio. **Cypherpunks**: Liberdade e o futuro da Internet. Tradução de Cristina Yamagam. São Paulo: Boitempo, 2013.

BOBBIO, Norberto. **Teoria geral da política**: a filosofia política e as lições de clássicos. Organização de Michelangelo Boneso. Tradução Danila Beccaccia Versiani. Rio de Janeiro: Elsevier, 2000.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ ccivil_03/leis/L9296.htm>. Acesso em: 4 out. 2017.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2012/lei/l12737 .htm>. Acesso em: 4 out. 2017.

_____. **Decreto nº 8.135, de 4 de novembro de 2013**. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm>. Acesso em: 6 maio 2014.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 4 out. 2017.

_____. **Lei Complementar nº 149, de 12 de janeiro de 2015**. Altera a Lei Complementar no 90, de 1o de outubro de 1997, que determina os casos em que forças estrangeiras possam transitar pelo território nacional ou nele permanecer temporariamente. Disponível em: <http://www.planalto.gov.br/ccivil _03/leis/lcp/Lcp149.htm>. Acesso em: 15 fev. 2015.

CASTELLS, Manuel. **A sociedade em rede**: a era da informação, economia, sociedade e cultura. v. 1. Tradução de Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999.

CEPIK, Marco. Inteligência e políticas públicas: dinâmicas operacionais e condições de legitimação, **Security and Defense Studies**, v. 2, winter 2002-2003.

CORONATO, Marcos; BARIFOUSE, Rafael. Somos todos vigiados. **Revista Época**, Rio de Janeiro, n. 790, p. 25, jul. 2013. Disponível em: <http://epoca.globo.com/tempo/noticia/2013/07/somos-todos-vigiados-pelo-bgoverno-americanob.html>. Acesso em: 23 jul. 2015.

DUNN M.; WIGERT I. **O PICI International Hanbook 2004**: um inventário de pró-políticas tection em catorze países. Zurique: Centro de Estudos de Segurança, 2004.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

FREITAS, Neisser Oliveira. Aspectos jurídico-históricos das Patentes de Interesse da Defesa Nacional. **Revista Brasileira de Inteligência**, Brasília, n. 6, 2005.

FDIDA, Serge. **Das auto-estradas da informação ao ciberespaço**. Tradução de Ana Cristina Leonardo. Lisboa (PT): Ed. Piaget, 1997.

GRECO FILHO, Vicente. **Interceptação telefônica**. São Paulo: Saraiva, 1996.

KALMYKOVA, Svetlana. **Ciberespionagem desafia direito internacional**. Disponível em: <http://portuguese.ruvr.ru/news/2014_10_22/Ciberespionagem-desafia-direito-internacional-9648>. Acesso em: 23 ago. 2014.

LUKE, Victor. Seguridad informática y derecho internacional público em el siglo XXI: desafios frente a la protección de infraestructuras informáticas. **Revista de Direito Público**, Madri, v. 77, 2013.

MARTIN, Willian J. apud VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sérgio Antônio Fabris Ed, 2007.

MERT, Uneri; BILGE, Karabacak. **Securing Networks in the Information Age**. Published in cooperation with NATO public diplomacyp. Lisbon, 2006.

MINGST, Karen; TOFT, Ivan M. Arreguín. **Princípios das Relações Internacionais**. Tradução de Cristina de Assis Serra. Rio de Janeiro: Elsevier, 2014.

NOGUEIRA, Sandro D`Amato. **Crimes de informática**. São Paulo: BH Editora, 2009.

PERROW, C. **Normal Accidents**: Living with High-Risk Technologies. New York: Basic Books, 1984.

PIOVESAN, Flávia. **Direitos humanos e justiça internacional**: um estudo comparativo dos sistemas regionais europeus, interamericano e africano. 5. ed., ampl. e atual. São Paulo: Saraiva, 2014.

SENADO FEDERAL. **CPI da Espionagem**: Relatório final. Disponível em: <http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em: 18 jun. 2015.

SILVA, Ângelo Roberto Ilha da; SHIMABUKURO, Angela (Org.). Crimes Cibernéticos.: In: FALCÃO JÚNIOR, Alfredo Carlos G.; BUFFON, Jaqueline Ana. **Ciberterrorismo**: entre a prevenção e o combate. Porto Alegre: Livraria do Advogado, 2017.

TOFFLER, Alvin. **A terceira onda**. Tradução de João Távora. 11. ed. Rio de Janeiro: Record, 1980.

WENDT, Emerson. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. **Revista Brasileira de Inteligência**, Brasília, n. 6, 2005.

WOLOSZYN, André Luís. **Vigilância e Espionagem Digita**l: a legislação internacional e o contexto brasileiro. Curitiba: Juruá Ed., 2016.

VELOSO, Marcelo de Alencar. Ciberespionagem Global e o Decreto 8.135: uma avaliação segurança das informações do governo brasileiro. Painel 49/142. Segurança das Informações. In: CONGRESSO CONSAD DE GESTÃO PÚBLICA, 7., mar. 2014. Brasília, DF. **Anais**... Brasília: Consad: 2014, p. 14. Disponível em: <http://pt.slideshare.net/mvsecurity/artigo-consad-2014-ciberespionagem-global-e-o-decreto-8135-uma-avaliao-da-segurana-das-informaes-do-governo-brasileiro>. Acesso em: 6 maio 2014.

VOLKMAN, Ernest. **A história da espionagem**. Tradução Ciro Mioranza e Antônio Carlos Braga. São Paulo: Ed. Escala, 2013.

8 DIREITO INTERNACIONAL E O COMBATE À CIBERCRIMINALIDADE CONTRA CRIANÇAS

Paulo Ernani Bergamo dos Santos[1]

Resumo: Com o incremento da utilização da rede mundial de computadores e de outros dispositivos eletrônicos que a ela facilmente se conectam, também a criminalidade informática, ou cibercriminalidade, nela encontra lucrativo campo de atuação. A rapidez da comunicação via web, a dificuldade de identificação do criminoso e do local originário da conduta e a problemática da definição da jurisdição aplicável são fatores que viabilizam a realização da conduta criminosa com anonimato praticamente intocável. As crianças representam um público em crescimento na rede, onde fazem contatos com pessoas desconhecidas, tornando-se presa fácil de pedófilos e de organizações criminosas que se utilizam da web para cometerem abusos ou exploração sexual de menor. Como o Direito é reflexo da sociedade de determinada época e protege os bens jurídicos que o corpo social reputa como relevantes, o Direito na atualidade tenta dar uma resposta mais veloz à crescente cibercriminalidade contra crianças, por meio não só do Direito Penal, mas também por outras medidas de natureza preventiva. Neste artigo será analisada a conexão existente entre Direito Internacional, ordem jurídica interna dos Estados – mais especificamente, da Espanha e do Brasil – e Direito Penal no combate à cibercriminalidade contra crianças, e a necessidade de uma estratégia de combate de natureza preventiva e ressocializadora, que envolva também cooperação internacional, colaboração entre provedores, usuários da internet, famílias, governos e associações civis. Ao final, conclui-se que apesar dos esforços da comunidade internacional e desses países, ainda há muito a fazer no combate efetivo à ciberciminalidade contra a criança.

Palavras-chave: Direito internacional. Estado. Direito Penal. Cibercriminalidade. Crianças.

Abstract: *The cybercrime has found a profitable field of action in the Web. The high speed of communication, the difficulty in identifying the criminal and the place of the conduct, and also the barriers to define the applicable jurisdiction are factors that enable the criminal conduct in Internet with virtually untouchable anonymity. As children represent a growing public in the network, they become easy preys to pedophiles and criminal organizations that perpetrate abuses or sexual exploitation of children. The Law system has incorporated some issues related to cybercrime against children, not only by Criminal Law but also by other preventive measures. This article will analyze the connection between international and crimnal law, the legal order of Spain and Brazil, and*

1 Paulo Ernani Bergamo dos Santos é mestre em Direito Penal Internacional pela Universidade de Granada, Espanha, mestre em Administração Pública pela Universidade de Columbia, Nova Iorque, especialista em Direito Público pela Escola Paulista da Magistratura, especialista em Direito Tributário pela FGV-SP e auditor fiscal tributário.

the need for a preventive and ressocializing strategy to fight cybercrime against children which also involves international cooperation, collaboration between providers, Internet users, families, governments and civil associations. The conclusion is that despite all the efforts of the international community and the States much more remains to be done, in order to fight cybercrime against children.

Keywords: International Law. State. Criminal Law. Cybercrime. Children.

1 Introdução

Com a verdadeira revolução tecnológica a que assistimos nas últimas décadas, em que todos interagem por meio da internet como parte ativa e passiva ao mesmo tempo, a noção de tempo e espaço se movimenta no sentido do "aqui e agora" em tempo real, ultrapassando limites territoriais.

O número total de usuários da internet estimado em 2016, segundo estudo do Banco Mundial e da *International Telecommunication Union*, foi de 3.5 bilhões – 1/4 desse total corresponde a jovens entre 15 e 24 anos, e o número de subscrições de telefones celulares atingiu 7.3 bilhões, quase 98% da população mundial. Na Espanha, quase 78% da população tiveram acesso à internet e no Brasil, quase 59%.

Estando cada vez mais presente na vida das pessoas, tanto os aspectos positivos como os negativos da internet se difundem, e nela a criminalidade encontra um veículo poderoso para a disseminação de condutas reprovadas pela sociedade.

Os ambientes "virtuais" – como *sites* de busca, de redes sociais, dos provedores de acesso e de conteúdo, as propagandas que permeiam os milhares de *sites* na *web* –, são propícios para condutas perniciosas de pedófilos e criminosos de todos os matizes, podendo desembocar em crimes como calúnia, difamação, injúria, ameaça, pornografia infantil, induzimento ao suicídio, falsa identidade, fraudes, que acabam atingindo crianças e adolescentes, ainda em fase de formação física, psíquica e emocional.

Um estudo do Escritório das Nações Unidas sobre Drogas e Crime (UNODC) (Estudo sobre o Cibercrime, 2013) concluiu, com base nos dados fornecidos por 69 Estados-Membros, 40 organizações do setor privado, 16 organizações acadêmicas, 11 agências intergovernamentais e consulta a mais de 500 documentos de acesso livre na web, que muitas das formas de abuso contra crianças facilitadas pela internet possuem a mesma

dinâmica, padrões e estruturas daqueles perpetrados sem o uso da internet (UNODC, 2015).

Em 2016, a cada 9 minutos uma página da web mostrava imagens com abuso ou exploração de menor.

Nesse mesmo ano, a *Internet Watch Foundation* (IWF, 2017) removeu 57.335 páginas da web contendo imagens ou vídeos de abuso sexual contra crianças e processou 105.420 denúncias de abuso contra crianças via web, 56% com conteúdo criminal (IWF, 2017).

Um total de 57.335 *Uniform Resource Locators* (URLs) espalhados por 50 países continham imagens e vídeos de abuso sexual contra crianças, um aumento de 21% em relação a 2015; e essas URLs estavam vinculadas a 2.416 domínios, especialmente aos cinco principais domínios (.com .net .se .io .cc), nos quais foram rastreadas 80% dessas imagens e vídeos (IWF, 2017).

O Direito também se transforma e passa à regulação de relações jurídicas novas ou antigas, relações agora em novo formato, e, por consequência, também o Direito Penal precisa ser adaptado às novas realidades, para proteger não somente bens jurídicos individuais, mas também supraindividuais (interesse público, interesse coletivo), dentre os quais a infância.

Tem-se, então, no Direito Penal a *ultima ratio* para inibição ou punição da realização de um determinado fato ou ato humano não tolerado pela sociedade em certa época, "a fim de garantir a integridade da ordem jurídica" (AMBOS, 2006, p. 23); o ordenamento jurídico também prevê, a depender do bem protegido, sanção de ordem civil e/ou administrativa, sem necessidade de regulação de ordem eminentemente penal.

A discussão atual aparece centrada muito mais na determinação de qual é a "proteção (civil, penal, administrativa) que se deve prestar a determinados bens sobre cuja natureza de objetos passíveis de proteção jurídica não existem dúvidas" (SILVA SÁNCHES, 2011, p. 419).

No Brasil, a relação entre provedores e usuários dos serviços de internet, por exemplo, foi disciplinada pela Lei nº 12.965, de 23 de abril de 2014 – o "Marco Civil da Internet", uma norma de natureza eminentemente administrativa.

É também o Direito Penal um instrumento subsidiário a outros de natureza extrapenal – como a colaboração entre provedores, usuários da internet, famílias, governos e associações civis, com a finalidade de regulação do uso adequado da internet (SILVA SÁNCHES, 2011, p. 419).

Principalmente quando se constata que a dinâmica fluida das condutas delituosas cometidas na web e a dificuldade de definição da jurisdição aplicável tornam mais difícil o combate à cibercriminalidade.

A harmonização entre o Direito Internacional, seus instrumentos jurídicos como Declarações, Convenções, Acordos multilaterais ou bilaterais, e as legislações internas dos diferentes Estados nacionais passa a ser elemento essencial para a efetividade desse combate.

No capítulo 1, será abordada a conexão entre Direito Penal e cibercrime, discorrendo-se no capítulo 2 sobre a cibercriminalidade, a Convenção de Budapeste, algumas classificações doutrinárias de cibercrime e como esse tipo de crime afeta as crianças. Serão fornecidos dados que demonstram o vertiginoso aumento da navegação de usuários jovens na web no Brasil.

No capítulo 3, será analisada a conexão entre o Direito Internacional, o ordenamento jurídico interno, em específico do Brasil e da Espanha, e as normativas emanadas da União Europeia que, no conjunto, fornecem uma estratégia de natureza preventiva, punitiva e ressocializadora ao cibercrime contra crianças.

Em seguida, registram-se as conclusões do estudo.

2 Direito Penal e Cibercriminalidade

O Direito como fenômeno humano cultural (PRADO, 2010) não está imune às transformações sociais, sendo delas um reflexo e nelas exercendo também sua influência.

Existem condutas que são rejeitadas pelo corpo social em determinada época, mas que, em momento posterior, podem deixar de ser socialmente reprovadas (AMBOS, 2006, p. 20).

Por exemplo, a conduta "ter conjunção carnal com mulher honesta, mediante fraude" que integrou o Código Penal Brasileiro (CPB) de 1940 até 2005 (art. 215), suprimida com a Lei nº 11.106/2005.

O art. 215 do CPB, inserido no Título IV (Dos Crimes Contra os Costumes), antes da edição dessa lei, punia a conduta "ter conjunção carnal com mulher honesta, mediante fraude", de maneira a deixar de fora da tipificação penal a conjunção carnal mediante fraude de mulher que não fosse "honesta"; a mulher que não seguisse os padrões de conduta socialmente aceitos não teria, portanto, direito à proteção da lei penal em caso de conjunção carnal, mediante fraude.

Ocorre que, num mundo em que os direitos das mulheres foram sendo paulatinamente garantidos em declarações e em outros documentos internacionais, não havia mais na sociedade justificativa para manter esse resquício de subordinação preconceituosa das mulheres na legislação penal.

O cenário internacional de tratamento desigual entre homens e mulheres, com prejuízo para estas, modificou-se a partir da Declaração Universal dos Direitos do Homem (1948), com a construção paulatina do sistema internacional de proteção dos direitos humanos, integrado por "instrumentos de caráter geral (como os Pactos Internacionais dos Direitos Civis e Políticos e de Direitos Econômicos, Sociais e Culturais de 1966) e por instrumentos de caráter específico" (PIOVESAN, 2006, p. 207), como a Convenção Sobre a Eliminação de Todas as Formas de Discriminação Contra as Mulheres (1979), ratificada pelo Brasil em 1984, em que se declarava a igualdade entre homens e mulheres, e a Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher, ratificada pelo Brasil em 1995.

Mesmo que bem depois da ratificação das Convenções mencionadas e da promulgação da Constituição Brasileira de 1988 (CFB), a alteração na redação do art. 215 do CPB, suprimindo a expressão "honesta", fez com que a lei penal passasse a considerar vítima dessa conduta qualquer mulher ("ter conjunção carnal com mulher, mediante fraude"), e não exclusivamente a que, segundo o que se entendia como tal em época anterior, fosse "honesta" (GRECO, 2011, p. 503).

Num outro giro, relações antes inexistentes, passam a ser objeto de regulação normativa, considerando novos contextos sociais.

No Brasil colônia, em final do século XVIII e início do século XIX, por exemplo, aplicavam-se as normas penais das Ordenações Filipinas, em que o crime era confundido com o pecado e com a ofensa moral, fixando a maioridade a partir dos sete anos, a "idade da razão", segundo o direito canônico; dos sete aos dezessete anos, o tratamento penal era similar ao que se destinava aos adultos, com atenuação das penas. E dos dezessete aos vinte e um anos, os jovens adultos eram passíveis da pena de morte por enforcamento.

Em 1979, quase dois séculos depois, o Código de Menores é aprovado, consolidando a doutrina da Situação Irregular, estabelecendo medidas tutelares para os menores de 18 anos e medidas de segurança para maiores, com a transferência para a penitenciária e necessidade de laudo de inexistência de periculosidade para sua soltura.

A internet não fazia parte das relações humanas nessa época e, portanto, não existia para o Direito.

Na atualidade, porém, a presença transnacional e ubíqua da tecnologia da informação nas relações humanas, inclusive na criminalidade, demanda que o Direito – no caso específico, o Direito Penal – passe a tipificar penalmente condutas rechaçadas pela sociedade.

Por exemplo, o art. 244-B do Estatuto de Criança e do Adolescente que, para proteger a formação moral da criança e do adolescente, tipifica a conduta de corromper ou facilitar a corrupção do menor para: (a) com ele praticar infração penal ou (b) induzi-lo a praticá-la – e nas mesmas penas incorrendo quem praticá-las utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet. "Como meio de corromper ou facilitar a corrupção pode ser utilizada a Internet através, por exemplo, das salas de bate-papo" (ISHIDA, 2010, p. 529).

O conjunto de normas jurídico-penais inclui normas primárias e secundárias, e a relação entre elas.

As normas primárias são aquelas "dirigidas aos cidadãos para proibir-lhes o cometimento de delitos" (SILVA SÁNCHES, 2011, p. 548) (normas de conduta, de comportamento) e as secundárias, "dirigidas aos juízes para ordenar-lhes a imposição de sanções no caso de que se cometam delitos" (SILVA SÁNCHES, 2011, p. 548) (normas de sanção).

As primeiras estão posicionadas numa perspectiva prévia ao cometimento do delito, definindo o "âmbito de liberdade pessoal de ação e o âmbito das condutas cuja reali-

zação está vedada" (SILVA SÁNCHES, 2011, p. 548) e as segundas, numa perspectiva posterior ao cometimento, definindo o punível; a relação entre elas se dá no sentido de as normas secundárias (menos amplas) servirem de reforço às normas primárias (mais amplas), numa relação lógica que caminha das normas primárias para as secundárias – e não o contrário (PUIG, 1982, p. 46).

Um caso conhecido no Brasil foi o do furto de imagens de uma atriz muito conhecida do público brasileiro (Carolina Dieckmann), com a finalidade de se auferir vantagem ilícita, e que acabou culminando na tipificação penal de invasão de dispositivo informático, como resultado da pressão social resultante daquela conduta (art. 154-A do Código Penal Brasileiro).

Trata-se de "crime cibernético próprio. É um crime de intrusão ou, segundo o nome legal, invasão de dispositivo informático (*hacking*)" (DODGE, 2013, p. 337), ao qual a norma primária funciona como um aviso de que a conduta descrita não é aceita pela sociedade e que, se for realizada, sujeitará o autor à punição pelo Estado.

Essa punição é descrita na norma secundária a ser aplicada pelo juiz: detenção, de 3 (três) meses a 1 (um) ano, e multa.

Numa sociedade marcada pela transnacionalidade do crime e pela sensação do risco em razão do desenvolvimento da tecnologia, opera-se um movimento de descodificação e de ampliação do número de normas penais em legislações especiais, aliada à criação de tipos penais de perigo abstrato (ANITUA, 2008, p. 831), visando proteger os bens jurídico-penais contra violações.

O "bem jurídico-penal" é o bem jurídico tutelado pelo Direito Penal, com substrato na realidade social e na Constituição, e podem ser assim classificados:

a. bens jurídico-penais de natureza individual (referentes a bens jurídicos divisíveis e disponíveis em relação ao seu titular e cuja disponibilidade não afeta os demais indivíduos, como a vida, a integridade física, a honra);
b. bens jurídico-penais de natureza coletiva (referentes àqueles bens jurídicos indivisíveis e que o indivíduo não pode disponibilizar sem que afete os demais titulares desses bens, como a incolumidade pública, a paz pública);
c. os bens jurídico-penais de natureza difusa (referentes àqueles bens jurídicos indivisíveis, de toda a sociedade e que o indivíduo não pode disponibilizar sem que afete a coletividade – e que carregam uma conflitualidade social – como a prote-

ção ao meio ambiente, a proteção da relação de consumo, a proteção da saúde pública, da infância e juventude).

Os bens jurídicos lesionados por meio da internet podem ser tanto o sistema informático em si mesmo, os dados pessoais arquivados ou disponibilizados por meio do sistema informático, como ainda outros bens jurídicos lesionados em razão do conteúdo veiculado por meio do sistema informático (publicidade enganosa e abusiva, pornografia infantil), e que devem ser tipificados penalmente.

A segurança da informação passa a bem jurídico-penal de natureza difusa, segundo o trinômio "perda de confidencialidade (quebra de sigilo de senha) – perda de integridade (manipula-se uma informação de acesso restrito) – perda de disponibilidade (erro no sistema causado por intrusão de terceiros e causando impossibilidade de acesso à informação por quem precisa dela)" (ROSSINI, 2004, p. 31-53), gerando conflito entre os interesses dos usuários da internet atingidos pela conduta e os interesses de grandes empresas prestadoras de serviço na internet, como provedores de conteúdo e provedores de acesso.

Uma conduta realizada com utilização de equipamento eletrônico e que venha a caluniar alguém, terá como bem jurídico lesionado a honra objetiva; na ameaça por e-mail, o bem afetado será a liberdade individual e assim por diante, ou seja, "proteger-se-á o bem jurídico tutelado pela norma e que efetivamente corresponde à lesão provocada pela conduta praticada" (SILVA, 2003, p. 66).

No caso da Espanha, por exemplo, foi incorporado recentemente em seu Código Penal o art. 183 ter, "2", que protege o bem jurídico correspondente à identidade sexual, o bem-estar psíquico e o processo de formação sexual do menor de dezesseis anos, quando penaliza aquele que utilizar meios tecnológicos para contatar e enganar um menor de 16 anos, com a finalidade de conseguir dele acesso a material pornográfico ou imagens pornográficas em que represente ou em que apareça um menor (MARTÍNEZ SÁNCHEZ, 2017).

Há no art. 184 quater do Código Penal Espanhol uma cláusula pessoal de exclusão, em que a responsabilidade penal pelo delito mencionado é excluída, se houver consentimento livre do menor e o autor seja uma pessoa de idade próxima à dele, com grau equivalente de desenvolvimento e maturidade.

Na Comissão Parlamentar de Inquérito (CPI) destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade no Brasil (CPI – crimes cibernéticos), conduzida pela Câmara Federal, conclui o Relator, no Re-

latório Final da CPI (30 de março de 2016), pela "necessidade de melhorar alguns tipos penais, certos dispositivos legais, procedimentos de investigação, o aparelhamento de nossas autoridades de investigação e, também, a educação dos internautas".

A efetividade das normas penais depende, portanto, de outros fatores, além de estarem formalmente vigentes.

Há necessidade de estratégias que envolvam políticas públicas bem elaboradas para prevenir a ocorrência do delito, para punir o autor do delito, tratar o delinquente, dar apoio e proteção às vítimas, e criar mecanismos de cooperação internacional (jurídica, policial etc.) entre Estados e organizações internacionais públicas e privadas.

O combate à cibercriminalidade precisa seguir uma "macropolítica" que interconecte esse conjunto de aspectos, sem o que esse combate estará fadado ao insucesso.

A internet propicia velocidade, ambiente desprotegido e relativo anonimato para o cometimento da conduta criminosa, o que vem incentivando organizações criminosas a utilizarem a *web* como meio de auferirem maior lucratividade em suas atividades criminosas[2].

Um ataque hacker à empresa de crédito *Equifax*, dos EUA, ocorrido em julho de 2017, por exemplo, expôs os perfis de mais de 143 milhões de pessoas[3]; outro caso notório foi a invasão de mais de 200 mil computadores de 150 países pelo vírus *WannaCry*, em maio de 2017. A expectativa para o futuro próximo é a utilização da inteligência artificial para ataques cibernéticos maliciosos[4].

3 Cibercriminalidade

O desenvolvimento da tecnologia de informação e a rápida inclusão de milhões de usuários da internet em todo o mundo, interligando indivíduos das mais diversas nações e de diferentes culturas em nível mundial, transformam a relação do homem com o Estado-Nação e a relação entre pessoas e entre estas e empresas; as transações comer-

2 Disponível em: <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>. Acesso em: 11 set. 2017.

3 Disponível em: <https://g1.globo.com/tecnologia/noticia/equifax-empresa-de-credito-dos-eua-sofre-ataque-hacker-e-dados-de-143-milhoes-de-pessoas-sao-expostos.ghtml>. Acesso em: 11 set. 2011.

4 Disponível em: <http://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/09/inteligencia-artificial-pode-ser-usada-em-ciberataques-diz-pesquisador.html>. Acesso em: 11 set. 2017.

ciais e as relações sociais passam a ocorrer de forma muito mais acelerada, em tempo real, encurtando distâncias e rompendo barreiras de tempo e espaço.

A soberania dos Estados exercida em território específico, o seu poder independente e supremo aplicado nos limites desse território, passa a plano secundário, em meio à "diversidade, heterogeneidade e complexidade do processo de transnacionalização dos mercados de insumo, produção, capitais, finanças e consumo" (FARIA, 2004, p. 23).

Sua autoridade, antes soberana, se enfraquece, apesar de, em termos formais, continuar a exercer essa soberania; constata-se a "fragilização de sua autoridade, o exaurimento do equilíbrio de poderes e a perda de autonomia de seu aparato burocrático" (FARIA, 2004, p. 25).

Contraditoriamente, o Estado é chamado para atuar de maneira a dar proteção às liberdades individuais em tempos de publicização da vida privada.

Nesse contexto, tem havido um alargamento dos conflitos entre as diferentes legislações nacionais no âmbito da proteção das liberdades e das operações comerciais, fiscais e financeiras, que passam a conviver com a criminalidade transnacional que, a seu turno, encontra na internet um meio propício de alavancar suas operações, diante da dificuldade de aplicação da lei penal no espaço e de maior cooperação policial entre as nações.

Os delitos no ciberespaço podem ser classificados como: "delitos informáticos", em que se incluiriam os delitos perpetrados "*en torno a sistemas informáticos*", em "*redes cerradas ou de acceso restringido*"; e os "cibercrimes", que corresponderiam a uma segunda onda de crimes perpetrados no meio informático e "*girarían em torno a redes telemáticas (abiertas, cerradas o de acceso restringido), siendo en estos casos los sistemas informáticos más instrumentales o secundários para la comisión del delito*" (CASABONA, 2006).

Os cibercrimes podem ser denominados "puros" (condutas ilícitas que recaem sobre recursos tecnológicos, informacionais e comunicacionais) ou "impuros" (condutas ilícitas que têm na tecnologia de informação o meio para a realização do crime).

O acesso não autorizado, a obtenção e transferência ilegal de dados, o dano informático, a disseminação de vírus, a divulgação ou utilização indevida de informações, a

interferência no funcionamento de sistemas, a engenharia social e a interceptação ilegal de dados são exemplos de cibercrimes puros.

Os crimes contra a honra, de ameaça, de falsidade ideológica, de estelionato, violação de direitos autorais, crime de racismo e de produção e distribuição de pornografia infantil são exemplos de cibercrimes impuros: normalmente, são figuras típicas já reguladas nos ordenamentos jurídicos nacionais e nas quais a tecnologia é o meio utilizado para seu cometimento.

Outra classificação agrupa os crimes "virtuais" em três grupos: o crime virtual puro, o crime virtual misto e o crime virtual comum.

a. O crime virtual puro corresponderia à conduta ilícita voltada para o sistema do computador, para a violação do equipamento e de seus componentes, inclusive dados e sistemas (software, hardware e meios de armazenamentos);
b. Os crimes virtuais mistos aqueles em que o uso de meios computacionais é condição necessária para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático (transferência ilícita de valores ou "*salemislacing*" – retiradas diárias de pequenas quantias de milhares de contas bancárias);
c. Os crimes virtuais comuns corresponderiam àqueles em que a internet é utilizada como instrumento de realização do delito que já tipificado na lei penal (como os crimes contra a honra e a veiculação de pornografia infantil) (FIORILLO, 2012, p. 140-145).

Na "Comunicação da Comissão ao Parlamento Europeu ao Conselho e ao Comitê das Regiões", COM(2007) 267 final, o cibercrime é definido como o ato criminoso praticado com recurso das redes de comunicações eletrônicas e sistemas de informação, ou contra esse tipo de redes e sistemas, e engloba três formas de atividade.

A primeira abrange as formas tradicionais da criminalidade, tais como a fraude ou a falsificação, a segunda se refere à publicação de conteúdos ilícitos em meios de comunicação eletrônicos (pornografia infantil ou incitamento ao racismo) e a terceira, os crimes perpetrados exclusivamente nas redes eletrônicas (ataques contra sistemas de informação, bloqueio de serviços e pirataria).

A falta de instrumentos efetivos de cooperação entre os países corre a favor da cibercriminalidade, considerando que, dadas as características da rede, nenhum país pode atualmente combater o cibercrime sozinho; a conduta criminosa pode se originar de

qualquer lugar e atingir qualquer lugar do mundo. Também grande é a dificuldade em identificar os seus autores (HOLLIS, 2011).

Como mais de 50% dos crimes cometidos na internet têm algum aspecto transnacional, as investigações desses crimes envolvem diferentes jurisdições, o que demanda – quer por meio de tratados multilaterais ou bilaterais, quer pelas leis internas dos países – uma cooperação mútua dinâmica, que não seja emperrada pela falta de instrumentos jurídicos que viabilizem essa cooperação.

Quase 40% dos países que participaram do Estudo do Cibercrime responderam que existem leis em seus ordenamentos jurídicos internos ou políticas públicas voltadas para a prevenção do cibercrime.

Por volta de 70% dos países participantes desse estudo relataram ter estratégias nacionais para chamar a atenção para o problema, para cooperação internacional e para a devida aplicação da lei, enquanto mais de 50% dos países respondentes relataram ter estabelecido parcerias público-privadas relativas ao combate ao cibercrime.

Como resultado da necessidade da adoção de uma política criminal comum para a proteção da sociedade contra a criminalidade nas redes informáticas, e complementando a "Convenção Europeia de Extradição" (1957), a "Convenção Europeia de Auxílio Mútuo em Matéria Penal" (1959) e o "Protocolo Adicional à Convenção Europeia de Auxílio Mútuo em Matéria Penal" (1978), foi assinada a "Convenção do Conselho da Europa sobre Cibercrime" (2001) (conhecida como "Convenção de Budapeste").

Nela, os Estados signatários, entre outras ações, comprometem-se a adaptar suas legislações aos termos do acordado nesse instrumento jurídico internacional, especialmente no âmbito penal, e, ainda, a melhorar a cooperação para o combate a essa criminalidade.

A definição de sistema de informação na Convenção não se limita a computadores, o que traz adaptabilidade às mudanças que vão ocorrendo no mundo da internet.

Posteriormente, em 2003 (com entrada em vigor em 2006), foi firmado o Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Atos de Natureza Racista e Xenófoba Praticados por meio de Sistemas Informáticos.

No "Estudo do Cibercrime" de 2013, o cibercrime é classificado pelo tipo de ato praticado.

a. Atos contra a confidencialidade, integridade e disponibilidade dos dados ou sistemas do computador (acesso ilegal ao sistema do computador; acesso ilegal, interceptação ou aquisição de dados do computador; interferência ilegal com um computador ou dados de computador; produção, distribuição ou posse de ferramentas de uso indevido de computadores; violação da privacidade ou de medidas de proteção de dados).
b. Atos relacionados ao computador para ganho pessoal ou financeiro, ou somente para prejudicar (fraude ou falsificação relacionada ao computador; ofensa à identidade relacionada ao computador; ofensa a direito autoral ou a marca relacionada ao computador; envio ou controle de envio de Spam; ato relacionado a computador que cause dano pessoal; ato relacionado ao computador visando ganhar a confiança de crianças);
c. Atos relacionados ao conteúdo do computador (atos relacionados ao computador envolvendo crimes de ódio; produção, distribuição ou posse de pornografia infantil, relacionados ao computador; atos relacionados ao computador em apoio ao terrorismo).

Na Convenção de Budapeste, os Estados Partes concordam quanto à necessidade de cooperação entre os Estados no combate à cibercriminalidade e de tipificação penal de certas condutas e, já em seu preâmbulo, proclama o respeito aos direitos fundamentais do ser humano, à Convenção das Nações Unidas sobre os Direitos da Criança (1989) e à Convenção da Organização Internacional do Trabalho Sobre as Piores Formas de Trabalho Infantil, descrevendo, entre as modalidades da criminalidade informática, a pornografia infantil.

No Título III, art. 9, I, essa Convenção exorta os países signatários a adotarem as medidas legislativas adequadas à tipificação como infrações penais as seguintes condutas relativas à pornografia infantil: produzir pornografia infantil com o objetivo de sua difusão por meio de um sistema informático; oferecer ou disponibilizar pornografia infantil por meio de um sistema informático; difundir ou transmitir pornografia infantil por meio de um sistema informático; obter pornografia infantil por meio de um sistema informático para si próprio ou para terceiros; possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados; tráfico de menores (art. 177 *bis*).

A pornografia infantil nessa Convenção inclui qualquer material pornográfico que represente visualmente: um menor envolvido num comportamento sexual explícito; uma pessoa que aparente ser menor envolvida num comportamento sexual explícito; imagens realísticas que representem um menor envolvido num comportamento sexual explícito.

Os abusos contra crianças facilitados pela tecnologia de informação podem ser perpetrados por meio de: material de apelo sexual abusivo para crianças (pornografia infantil); exploração sexual e comercial de crianças; *cyberenticement* (ciberseducção), *solicitation* (convite malicioso dirigido à criança) e *grooming* (ganhar a confiança do menor); *cyberbullying*, *cyberharassment* (assédio pela internet) e *cyberstalking* (perseguição na internet); e exposição a conteúdo prejudicial (UNODC, 2015).

Entre as novas formas de abuso e exploração de crianças, podem ser citadas:

* A produção *on demand* de material com conteúdo abusivo contra crianças, i.e., o "cliente" faz um pedido de material específico envolvendo abuso sexual de crianças; o perpetrador alicia a criança via chat e produz o vídeo com *webcam*, da forma como contratado e recebendo por tempo de visualização do material na web ou pelo vídeo em si;
* A produção de conteúdo sexual criado e publicado por crianças em *blogs*, vídeos, *podcasts*, em fóruns, social media postings, e contribuições a wiki sites. Um subtipo dessa conduta é o *sexting* – troca de mensagens ou imagens de natureza sexual, sugerindo nudez ou contendo nudez explícita, divulgada por meio da internet – via smartphone ou computador, e que podem ser replicadas pela rede sem autorização, num nível que atinge quase 88% dos casos;
* Transmissão ao vivo de abuso sexual on-line de criança por um adulto, comumente adquirida via cartão de crédito. Pode ainda ser comercializada posteriormente.
* O perfil do ofensor de cyberenticement e de grooming, por exemplo, pode ser classificado em três categorias:
* "*Intimacy seeker*": considera que suas relações com as crianças são consensuais e tendem a abster-se de colecionar grande quantidade de material com conteúdo de abuso sexual infantil, concentrando-se em pressionar a criança para encontros pessoais;
* "*Adaptable offenders*": considera que as crianças têm maturidade sexual precoce e que são capazes, portanto, de consentirem numa relação sexual;
* "*Hypersexual offenders*": constitui o perfil mais agressivo, que coleciona uma vasta gama de material contendo pornografia infantil (WEBSTER, 2013-2014).

A maior parte das vítimas é do sexo feminino (proporção de 4/1), numa proporção ainda maior no *sexting*. No *cyberenticement*, 99% dos abusadores são jovens ou jovens adultos, que se dirigem às meninas (70-75%) entre 14 e 17 anos. Quase 81% das imagens de pornografia infantil na internet é de crianças de 10 anos ou menos (UNODC, 2015).

No Brasil, segundo pesquisa do Comitê Gestor da Internet, *TIC Kids Online*, entre maio de 2015 e junho de 2016, 41% das crianças e adolescentes entre 9 a 17 anos no país utilizaram computador de mesa para acessar a internet, enquanto 85% utilizaram o aparelho de telefone celular para acessar a internet, o que demonstra ser este último o meio mais utilizado por elas.

Dessas crianças e adolescentes, 87% tinham perfil em redes sociais, sendo 79% no Facebook e 71% no WhatsApp; 80% compartilharam foto com seus rostos e 75% deixaram registrado seu verdadeiro sobrenome. Aproximadamente 20% delas foram tratadas de forma ofensiva na internet e 16% viram imagens ou vídeos de conteúdo sexual na internet no período. Mais preocupante: 40% delas tiveram contato com alguém na internet que não conheciam pessoalmente e 17% já se encontraram pessoalmente com alguém que conheceram na internet.

A efetiva cooperação internacional no combate à cibercriminalidade contra crianças encontra barreiras, porém, nas divergências de escopo existentes em acordos multilaterais ou bilaterais, bem como na falta de obrigatoriedade de resposta num prazo determinado e nas variações das salvaguardas existentes nesses acordos, afetando, assim, a efetividade desse combate[5].

Têm sido formadas, com relativo sucesso, forças-tarefa para combater esse tipo de criminalidade na web, como a Virtual Global Task Force (VGT), *the Financial Coalition against Child Pornography* (FCACP), e *the International Association of Internet Hotlines* (Inhope), além de grupos de trabalho financiados por entidades privadas, por um Estado individualmente ou por coalizações internacionais, que se tornaram importantes instrumentos na troca de informações técnicas[6].

No 13º Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, realizado em 2015 na cidade de Doha, a Declaração da União Europeia na abertura do evento propôs que a Convenção do Cibercrime do Conselho Europeu (2001) seja utilizada como modelo para a cooperação internacional, visando a uma internet aberta e segura[7].

Nesse Congresso, a Espanha faz um breve resumo das alterações em seu sistema penal, na busca do equilíbrio entre a firmeza que deve ter o estado na sanção da crimi-

5 Disponível em: <https://www.weforum.org/projects/cybercrime>. Acesso em: 11 set. 2017.

6 Disponível em: <https://www.weforum.org/projects/cybercrime>. Acesso em: 11 set. 2017.

7 Disponível em: <http://www.un.org/es/events/crimecongress2015/about.shtml>. Acesso em: 7 set. 2017.

nalidade mais grave e a proteção das vítimas desses crimes – anunciando a criação do Estatuto das Vítimas. Reitera a importância da cooperação internacional e das Convenções das Nações Unidas para o combate aos crimes graves[8].

A delegação brasileira reiterou o compromisso do país com a implementação da Convenção de Palermo e seus Protocolos, anunciando ter aprovado internamente a Lei sobre o Crime Organizado (Lei nº 12.850/2013). No que tange ao cibercrime, deixou registrada sua posição favorável à cooperação internacional e anunciou a aprovação do Modelo Regulatório da Internet (Lei nº 12.965/2014)[9].

No Brasil, o Projeto de Lei nº 86/1999 (PL), que pretendia dispor sobre os crimes cometidos na área de informática e suas penalidades, tinha como um dos objetivos ajustar a legislação brasileira à Convenção de Budapeste.

Diversos dispositivos constantes do substitutivo do Senado Federal ao mencionado PL, sobre novas tipificações penais e obrigações administrativas dos provedores de acesso à internet, foram rejeitados pela Câmara Federal, e, com os vetos presidenciais, a Lei nº 12.735/2012 ficou restrita aos seus arts. 4º ("Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado") e 5º (autorizando o juiz a determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio, das condutas "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional", Lei nº 7.716/1989, art. 20, § 2º, II).

A Lei nº 12.737/2012, que dispõe sobre a tipificação criminal de delitos informáticos, incluiu o novo tipo penal "invasão de dispositivo informático" (art. 154-A e 154-B do CPB), e alterou os arts. 266 e 298 do CPB, tipificando penalmente a conduta de quem "interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" e equiparando a documento particular o cartão de crédito ou débito, tipificando penalmente o crime de falsificação de cartão, respectivamente.

O Marco Civil da Internet (MCI) (Lei nº 12.965/2014) estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil. Contudo, a "CPI – crimes cibernéticos"

8 Disponível em: <http://www.un.org/es/events/crimecongress2015/about.shtml>. Acesso em: 7 set. 2017.

9 Disponível em: <http://www.un.org/es/events/crimecongress2015/about.shtml>. Acesso em: 7 set. 2017.

apontou para a necessidade de alteração do MCI, para nele incluir dispositivo que dê maior celeridade para a retirada de conteúdo ofensivo à honra das pessoas e para impedir a replicação desses mesmos conteúdos.

Outra alteração proposta pela CPI foi a de incluir no rol das informações cadastrais de usuários o endereço IP (*Internet Protocol*), o que "facilitaria a identificação de criminosos ou pessoas investigadas, diminuiria os tempos de atuação e aumentaria a eficácia no combate aos crimes digitais" (CPI – crimes cibernéticos, 2016).

O *cyberbullying* na Lei nº 13.185/2015 é concebido como sendo a intimidação sistemática na rede mundial de computadores, "quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial" (art. 2º, parágrafo único).

Não há, contudo, tipificação penal para as condutas que configuram o *cyberbullying*, as quais, no entanto, "podem ser sancionadas com a utilização do art. 138 (Calúnia), art.139 (Difamação), art.140 (Injúria) e art. 147 (Ameaça), este último condicionado à representação da vítima" (DODGE, 2013, p. 159), todos do CPB.

4 Direito Internacional e Ordem Jurídica Interna

Nem sempre a criança contou com tratamento condigno na legislação e na ação do Estado e da sociedade, mas desde principalmente a Declaração Universal dos Direitos do Homem, o sistema de proteção dos direitos humanos passou a incorporar a concepção de que a criança é sujeito de direitos, um marco para estender a incorporação desse entendimento a diversos ordenamentos jurídicos.

Destaca-se, em especial, a Convenção Sobre os Direitos da Criança (1989) – que considera criança todo ser humano menor de 18 anos de idade –, e seus dois Protocolos Facultativos: o Protocolo Facultativo Referente à Venda de Crianças, à Prostituição Infantil e à Pornografia Infantil (2000), o Protocolo Facultativo Relativo ao Envolvimento de Crianças em Conflitos Armados (2000).

A responsabilidade dos Estados nacionais na garantia de medidas eficazes de proteção dos direitos da criança está cabalmente consignada nos diversos instrumentos jurídicos internacionais; e a concreção dessa responsabilidade deve estar amparada

também no Direito Penal, na elaboração de tipos penais adequados e na condenação dos que cometem crimes contra crianças.

A proteção passa a ser direcionada ao desenvolvimento integral do ser humano em sua fase de formação; quer seja ao seu desenvolvimento físico quer seja ao seu desenvolvimento psicológico, intelectual, sexual, a proteção é integral e se faz pela família, pela sociedade e pelo Estado.

No que toca ao cibercrime, considerando o fluxo transnacional das ações delituosas cometidas pela internet, tornou-se imperativa a elaboração de um marco normativo penal que não ficasse limitado pela soberania do Estado-nação e pelo princípio da territorialidade.

A "Internet é uma tecnologia global, e muitas das regulações relativas a ela são inspiradas nesse pressuposto [...] as suas disposições devem ser interpretadas conforme o caráter internacional" (LORENZETTI, 2004, p. 90).

Os ordenamentos jurídicos internos dos Estados preveem maneiras de incorporar tratados e convenções internacionais, como parte importante da consolidação da proteção internacional aos direitos humanos.

A Constituição da Espanha, por exemplo, reconhece expressamente a Declaração Universal dos Direitos Humanos, os tratados e os acordos internacionais por ela ratificados, como sendo fontes de interpretação das normas relativas aos direitos fundamentais e às liberdades nela expressas (art. 10.2).

Ainda, em seu art. 96.1, prevê que, depois de publicados oficialmente no país, os tratados internacionais validamente celebrados formarão parte de seu ordenamento jurídico interno e suas disposições somente poderão ser derrogadas, modificadas ou suspensas pela forma prevista nos próprios tratados ou de acordo com as normas gerais de Direito Internacional, o que autoriza que qualquer particular pode invocar os direitos das crianças enunciados na Convenção sobre os Direitos das Crianças, frente a juízes e tribunais espanhóis.

Reforçando a matéria dos citados artigos, o disposto no art. 39.4 da Constituição de Espanha prevê que as crianças gozarão da proteção prevista nos acordos internacionais que velam por seus direitos.

A Constituição Federal Brasileira (CFB), por seu turno, determina que "as normas definidoras dos direitos e garantias fundamentais têm aplicação imediata" no país (art. 5º, § 1º), admitindo a inclusão de outros direitos e garantias, além dos já nela expressos, que sejam "decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte" (art. 5º, § 2º).

Além disso, prevê que "os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros", equivalham à norma constitucional resultante do poder derivado (emenda constitucional).

O Brasil também se submete à jurisdição do Tribunal Penal Internacional, nos termos do art. 5º, § 3º, CFB (TRINDADE, 2003, p. 506), e incorporou a doutrina da proteção integral da criança e do adolescente, ao teor dos arts. 226 e 227 da Constituição Federal. No "Estatuto da Criança e do Adolescente" (ECA) (Lei nº 8.069/1990), criança é a pessoa com até 12 anos incompletos e, adolescente, a pessoa de 12 até 18 anos incompletos.

O Direito Comunitário desponta como uma ordem jurídica de cunho constitucional e supranacional, "com capacidade, inclusive, para submeter as constituições nacionais ao seu poder supremo" (RODRIGUES, 2000, p. 96).

Exemplo mais firme é o da União Europeia (UE), ganhadora do Prêmio Nobel da Paz (2012), da qual a Espanha é membro e com a qual, portanto, compartilha sua soberania em assuntos comunitários.

Os Estados, ao formarem a UE, transferiram a primazia de sua soberania à comunidade que eles mesmos criaram e, como um dos princípios dos direitos dos tratados é o de que nenhum Estado-Membro pode atentar contra a validez do Direito Comunitário no âmbito dessa comunidade, prevalecerá a norma comunitária em caso de conflito com uma norma interna.

A harmonização das legislações internas dos Estados-Membros da UE é realizada por meio dos Regramentos comunitários, das Diretivas e das Decisões Marco, de natureza eminentemente supranacional.

As normas emanadas das instituições comunitárias (Parlamento, Conselho e Comissão) têm eficácia direta e primazia sobre as normas internas dos Estados; somente em

caso de a situação envolver conflitos exclusivamente internos ou que afetem cidadãos de terceiros países, o Direito Comunitário pode deixar de ser aplicado.

Com o Tratado Sobre o Funcionamento da União Europeia (2007), foi atribuída ao Parlamento e ao Conselho Europeu a competência para estabelecer, por meio do processo legislativo adequado, regras mínimas relativas à definição das infrações penais e das sanções em domínios de criminalidade particularmente grave e com dimensão transfronteiriça – como o terrorismo, tráfico de seres humanos, exploração sexual de mulheres e crianças, criminalidade informática e criminalidade organizada (art. 83).

A Decisão 2004/68/JAI do Conselho Europeu, relativa à Luta contra a Exploração Sexual de Crianças e a Pornografia Infantil, foi posteriormente substituída pela Diretiva 2011/92/UE do Parlamento Europeu e do Conselho, relativa à Luta contra o Abuso Sexual e a Exploração Sexual de Crianças e a Pornografia Infantil, mas sua importância reside na sua finalidade de reduzir "as disparidades entre as abordagens jurídicas nos Estados-Membros" para o desenvolvimento de uma cooperação eficaz nos domínios policial e judiciário contra a exploração sexual de crianças e a pornografia infantil.

Considerando que algumas vítimas do tráfico de seres humanos também foram crianças vítimas de abuso sexual ou de exploração sexual, a nova Diretiva 2011/92/UE tem natureza complementar da Diretiva 2011/36/UE, relativa à prevenção e luta contra o tráfico de seres humanos e à proteção das vítimas, e que substituiu a Decisão-Quadro 2002/629/JAI do Conselho.

Cabe também fazer referência à Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, que alterou e alargou o âmbito das disposições da Decisão-Quadro 2005/222/JAI do Conselho, abrangendo os ataques contra os sistemas de informação utilizando botnets (o ato de estabelecer o controle a distância de grande número de computadores mediante a respectiva contaminação com software maligno por meio de ciberataques focalizados), incluindo ataques na forma de navegação de serviço, ataques contra sistemas de informação perpetrados por organizações criminosas, conforme a Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada.

A Diretiva 2013/40/UE compele os Estados-Membros a tipificarem penalmente em seus ordenamentos jurídicos internos o acesso ilegal aos sistemas de informação, a interferência ilegal nesse sistema, a interferência ilegal nos dados e a instigação, o auxílio, a cumplicidade e a tentativa.

Estipula penas máximas de prisão não inferior a dois anos de prisão, ou de três anos, nos casos de interferência ilegal no sistema ou nos dados e se essas infrações forem cometidas intencionalmente, afetando um número significativo de sistemas de informação, ou de cinco anos de prisão, se as infrações forem cometidas no âmbito de uma organização criminosa – na acepção da Decisão-Quadro 2008/841/JAI –, e, independentemente da sanção nela prevista, causem danos graves ou forem cometidas contra um sistema de informação que constitua uma infraestrutura crítica.

Percebe-se no teor dessa Diretiva o estímulo à utilização de outros instrumentos além do Direito Penal na luta contra a cibercriminalidade, tais como medidas de prevenção, educação, segurança, e a criação de uma entidade reguladora na União Europeia – o Centro Europeu da Cibercriminalidade, criado em 2013.

No documento "Estratégia 2009-2011 – Construir uma Europa para e com as Crianças", atribuiu-se ao Conselho da Europa o papel de motor regional e coordenador das iniciativas nacionais e regionais de combate à violência contra as crianças, e ao Fórum Europeu o papel de acompanhar a aplicação das recomendações formuladas no Estudo do Secretário-Geral das Nações Unidas sobre a Violência contra as Crianças – que recomenda a adoção de uma legislação que proíba todas as formas de violência contra as crianças em todos os contextos.

Entre as Diretrizes do Conselho da Europa sobre as estratégias nacionais integradas de proteção das crianças contra a violência, Resolução do Conselho de Ministros (2009)10, registra-se:

a. Dar prioridade à prevenção da violência e proteção aos direitos da criança, segundo as seguintes ações: (*i*) definindo uma idade mínima para consentimento sexual; (*ii*) proibindo o emprego em trabalhos que envolvam contato com crianças a pessoas condenadas por crimes violentos, incluindo de natureza sexual, cometidos contra crianças; (*iii*) desenvolvendo programas de intervenção e medidas para avaliar e prevenir o risco de práticas de violência contra as crianças.
b. Devem ser tomadas as medidas legislativas, administrativas, sociais e educacionais apropriadas para proibir: (*i*) todas as formas de abuso e violência sexual, corrupção de crianças e solicitação para fins sexuais; (*ii*) todas as formas de exploração das crianças, incluindo prostituição, pornografia, exploração sexual infantil em viagens e turismo, tráfico, venda de crianças, adoção ilegal, trabalhos ou serviços forçados, escravatura e práticas similares, remoção de órgãos, para qualquer fim ou sob qualquer forma; (*iii*) todas as formas de exploração das crianças pelo

uso das novas tecnologias; (*iv*) a exposição das crianças a conteúdos violentos ou prejudiciais, independentemente da sua origem e por qualquer meio; (*v*) todas as formas de violência em instituições residenciais; (*vi*) todas as formas de violência na escola.

c. *Devem ser tomadas as medidas legislativas* e outras que se façam necessárias para assegurar que as pessoas coletivas possam ser responsabilizadas pelos crimes previstos no art. 26º da Convenção do Conselho da Europa sobre a Proteção das Crianças contra a Exploração e o Abuso Sexual.
d. *Devem ser adotadas sanções*: (*i*) nos crimes violentos, incluindo os de natureza sexual, cometidos contra crianças, os quais devem ser punidos por sanções e medidas efetivas, proporcionais e dissuasórias, tendo em consideração a gravidade dos crimes.
e. Devem ser adotadas as seguintes medidas: (*i*) os condenados por crimes violentos, incluindo os de natureza sexual, cometidos contra crianças, assim como os sujeitos a processo penal, devem ter acesso a medidas e programas efetivos de intervenção com vista à prevenção e minimização dos riscos da repetição dos crimes; (*ii*) em conformidade com os princípios de integração social e educação e da prevenção de reincidência, qualquer sistema judicial que lide com crianças autoras de violência deve ser integrado com as iniciativas sociais mais abrangentes com vista a assegurar uma abordagem holística e de continuidade dos cuidados dessas crianças (princípio do envolvimento da comunidade e cuidados permanentes).
f. *Considerar circunstâncias agravantes*: (*i*) o recurso à violência contra as crianças deve ser considerado como uma circunstância agravante na determinação de uma sanção; (*ii*) outras circunstâncias a considerar, na medida em que não integrem os elementos constitutivos do crime, devem incluir o abuso de uma posição reconhecida de confiança, autoridade ou influência sobre a criança, de uma relação baseada em dependência econômica ou outra e o envolvimento numa organização criminosa.
g. *Medidas relativas à jurisdição*: (*i*) devem ser tomadas as medidas legislativas e outras necessárias para estabelecer a jurisdição sobre crimes violentos, incluindo os de natureza sexual, cometidos contra as crianças que sejam nacionais do país ou tenham a sua residência habitual nesse território; (*ii*) em concordância com os requisitos dos tratados internacionais, devem tomar-se as medidas legislativas ou outras necessárias para estabelecer a jurisdição nacional sobre crimes violentos, incluindo os de natureza sexual, cometidos contra as crianças no estrangeiro por nacionais do país e pessoas que tenham a sua residência habitual nesse território; (*iii*) para assegurar legislação efetiva extraterritorial, a acusação dos autores

e a imposição de sanções, deve ser abolido o requisito de dupla incriminação e facilitada a assistência judiciária mútua.

Os seguintes instrumentos jurídicos emanados da União Europeia, recentemente incorporados à legislação da Espanha, tratam não só de tipificação jurídico-penal, mas incluem outras medidas concernentes à comunidade, ao delinquente, às vítimas e aos sistemas informáticos: a Diretiva 2011/93/EU (relativa à luta contra a exploração sexual de crianças e a pornografia infantil), a Diretiva 2013/40/EU (relativa aos ataques contra os sistemas de informação e a interceptação de dados eletrônicos quando não se tratar de comunicação pessoal), a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho (relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União), as exigências da Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e o Abuso Sexual (proteção das crianças contra a exploração e o abuso sexual), de 25 de outubro de 2007, e a Diretiva 2014/42/EU (sobre o congelamento e a perda dos instrumentos e produtos do crime na União Europeia).

5 Conclusão

Em face de todo o exposto, podem-se tirar algumas conclusões sobre o movimento de expansão do Direito Penal num mundo de crescente aumento no número de usuários da internet, principalmente de crianças (menores de 18 anos), no contexto internacional, regional e nacional de proteção dos direitos humanos, e das crianças, em específico.

O fenômeno da globalização é causa e consequência da revolução tecnológica que vem se consubstanciando no mundo nas últimas décadas e, a despeito das inúmeras vantagens que a interconexão global por meio da internet vem trazendo, vem acompanhada de uma série de condutas reprovadas pela sociedade, passíveis de ser objeto de proteção pelo Direito Penal.

Algumas dessas condutas já estão previstas em ordenamentos jurídicos nacionais e têm tipificação penal capaz de a elas serem aplicadas; outras condutas, porém, passam a exigir a criação de novos tipos penais pelo legislador, obrigado então a criar tipos penais que se amoldem à necessidade de proteção de bens jurídicos individuais e supraindividuais passíveis de serem alcançados pela cibercriminalidade.

Com a sociedade de risco, passa a ser demandada a antecipação da tutela penal, por meio de tipos penais de perigo, e a adequação da ordem jurídica internacional e nacional à proteção dos direitos humanos universais e indivisíveis, interconectados e cada vez mais fortalecidos internacionalmente.

Diversos tratados e convenções internacionais vêm sendo firmados pelo conjunto de Estados-Nação com a finalidade de tentar uniformizar as ações e de traçar diretrizes de cooperação mútua no âmbito jurídico-penal e policial, para o combate à cibercriminalidade em ascensão.

Seja a criminalidade organizada, seja a criminalidade individual, a internet tem demonstrado ser um instrumento quase perfeito para delinquentes dos mais diversos matizes, que nela encontram o fluxo livre para sua conduta criminosa, tendo em vista a enorme dificuldade de regulação global da internet.

Cada país tem sua legislação própria e sua jurisdição normalmente fundada no princípio da territorialidade, em contraste com a falta de território definido no ciberespaço.

Sendo assim, é a criança, ser humano em formação, que passa a ser foco de abusos de todo o tipo, exigindo um esforço das autoridades em traçar estratégias de sua proteção contra esses abusos.

A União Europeia vem demonstrando ser um exemplo a ser seguido em muitas de suas ações voltadas para a proteção às crianças, incorporadas nos ordenamentos jurídicos internos em decorrência da supremacia do Direito Comunitário formado pelas importantes Decisões Marco e Diretivas.

A agregação ao ordenamento jurídico espanhol de tipos penais relativos à cibercriminalidade contra crianças, por exemplo, vem ocorrendo no âmbito da inclusão de diretrizes e normas jurídicas emanadas da União Europeia ao seu ordenamento interno, em especial a inclusão de normas jurídico-penais ao seu Código Penal, seguindo os princípios de sua Constituição.

No Brasil, tem ocorrido uma maior previsão de tipos penais novos em leis especiais, formando, em conjunto com o Código Penal Brasileiro, um plexo de normas penais que abrange diversos delitos, inclusive condutas danosas perpetradas por meio da internet.

Por fim, apesar dos esforços da comunidade internacional e dos países – em específico, da Espanha e do Brasil –, ainda há muito para se caminhar no combate à cibercriminalidade contra a criança, tanto pela transformação contínua das condutas delitivas que vão sendo constantemente inovadas na internet, como pela necessária transposição das barreiras territoriais e o fortalecimento de uma cooperação internacional mais sólida.

Referências

AMBOS, Kai. **Direito Penal**: fins da pena, concurso de pessoas, antijuridicidade e outros aspectos. Porto Alegre: Sergio de Fabris, 2006.

ANITUA, Gabriel Ignacio. **Histórias dos pensamentos criminológicos**. Rio de Janeiro: Revan – Instituto Carioca de Criminologia, 2008.

CASABONA, Carlos María Romeo. De lós Delitos Informáticos al cibercrimen. Una aproximación conceptual y político-criminal. In: CASABONA, Carlos María Romeo (Coord.). **El cibercrimen**. Granada: Comares, 2006.

BRASIL. Câmara Federal. Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade no Brasil (CPI – crimes cibernéticos). **Relatório**, 2016.

DODGE, Raquel E. F. (Org.). **Roteiro de atuação**: crimes cibernéticos. 2. ed. rev. Brasília: MPF/2CCR, 2013.

ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME – UNODC. **Comprehensive Study on Cybercrime**. 2013. Disponível em: <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>. Acesso em: 14 set. 2017.

FARIA, José Eduardo. **O Direito na Economia Globalizada**. São Paulo: Malheiros, 2004.

FERNÁNDEZ, Antonia Monge. **De los Abusos y Agresiones Sexuales a Menores de Trece Años**. Barcelona: Bosch, 2011.

FIORILLO, Celso Antonio Pacheco. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

GRECO, Rogério. **Curso de Direito Penal** – Parte Especial. Niterói: Ímpetus, 2011. v. 3.

HOLLIS, Duncan B. An e-SOS for Cyberspace. **Harvard International Law Journal**, v. 52, n. 2, p. 374-431, 2011.

INTERNET WATCH FOUNDATION – IWF. **IWF Annual Report 2016**. 2017. Disponível em: <https://www.iwf.org.uk/sites/default/files/reports/2017-04/iwf_report_2016.pdf>. Acesso em: 11 set. 2017.

ISHIDA, Válter Kenji. **Estatuto da Criança e do Adolescente**: doutrina e jurisprudência. São Paulo: Atlas, 2010.

LORENZETTI, Ricardo L. **Comércio Eletrônico**. São Paulo: RT, 2004.

MARTÍNEZ SÁNCHEZ, M. Teresa. **El acceso a menores con fines sexuales através de las TIC**: delito online child grooming y embaucamiento de menores, tras la reforma del CP por la LO 1/2015. Disponível em: <http://www.elderecho.com/tribuna/penal/Delitos-sexuales-menores-internet-TIC-child-grooming_11_1080055001.html>. Acesso em: 19 set. 2017.

PIOVESAN, Flávia. **Direitos Humanos e Justiça Internacional**. São Paulo: Saraiva, 2006.

_____. **Temas de Direitos Humanos**. São Paulo: Saraiva, 2009.

PRADO, Luiz Regis. Norma Penal como Norma de Conduta. **Ciências Penais**, v.12, p. 231, jan. 2010. DTR\2010\585.

_____. **Bem Jurídico-Penal e Constituição**. São Paulo: RT, 2011.

PUIG, Santiago Mir. **Función de La Pena y Teoria del Delito em el Estado Social y Democratico de Derecho**. Barcelona: Bosch, 1982.

RODRIGUES, Mauricio Andreiuolo. **Poder Constituinte Supranacional**: esse novo personagem. Porto Alegre: Antonio Fabris, 2000.

ROSSINI, Augusto. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: RT, 2003.

SILVA SÁNCHES, Jésus-María. **Aproximação ao Direito Penal Contemporâneo**. São Paulo: RT, 2011.

SMANIO, Gianpaolo Poggio. Princípios da Tutela Penal dos Interesses ou Direitos Difusos. **Justitia**, São Paulo, v. 64, n. 197, jul./dez. 2007.

TRINDADE, Antônio Augusto Cançado. **Tratado de Direito Internacional dos Direitos Humanos**. Porto Alegre: Sergio Fabris, 2003. v. 1.

_____. **Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children**. 2015. Disponível em: <https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_ Effects.pdf>. Acesso em: 14 set. 2017.

WEBSTER, S. et al. **European Online Grooming Project Final Report**. 2013-2014. Disponível em:<https://www.unodc.org/documents/organized-crime/ cybercrime/Study_on_the_Effects.pdf>. Acesso em: 14 set. 2017.

CRIMES CIBERNÉTICOS

9 ÉTICAS EM REDE: PAUTAS PARA A LUTA CONTRA A PORNOGRAFIA INFANTIL E OS DELITOS DE ÓDIO NOS SITES DE REDES SOCIAIS

Clóvis de Barros Filho[1]
Luiz Peres Neto[2]

Resumo: Este trabalho busca problematizar a luta contra a pornografia infantil e delitos de ódio nos sites de redes sociais a partir de questões éticas. Para tal, argumenta-se, em um primeiro momento, a necessidade de uma abordagem multidisciplinar pela via da complexidade visto que, sem uma visão holística, tende-se a vislumbrar uma questão jurídica ignorando o problema ético que a permeia e dá fundamento. Isso posto, entende-se, em um segundo momento, que a intolerância e os limites da ação moral, problemáticos nos sites de redes sociais, são os mesmos existentes fora de tal âmbito. Precisamente por isso, essa discussão requer situar a alteridade como elemento humanista central. A intolerância como tendência de não aceitar o outro é a base moral para o mal. Sem o respeito à alteridade como elemento ético, argumenta-se que perdemos a base mínima que sustenta o garantismo pragmático essencial para enfrentar problemas como a pornografia infantil ou os delitos de ódio que, desde a sua genealogia moral, constituem-se como exemplos execráveis da banalização do mal absoluto sem cair no chamado populismo punitivo.

Palavras-chave: Ética. Pornografia infantil. Discurso de ódio. Sites de redes sociais.

Abstract: *From ethical perspectives, this work aims to question the fight against child pornography and hate felonies in social media sites. Hence, it is argue, firstly, the necessity of a multidisciplinary approach from a complexity point of view considering that without a holistic attitude it tends to be glimpsed the juridical problem deprived of its ethical problem. Secondly, it is assumed that intolerance and the limits of moral action so problematic in social media websites are the same outside of it. Therefore, this discussion must put the otherness as a key humanistic element. Intolerance, as a shut down to the otherness is the moral foundation to the evil. It is argued, thirdly, that without the otherness as an ethical element, we lose the minimal basis of the garantism paradigm that are essential to deal against child pornography and hate felonies far away from penal populism, facing its moral foundations that are examples of the banality of the absolute evil.*

1 Palestrante e consultor no Espaço Ética. Livre-docente e doutor em comunicação pela Escola de Comunicações e Artes da Universidade de São Paulo (ECA-USP). Doutor em Direito pela Université de Paris III (Sorbonne-Nouvelle), mestre em Science Politique pela Université de Paris II, bacharel em Jornalismo pela Faculdade de Comunicação Social Cásper Líbero e bacharel em Direito pela Universidade de São Paulo.

2 Professor titular do Programa de Pós-Graduação em Comunicação e Práticas de Consumo da ESPM-SP. Pós-doutor em comunicação como Capes/Fulbright Fellow na Annenberg School for Communication da University of Pennsylvania. Doutor e mestre em comunicação pelo Departament de Ciències Polítiques i Dret Públic da Universitat Autònoma de Barcelona. Bacharel em Comunicação pela Escola de Comunicações e Artes da Universidade de São Paulo.

Keywords: Ethics. Child pornography. Hate speech. Social media sites.

1 Ponto de partida: complexidade exige multidisciplinariedade

Abordar o tema do crime de pornografia infantil e dos delitos de ódio nos sites de redes sociais a partir da ética requer um exercício epistemológico de grande envergadura. Blaise Pascal (2004), nos seus "Pensamentos", ensina-nos sobre a tragédia do conhecimento. Muitas obras são grandes, ainda que inacabadas. Outras são inacabadas porque simplesmente são incompletas. Sob essa última assertiva emoldura-se o presente artigo. Sabemos de antemão que este trabalho será incompleto. Cabe-nos como autores, contudo, apontar, sinalizar as brechas que serão deixadas. E não serão poucas.

A partir das lentes teóricas da ética, glosaremos sobre dois âmbitos da criminalidade – a pornografia infantil e os delitos de ódio – que têm fortes vínculos com o âmbito das comunicações mediadas por computadores, em geral, e os chamados sites de redes sociais, em particular. Como pergunta de investigação, lançamos o questionamento de qual seria o papel da ética no combate/prevenção do crime de pornografia infantil e dos delitos de ódio que se valem de uma ambiência comunicacional nos sites de redes sociais.

Os autores são conscientes de que será impossível abordar todos os aspectos e variáveis imbricadas no fenômeno em questão. Deixaremos de fora as considerações acerca das tipificações das condutas ilícitas ou das nuances dos tipos penais abordados. Falta-nos competência para tal e sabemos que outros o farão, nesta obra, com maior valia. Tampouco seremos capazes de discutir a fundo estratégias integrais de prevenção. Limitar-nos-emos, com mesóclises e tudo o que a linguagem nos permitir, àquilo a que dedicamos as nossas pesquisas: o fenômeno da moralidade. Interessa-nos a questão ética que dá corpo e fundamento ao problema social desses delitos, forjados e ampliados em ambiências comunicacionais. Isso não impede – e de certo modo requer – uma abordagem multidisciplinar, necessária ante a complexidade do tema em pauta.

Antes de qualquer outra consideração é imperativo explicitar o que entendemos, neste trabalho, por multidisciplinariedade e por complexidade, dois conceitos caros a grande parte dos cientistas sociais que recorrem a ambos. Ademais do acesso a vários autores e paradigmas de filiações disciplinares diversas, uma abordagem multidiscipli-

nar é aquela que contempla uma tessitura plural. Mais do que o prefixo latino de muitos, o viés da multidisciplinaridade nos permite explorar autores e escolas diversos entre si.

Por sua vez, a complexidade exige cautela. O pensamento complexo, ensina Edgar Morin (2005), é aquele que vislumbra uma compreensão do mundo como uma entidade na qual tudo está entrelaçado. Destarte, uma análise sob a égide da complexidade é aquela que caminha na direção contrária do tradicional fazer científico cartesiano. Não há partes. Há um todo urdido. O crime de pornografia infantil e os delitos de ódio precisam, por exemplo, de considerações que transcendam o universo jurídico sem que, contudo, abandone-se a dimensão legal. Deslindando a teia que os contorna, bem como em questões que nos afligem eticamente, deve-se explorar os fios com os quais esses gravíssimos problemas estão entrelaçados com elementos culturais, econômicos, sociais, comunicacionais etc. Ainda que distintos entre si, hodiernamente, ambos os delitos têm raízes comunicacionais.

Precisamente por isso enfrentamos o objeto em questão, em um primeiro momento, pelos vínculos comunicacionais que o atravessam, muito em particular a comunicação mediada por computadores. Alex Primo (2007) explica que comunicação mediada por computadores envolve toda a interação entre pessoas no ciberespaço.

Cabe aqui um parêntese. O crime de pornografia infantil e os delitos de ódio existem muito antes dos computadores e das redes sociotécnicas estabelecidas a partir destes. No entanto, ganham novos nuances e contornos a partir da sua dimensão *cyber*. O primeiro, como explica Ramos Vásquez (2016), tem uma ampla relação com o âmbito da internet, quer seja por práticas como o "*grooming*" – utilizar a internet para atrair menores com propósitos sexuais –, o armazenamento e difusão de conteúdo pornográfico envolvendo menores ou a criação de redes para a exploração de menores com fins de difusão e intercâmbio de arquivos em rede[3]. Já o segundo também adquire certas especificidades com a popularização da internet, muito especialmente por aquilo que a literatura anglo-saxã convencionou chamar de "hate crimes" cuja natureza criminal ganha uma enorme po-

3 Ao fazer pequena matização, a partir do que trabalham autores como Ramos Vázquez (2016), Mitchell et al. (2013) ou Wolak (2008) há uma obsessão do legislador para com a relação entre crimes sexuais envolvendo menores e internet. Inúmeros estudos criminológicos arrolados pelos mencionados autores sinalizam que não haveria um problema social compatível com a profusão de leis penais nesse âmbito; apontam a marginalidade do grooming e criticam a ênfase na posse de material pornográfico em detrimento do combate aos âmbitos intrafamiliares e comunitários nos quais grande parte dos casos de delitos sexuais com menores vítimas ocorrem. Caberia aqui, ademais, uma matização ao termo de uso corrente "pedofilia", especialmente empregado nos meios de comunicação de massa, usado para designar crimes sexuais com vítimas menores de idade quando, em sua origem, trata-se de um termo psiquiátrico controverso na literatura médica, conforme explica Malón Marco (2012). É importante salientar que tais críticas não fazem do problema um mal menor. Pontuam, no entanto, questões a serem consideradas.

tência a partir do advento da web 2.0 e das possibilidades da "*mass self communication*" (CASTELLS, 2009), a comunicação de um para muitos (massa) via redes[4].

Durante muito tempo, no entanto, falou-se do ciberespaço como algo não real. Um lugar distante. Não é difícil entender algumas das razões. Argumentos de que existe um mundo "on-line" e outro "off-line" ainda perduram. Por essa razão, a internet foi (ou ainda é) tratada como um espaço de riscos. Um equívoco duplo. Em primeiro lugar, porque o virtual também é real. Não é preciso ser filósofo para saber que a sua conta bancária, acessada via site, é real. Ela existe. Talvez não tenha o saldo que você gostaria. Mas é real. Tudo aquilo que sucede nos sites de redes sociais também é real. Existe. Pode não ter uma correspondência com a realidade física. Porém, não carece de realidade. Em segundo lugar, porque a internet não é um espaço de risco em si. A sociedade do risco, diria Beck (2006), não se dá apenas dentro ou unicamente fora da internet. A visão de que a internet é um espaço de riscos é pautada muito mais pelo desconhecimento das dinâmicas comunicacionais desta do que por qualquer outra coisa. Os riscos que corremos ao nos conectarmos à rede global de computadores têm suas idiossincrasias. É inegável. Mas não são maiores ou menores do que atravessar a pé as pistas expressas da Marginal Tietê, em São Paulo, dar um passeio às 3 horas da madrugada na Avenida Vieira Souto, no Rio de Janeiro, empunhando um relógio da marca Rolex, fazer sushi a partir de um tutorial do YouTube ou engolir fogo em um espetáculo circense. A visão social do risco está muitas vezes mais atrelada ao medo do desconhecido socialmente, do constituído intersubjetivamente do que da potencialidade ou letalidade de situações concretas. A sociedade dos riscos opera baseando-se em perigos abstratos e medos difusos. Ambos forjados no seio da modernidade a partir do devir das sociedades industriais.

O novo, o desconhecido assustam. Isso não é de hoje. A história da indústria cultural ensina. Contam Briggs e Burke (2006) que foi assim com a chegada do cinema. Medo. Qual o efeito dessa mídia nas nossas mentes, olhos e cabeças, perguntaram assustados alguns detratores. Com a rádio tampouco foi diferente. Afinal, alterou-se até mesmo a dinâmica cotidiana das famílias, criando em muitos lares uma sala ou espaço para o consumo de tal mídia, o que aprofundou-se ainda mais com a televisão, cujos efeitos puderam ser vistos até mesmo na rotina de refeições. Durante grande parte da década de 1980, notabilizou-se a crítica – muitas vezes infundada – de que o consumo televisivo conduziria mimeticamente a condutas sociais indesejadas. Agulha hipodérmica revisitada. Superficialidade daqueles que acreditam que a audiência é composta por recep-

4 Por delitos de ódio, aludimos ao conjunto de crimes com base discriminatória cometido em função dos pertencimentos, etnicidades ou identidades da vítima, como nos casos de atos violentos impetrados em função de raça, religião, orientação sexual, identidades de gênero, idade, deficiência física ou mental, etnia ou nacionalidade. Sobre o conceito de delitos de ódio e casos, recomendamos a leitura do trabalho de Verkhovsky (2016), que realiza, ademais, um interessante exercício de direito comparado.

tores passivos. Outra coisa, bastante diferente, é falarmos em manipulação informativa, propaganda e formação de consensos a partir da economia política das mídias, como bem explicam Herman & Chomsky (2008). Mas, como dito, essa é outra questão que não nos toca neste trabalho.

A expansão das redes sociotécnicas de comunicação também é causa de medos, em particular, a partir da constituição daquilo que se convencionou chamar de redes sociais para aludir às redes sociais digitais ou aos sites de redes sociais, como denominam Charles Ess (2014) e a maior parte da literatura especializada em internet. Seguimos, neste trabalho, a denominação de "sites de redes sociais" (SRS). Afinal, as redes sociotécnicas de comunicação não nasceram com a internet. Já existiam com as chamadas mídias tradicionais. A rádio ou a televisão, por exemplo, sempre se articularam a partir de redes de afiliadas, repetidoras e retransmissoras. As redes sociais também não são exclusividade do universo virtual. Estabelecemos redes com fins sociais desde sempre.

O advento da internet ampliou, no entanto, as redes sociais e introduz uma série de particularidades, complexificando o processo comunicacional, como indica Raquel Recuero (2013). Em primeiro lugar, a comunicação mediada por computadores na internet permitiu a assincronia, o que foi decisivo para o surgimento de novos fóruns públicos de discussão. Em segundo lugar, deu maior poder ao usuário, sendo este chamado por alguns autores, como Castells (2009), de prossumidor, dado o caráter de consumidor proativo ou graças à simultaneidade na produção/consumo de conteúdos.

Contudo, foi precisamente a partir do surgimento e da popularização dos chamados sites de redes sociais (Facebook, Twitter, o falecido Orkut etc.) que temos uma nova dinâmica comunicacional cujos conflitos éticos nos interessam para discutir o objeto proposto neste trabalho. Aponta Recuero (2013) que os SRS permitiram a representação individual dos atores e a publicização das suas conexões o que, consequentemente, gerou novas práticas de sociabilidade e de interação com a alteridade. A intolerância para com o outro, latente no mundo de pessoas de carne e osso, ganhou forma, representação e publicização.

2 Tolerância e os limites da ação moral para a prevenção delitiva no ciberespaço

Perscrutar os sites de redes sociais revela-se uma tarefa que traz ao pesquisador da ética uma plêiade de conflitos morais. Dentre todos destaca-se, sobejamente,

a intolerância. O "Show do Eu", segundo descrito por Paula Sibilia (2016), constitui-se como traço marcante dos processos de sociabilidade contemporânea no ciberespaço. Neste, a intimidade rompe os muros domésticos e ganha uma dimensão pública. Os SRS elevam a uma potência inimaginável esse processo. A exposição é também ponte para a interação. Um convite à comunicação, ainda que nem sempre esta seja a finalidade dos atores imersos nos SRS. Observa-se que grande parte dos usuários de tais redes são acometidos por um exercício de eliminação da humanidade do outro até mesmo como esfera contemplativa. Por isso, fala-se muito da intolerância nos SRS como fundamento moral que reveste os delitos de ódio ou que banaliza o mal da pornografia infantil.

A tolerância, enquanto problema ético, tem sempre por objeto o outro. Outro esse que difere de nós. Mas que também é, em essência, humano como nós. Assim, excluímos do âmbito da tolerância tudo o que diz respeito à natureza não humana. Como o sol que castiga as nossas vistas, a tempestade que nos encharca, o vento que nos brinda com o cisco que invade o olho. Se a tolerância diz respeito, portanto, à nossa relação com os semelhantes, cabe precisar seu objeto. O que no outro pode exigir de nós tolerância? Sua mera presença, como alguém sentado em nosso assento na aeronave? Seu pensamento? O discurso que manifesta esse pensamento? A comunicação gestual desse pensamento? Práticas que decorrem de convicções?

A tolerância diz respeito sempre a algo no outro que se apresenta como obstáculo às nossas pretensões. Assim, excluímos do âmbito da tolerância tudo aquilo que no outro nos alegra, nos motiva, nos cativa, que coincide com nossas convicções, facilita alcançar nossas metas, nossos propósitos. O verbo tolerar, nesse sentido, parece sempre indicar um empecilho, um obstáculo que o outro pode representar para o sucesso, a satisfação de nossas pretensões.

Ora, se o objeto da tolerância é sempre algo que nos dificulta e, portanto, em um primeiro momento nos entristece, caberá sempre a pergunta sobre os limites da nossa ação ante essa dificuldade objetivada no outro. A palavra tolerar por ela mesma aponta apenas para um reconhecimento da existência da causa de uma tristeza. E a aceitação da sua existência. Mas a palavra tolerar não indica os limites dessa aceitação e as condições de um eventual empenho para a remoção do obstáculo citado.

Se partirmos de uma perspectiva consequencialista, que usa como referência para os limites da ação a obtenção do que está sendo desejado, talvez o orbital de tolerância se estreite e o mero reconhecimento da presença ali do outro como obstáculo não impeça a tentativa imediata da sua remoção. Mas se pensarmos, seguindo esse mesmo pa-

radigma moral, em termos do que é bom para a maioria – traço fundante da perspectiva utilitarista – ou se de maneira ambiciosa ainda pretendermos identificar o que é melhor para todos, aí talvez tenhamos que submeter as nossas pretensões a condições legítimas de sua obtenção, o que alarga de imediato o orbital da conduta tolerante.

Se a moral tem por objeto o que devemos fazer, em atividade íntima de consciência e requer razão prática para a identificação de princípios e máximas que fundamentem limites para a ação humana, podemos facilmente diferenciar tudo o que é moral das nossas simples preferências. Assim, ao entramos em uma sorveteria e perguntarmos pelo sabor do sorvete da nossa preferência, evidentemente, saberemos que a nossa decisão termina ali, na particularidade da situação vivida entre bijus, potes e coberturas caramelizadas.

No entanto, toda reflexão íntima sobre a própria conduta ganha estatuto de moralidade quando o protocolo de pensamento que usamos autoriza a pretender uma extensão de eficácia superior àquele caso vivido. Assim, quando escolhemos sorvete de pistache ou de milho verde, sabemos tratar-se de pura preferência, e não pretendemos nenhuma superioridade moral dessa escolha frente a outras escolhas possíveis a não ser a soberania do nosso próprio paladar. No entanto, não é o mesmo quando decidimos não roubar, não furtar, não iludir, não ludibriar, não magoar, não ofender, porque, nesses casos, nossa escolha vai além da simples preferência e presume um alcance maior do que a experiência moral vivida aponta.

Talvez seria muito se pretendêssemos a universalidade ética de certas decisões, ou seja, que todos, ante as mesmas condições de ponderações práticas chegassem à mesma conclusão sobre o acerto da decisão tomada. O imperativo, nesse caso, é categórico porque justamente independe das perspectivas, das preferências, das inclinações, da vida vivida no mundo real. Ou acreditamos na possibilidade de que haja uma forma de pensar que garanta uma espécie de resposta certa para o agir decorrente da boa razão ou estaremos para sempre submetidos às contingências e aos apetites do momento.

De tal sorte talvez importe refletir sobre a tolerância para além da vida vivida, dos ódios e dos rancores, dos amores e das decepções. E isso só será possível se tivermos claro que tipo de convivência, que tipo de sociedade, que tipo de interação queremos para nós. Seja mediada por computadores ou não. Eis o finalismo da ética. O bem comum, a convivência democraticamente forjada a partir de valores toleráveis.

Como sempre acontece em questões éticas, a tolerância nos coloca em "cobertor curto". Por que quando respeitar a existência do outro – ainda que objetivada em obstáculos para as nossas pretensões – constitui-se um dever moral, é óbvio que não é tudo que podemos tolerar. Assim, parece evidente que não deva haver tolerância com o facínora, com o canalha, com o destruidor, com o assassino. Não há possibilidade de tolerar a discriminação e o ódio, nem mesmo em nome da liberdade de expressão. Porque uma democracia deve zelar pelo bem comum, pelo respeito à alteridade. Ainda que em cada um dos casos supracitados possa haver problematização possível, quando a vítima é a criança, nada pode justificar nem a conduta, nem a tolerância em relação à violência. Pela fragilidade física, pela falta de condições completas de juízo, pela sua natureza em formação, por não dispor de meios completos de avaliação do que lhe sucede, tampouco das suas consequências, o mal feito a uma criança parece ser sem problematização possível.

Desprovido de dilema, não é por acaso que o pensador Marcel Conche (2003) chamará o sofrimento da criança como o "mal absoluto". E a causa humana desse sofrimento, a blasfêmia moral por excelência. Ou melhor, por essência. Assim, cabe em cada sociedade a definição do orbital legítimo de tolerância que garante a possibilidade de existir e se posicionar, bem como a definição da fronteira de tudo aquilo que na conduta humana não há que tolerar sobre pena de endosso, de cumplicidade e solidariedade com o vil. Não tolerar, contudo, não significa esvaziar a dimensão humana do outro. Há de se buscar, para tal, uma ética mínima que seja fiadora dos direitos humanos e evite que se faça mero populismo punitivo daquilo que requer fundamentalmente uma repulsa e uma reação ética.

3 Ética mínima e o garantismo penal como meios para evitar o populismo punitivo

Toda ética é um ato de religação com o outro. Precisamos do outro para encontrarmos a nós mesmos. Porque a ética é uma reflexão sobre a conduta humana. Porque a ética é fundamentalmente humana. Não há ética no mundo das pedras, dos sapos ou dos papagaios. Recuperar o humanismo, recolocar o outro na rota de discussão sobre a tolerância é apostar por uma visada ética. Muito do debate social, midiático e até mesmo acadêmico sobre a criminalidade elimina a alteridade como merecedora de qualquer esfera de dignidade. E cai no fosso, na vala da intolerância e do senso comum. Não aquela intolerância que fundamenta a repulsa de condutas eticamente inaceitáveis em qualquer contexto, em qualquer circunstância. Aludimos ao crime de pornografia infantil e aos delitos de ódio, mas poderíamos incluir todos aqueles crimes contra a humanidade

que são, conforme argumentamos, intoleráveis do ponto de vista da ética. Evidentemente, há condutas éticas reprováveis. Culturalmente discutíveis. O que não inclui os casos supracitados.

A repulsa e intolerância necessárias à luta contra a pornografia infantil e os delitos de ódio não devem, conforme argumentado anteriormente, servir de coarctada para eliminar a dignidade humana do outro. Razão pela qual se faz necessário o religamento com o outro pelo caminho da ética e, entendemos, do garantismo penal, defendido por Ferrajoli (2006b), entre outros. Ética e direito penal como fundamentos para coesão social e democrática na pólis.

Ao longo da história da filosofia moral, como explica Cortina (2009), duas visões buscaram copar o comedido da ética: a justiça ou a vida boa. Estas não precisam ser visões excludentes. "A finalidade ética tem duas faces complementares. A primeira é a resistência à crueldade e à barbárie. A segunda é a realização da vida humana" (MORIN, 2005, p. 202). Por essa razão, cabe buscar uma "ética mínima", como propõe a filósofa espanhola Adela Cortina (2009). Não se trata de uma ética menor, e sim de parâmetros éticos indispensáveis, um mínimo denominador comum acerca da justiça, que impeça a barbárie e garanta a vida boa, a felicidade.

Para tal, contudo, é indispensável aceitar a alteridade. Como argumenta Levinas (2011), é preciso ver o outro como nós mesmos. Sem isso, é fácil aceitar a armadilha da intolerância que o senso comum nos prepara. Aquela intolerância inumana, que no Direito Penal ganha vestes de política criminal democrática e nome pomposo: tolerância zero. Ao contrário do que possa parecer, trata-se de uma política intolerante, inumana, na contramão da democracia e eticamente indefensável, como argumenta Loïc Wacquant (2006, 2000). Além disso, o supracitado sociólogo ainda comprova – para aqueles que queiram ver – que as políticas de tolerância zero são ineficazes. Antes de mais nada, por uma definição sociológica de manual. Não há como obter uma taxa de criminalidade zero. Se há ordem social, há de se pressupor, como o fez Durkheim, que o crime e a desordem sejam funcionais à própria ideia de sociedade. Uma taxa de criminalidade zero suporia a inexistência da sociedade. Ademais, como explica Wacquant, o famoso caso da cidade de Nova Iorque é tributário muito mais de uma campanha bem orquestrada de *marketing* do que qualquer outra coisa, ainda mais quando comparado com outras localidades norte-americanas que adotaram estratégias radicalmente diferentes e obtiveram resultados similares ou melhores, no mesmo período.

Uma das conquistas da modernidade é a ideia de que a convivência requer o exercício do monopólio da violência legítima limitado à lei. De tal sorte, toda teoria do Estado moderno está sedimentada a partir da noção de que a lei deve ser a "fonte normativa principal das relações de convivência" (BOBBIO, 1984, p. 103). Tomando essa noção, o garantismo incorpora a visão humanista, reinterpretando as teorias da justiça desde uma perspectiva ética e política capaz de depositar um olhar no indivíduo, e não no controle social estrito.

Destarte, Ferrajoli (2006b) descreve três características deontológicas que fundamentam o paradigma garantista: a separação entre Direito e moral, como meio de impedir que o moralismo fundamente a lei, a aceitação do constitucionalismo social, base para o assentimento da legitimidade e alcance das leis e, por fim, a diferenciação entre o direito (norma) e a realidade (fatos), que deve pautar a regulação de determinadas condutas. Assim, deve ficar claro ao conjunto da sociedade uma diferença entre o por que se castiga e por que determinadas condutas devem ser castigadas, reformulando a ideia utilitarista e retribucionista da pena. O Direito Penal não pode ser a vingança da sociedade ou da parte ofendida. Violento deve ser a *ultima ratio*. Deve ser, ademais, mínimo e proporcionado, posto que representa uma violência que precisa ser legítima. O garantismo abre espaço para a retirada do direito em favor da ética. Mais ética, menos Direito Penal. Nas palavras do próprio Ferrajoli (2006a, p. 332),

> Hay, sin embargo, otro tipo de fin al que cabe ajustar el principio de la pena mínima, y es la prevención no ya de los delitos, sino de otro tipo de mal antitético al delito que suele ser olvidado tanto por las doctrinas justificacionistas como por las abolicionistas. Este otro mal es la mayor reacción – informal, salvaje, espontánea, arbitraria, punitiva pero no penal – que a falta de penas podría devenir de la parte ofendida o de fuerzas sociales o institucionales solidarias con ella. Es el impedir ese mal, del que sería víctima el reo o incluso personas ligadas a él, lo que representa, me parece, el segundo y fundamental fin justificador del derecho penal.

Isso tudo nos remete à possibilidade de enfrentar a banalização do mal absoluto escapando da retórica performativa do chamado populismo punitivo. Como explica Peres-Neto (2010), delitos graves, que sensibilizam a opinião pública pela violência intrínseca aos seus atos, suscitam nos representantes políticos, em jornalistas e opinantes, em juízes e demais operadores do direito, entre outros atores político-institucionais, a tentação de responder à gravidade de casos concretos com discursos simplistas de "mão dura" ou "tolerância zero", que reforçam uma opção equivocada, não garantista e díscola de pa-

râmetros éticos defensáveis. Essa postura populista encontra nos sites de redes sociais digitais ampla acolhida, quer seja pela sua superficialidade, quer seja pela intolerância que pauta grande parte da conduta dos "comentadores" dessa ambiência comunicacional, conhecidos pela alcunha nada alvissareira de "haters". Ademais, como bem descreve García Arán (2009) tais opções retóricas, características do populismo punitivo, não resolvem o problema de fundo, criam outro e favorecem a utilização político eleitoral do Direito Penal como mero instrumento simbólico.

4 À guisa de conclusão

A extensiva e intensiva presença dos meios de comunicação na vida contemporânea altera os modos de ser e de ver-se no mundo. A isso devemos acrescentar o apagamento das fronteiras entre o chamado mundo "on-line" e àquele que seria "off-line". Imersos em uma cultura da virtualidade real, o mundo de dentro ou de fora do universo *cyber* é um só.

De tal sorte parece-nos complicado separar ou circunscrever a intolerância – base dos delitos de ódio e mal absoluto que dá corpo a atos execráveis como o crime de pornografia infantil – como sendo um traço unicamente definidor dos sites de rede social, em particular, ou da internet, em geral. O que se observa nesses espaços é reflexo de grande parte da deterioração ética da sociedade contemporânea. Deterioração que se baseia em grande medida no esvaziamento da dimensão humana do outro.

Recuperando o humanismo e sabendo que não há soluções totalizantes – a despeito da retórica própria das políticas criminais neoconservadoras, como as de "tolerância zero" – advogamos pelo resgate da ética e de um Direito Penal que sejam mínimos. Que escapem do discurso fácil, simplista e intolerante que caracteriza o populismo punitivo. E que ofereçam fundamentos humanos sólidos para combater a banalização do mal absoluto que dá corpo e fundamento à pornografia infantil e aos delitos de ódio. Se há algo que a ética pode fazer em prol de uma sociedade mais justa e que permita a realização de uma vida boa é precisamente oferecer meios para que possamos religar-nos e (re) encantar-nos uns com os outros.

Referências

BARROS FILHO, C.; LOPES, F. T. P.; ISSLER, B. **A comunicação do eu**: ética e solidão. Petrópolis: Vozes, 2005.

BOBBIO, N. **El futuro de la democracia**. México, DF: Fondo de Cultura Económica, 1984.

BECK, U. **La sociedad del riesgo**. Hacia una nueva modernidad. Barcelona: Paidós, 2006.

BRIGGS, A; BURKE, P. **Social History of the Media**: From Gutenberg to the Internet. Nova Iorque: Polity, 2006.

CASTELLS, M. **Communication Power**. Oxford: Oxford University Press, 2009.

CONCHE, M. **Le fondement de la morale**. Paris: PUF, 2003.

CORTINA, A. **Ética mínima**. São Paulo: Martins Fontes, 2009.

GARCÍA ARÁN, M. "El derecho penal simbólico (a propósito del nuevo delito delito de dopaje deportivo y su tratamiento mediático". In: GARCÍA ARÁN, M; BOTELLA, J. **Malas Noticias. Medios de comunicación, política criminal y garantías penales en España**. Valencia: Tirant lo Blanch, 2009.

ESS, C. **Digital Media Ethics**. Cambridge: Polity Press, 2014.

FERRAJOLI, L. **Derecho y razón**. Teoría del garantismo penal. Madri: Trotta, 2006a.

_____. **Garantismo**. Una discusión sobre derecho y democracia. Madri: Trotta, 2006b.

HERMAN, E. S.; CHOMSKY, N. **Manufacturing Consent**: The Political Economy of the Mass Media. Londres: Random House, 2008.

LEVINAS, E. **De otro modo que ser o más allá de la esencia**. Salamanca: Sígueme, 2011.

MALÓN MARCO, A. Pedophilia: a diagnosis in search of a disorder. In: **Archives of Sexual Behavior**, n. 41, 2012.

MITCHELL, K. J.; JONES, L. M.; FINKELHOR, D.; WOLAK, J. "Understanding the decline in unwanted sexual solicitations for U.S. youth 2000-2010: findings from three Youth Internet Safety Surveys". **Child abuse and neglect**, n. 37, 2013.

MORIN, E. **O método 6**. Ética. Porto Alegre: Sulina, 2005.

PASCAL, B. **Pensées**. Paris: Folio France, 2004.

PERES-NETO, L. **Prensa, política criminal y opinión pública**: el populismo punitivo em España. 2010. 535f. Tese (Doctorado en Comunicación y Periodismo) – Departament de Ciència Política i de Dret Públic, Universitat Atònoma de Barcelona, 2010.

_____; BOTELLA, J. **Éticas em rede**. São Paulo: Estação das Letras e Cores, 2016.

PRICE, M. **Free expression, globalism and the new strategic communication**. Nova Iorque: Cambridge University Press, 2015.

PRIMO, A. **Interação mediada por computador**: comunicação, cibercultura, cognição. Porto Alegre: Sulina, 2007.

RAMOS VÁSQUEZ, José Antonio. **Política criminal, cultura y abuso sexual de menores**. Valencia: Tirant lo Blanch, 2016.

SIBILIA, P. **O show do eu**. A intimidade como espetáculo. 2. ed. Rio de Janeiro: Contraponto, 2016.

VERKHOVSKY, A. Criminal law on hate crime, incitement to hatred and hate speech. In: **OSCE participating states**. Haia: SOVA Center, 2016.

WACQUANT, L. **Las cárceles de la miséria**. Madri: Alianza Editorial, 2000.

_____. **Castigar els pobres**: el nou govern de la inseguretat social. Barcelona: Edicions 1984, 2006.

CRIMES CIBERNÉTICOS

10 CRIMES INFORMÁTICOS: COMENTÁRIOS AO PROJETO DE LEI Nº 5.555/2013

André Luiz Pereira Spinieli[1]

Resumo: Com o advento da rede mundial de computadores, é inegável que a pessoa humana perdeu parcialmente sua privacidade, ficando sujeita – apesar dos pontos benéficos, os quais são passíveis de citação a integração cibernética, o armazenamento e a coordenação de dados, bem como a facilitação para realizar determinadas atividades e processos – a riscos de exposição excessiva ou, até mesmo, graves danos à moral. Acontece que, nesse contexto, a internet contribui consideravelmente para o aumento do número de crimes, trazendo à tona os recém-chamados "delitos informáticos", visto que serve como verdadeiro instrumento para a prática delitiva. Em movimento de rechaço à nova modalidade criminosa, além da Lei nº 12.737/2012, alcunhada de "Lei Carolina Dieckmann", em referência à atriz global, encontra-se em trâmite congressual o Projeto de Lei nº 5.555/2013, instituindo nova perspectiva à defesa da mulher contra as infrações cibernéticas. Dessa maneira, o presente artigo busca comentar, brevemente e a partir das disposições já votadas, quais serão as possíveis consequências de eventual aprovação do projeto, bem como a posição atual do Direito, como um todo, no enfrentamento a tal espécie de crime.

Palavras-chave: Direito Penal. Direito Cibernético. Pornografia de vingança. Projeto de Lei.

Abstract: *With the advent of the global computer network, it is undeniable that the human person has partially lost its privacy, being subject – in spite of the beneficial points, which can be cited the cyber integration, data storage and coordination, as well as facilitation to carry out certain activities and processes – to the risk of excessive exposure or even serious damage to morale. In this context, the Internet contributes considerably to the increase in the number of crimes, bringing to light the so-called "computer crimes", since it serves as a true instrument for delinquent practice. In a move to reject the new criminal modality, in addition to Law nº 12.737/2012, nicknamed "Carolina Dieckmann Law", in reference to the global actress, the Bill Law 5.555/2013 is under congressional process, instituting a new perspective to the defense against cybercrime. In this way, this article seeks to comment, briefly and from the provisions already voted, what are the possible consequences of eventual approval of the project, as well as the current position of the Law, as a whole, in facing this kind of crime.*

Keywords: Criminal Law. Cyber Law. Revenge Porn. Bill.

1 É acadêmico de Direito pela Faculdade de Direito de Franca (2014 – 2018), tendo ingressado na qualidade do estagiário do Ministério Público do Estado de São Paulo (Gaeco – Núcleo Franca), com atuação na seara criminal, no ano de 2017. É pesquisador nas áreas de Direito Penal e Criminologia.

1 Introdução

A partir da evolução exacerbada da ciência tecnológica, em que se observam mudanças paradigmáticas que tomam cada vez mais espaço no contexto da sociedade moderna – ou "segunda modernidade", como opta por chamar o sociólogo alemão Ulrich Beck para designar o momento atual, em que a ciência e a técnica se desenvolvem de tal maneira que se torna impossível a predição e o controle dos riscos –, a internet desponta como fator criador de um novo espaço com características próprias, inviolável pelas regras básicas de competência processual penal ou, até mesmo, civil.

E mais. Tornou-se, ainda, local de livre circulação de ideias, um verdadeiro *marketplace of ideas* na concepção dos norte-americanos, e também de insubordinação aos típicos poderes punitivos do Estado.

De fato, a internet e a progressão tecnológica, em especial aquela presente no século XXI, são coeficientes que intervieram de forma direta no aparecimento de novas modalidades de crimes. Tendo em vista tal conjuntura, o Estado, por meio de seus órgãos, passa a ter a responsabilidade de chamar para si o controle punitivo de tais infrações, numa retomada do clássico conceito do *jus puniendi*.

Concomitantemente com a necessidade de uma resposta estatal que atenda às expectativas sociais, reside o fato de que inexiste legislação específica sobre o tema, que forneça elementos contundentes para uma erradicação dos delitos de tal natureza. Porém, é certo dizer que a sobredita responsabilidade de observância das relações cibernéticas pelo Estado teve um primeiro passo após o espalhafatoso acontecimento que vitimou a atriz global Carolina Dieckmann no ano de 2012 e, por conseguinte, fundamentou a Lei nº 12.373, de 30 de novembro daquele ano.

Ainda, entre os vários crimes passíveis de acontecimento em ambiente cibernético, insta citar que alguns decorrem de práticas que o próprio Direito Penal coíbe, desde sua gênese. Exemplo disso são os crimes contra a honra nas suas três espécies: calúnia, difamação e injúria. Além disso, não raras vezes se noticiam práticas de injúria racial ou pornografia infantil.

Visando acrescentar ao ordenamento jurídico mais um instrumento de combate às práticas delitivas em âmbito *on-line*, desde o ano de 2013, segue em tramitação no Con-

gresso Nacional o Projeto de Lei nº 5.555/2013, que institui entre as formas de violência contra a mulher, previstas na Lei Maria da Penha (Lei nº 11.340/2006), a divulgação de vídeos e fotos íntimas na internet, sem a devida permissão daquela que é exposta.

Nesse ínterim, o presente artigo objetiva trazer à baila os novíssimos conceitos de "crimes informáticos", bem como quais são os objetos jurídicos tutelados nesses delitos e como se mostram os primeiros passos do que pode vir a ser uma nova tipificação no Direito Penal, comparando-a com as infrações já existentes na seara repressiva brasileira, principalmente no que diz respeito às condutas previstas na Lei nº 8.069/1990, o Estatuto da Criança e do Adolescente.

2 Dos Crimes Informáticos

2.1 Adequação Terminológica

Muito se discute em sede doutrinária qual seria a terminologia mais adequada para se referir aos crimes que ocorrem no espaço virtual, ou seja, se o mais correto seria "delito cibernético", "delito eletrônico", "delito digital" ou "delito informático"[2].

Apesar de não haver um consenso entre aqueles que escrevem acerca do tema, ou, nem mesmo, na jurisprudência dos tribunais superiores, o Brasil conta, nos dias de hoje, com o Instituto Brasileiro de Direito Eletrônico (IBDE)[3], cuja posição é no sentido de que a melhor nomenclatura seria "crime eletrônico".

Augusto Eduardo de Souza Rossini, que escreve com propriedade sobre o assunto, assevera que a melhor denominação é aquela que leva o termo "informático" em sua composição, como demonstra:

> Ouso denominá-los "delitos informáticos", pois dessa singela maneira abarcam-se não somente aquelas condutas praticadas no âmbito da in-

2 Explicita-se, desde já, que aqui se adota, para a escrita do presente artigo, a terminologia "informático", vinculando as expressões referentes aos crimes e ao próprio ramo do Direito que regula as relações estabelecidas por meio da rede mundial de computadores. A princípio, essa terminologia parece ser a preferida da doutrina e da jurisprudência.

3 O Instituto Brasileiro de Direito Eletrônico é uma importante rede de profissionais, cujo objetivo comum é desenvolver a interdisciplinaridade no que toca aos temas específicos sobre internet e mundo virtual. Entre seus trabalhos, muitas vezes desenvolvidos com parceiros, como a ONG Marias da Internet, está uma capacitação de profissionais para serem referência no atendimento às vítimas da chamada "pornografia de vingança" ou *porn revenge*. Disponível em: <http://ibde.org.br/>. Acesso em: dez. 2017.

> ternet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível "conexão" à Rede Mundial de Computadores (ROSSINI, 2002).

Quer dizer que, conforme interpretação majoritária na doutrina jurídica penal moderna, delitos informáticos seriam gênero, do qual o delito cibernético – como explicita o sobredito autor, este se refere tão somente aos crimes realizados especificamente no âmbito da internet, cabendo também a expressão "delito telemático" – é espécie.

Não só no Brasil, mas também no exterior, essa tende a ser a opção mais acatada pelos respectivos ordenamentos jurídicos. Informa o doutrinador Aldemario Araújo Castro que outros países também utilizam a denominação "direito informático"[4] para fazer referências aos problemas de ordem civil e criminal que cercam a vida na web. Deveras, nos países francófonos é chamado de *Droit de L'informatique*; naqueles de língua espanhola, de *Derecho de Informatica*; *Diritto dell'Informatica* para os italianos; e, para os ingleses e norte-americanos, *Computer Law* ou *Cyber Law* (ALMEIDA FILHO, 2005).

Nesse sentido, importante a reflexão trazida à tona por Mário Antônio Lobato de Paiva, em artigo sobre o tema[5], considerando que o ramo jurídico denominado "direito informático" nada mais é senão o

> [...] conjunto de normas e instituições jurídicas que pretendem regular aquele uso dos sistemas de computador – como meio e como fim – que podem incidir nos bens jurídicos dos membros da sociedade; as relações derivadas da criação, uso, modificação, alteração e reprodução do *software*; o comércio eletrônico, e as relações humanas realizadas de maneira *sui generis* nas redes, em redes ou via *internet* (PAIVA, 2003).

Cumpre salientar, finalmente, a existência de certa divergência entre autores no que diz respeito ao reconhecimento do Direito Informático como ramo jurídico autônomo, o

4 Conforme a melhor doutrina, distingue-se também "direito informático" de "informática jurídica", uma vez que esta tem o Direito como instrumento e o ordena, sistematizando-o e organizando suas informações, ao passo que o primeiro faz expressa referência à atividade da informática como objeto de estudo jurídico, isto é, análise das relações que ocorrem por meio da informática, regulamentando e solucionando conflitos. BARBAGALO, Érica Brandini. **Contratos Eletrônicos**. São Paulo: Saraiva, 2001. p. 39.

5 Afirma o autor que o Direito Informático não se dedica tão somente ao estudo dos aparelhos de informática como meios auxiliares ao Direito, mas sim "constitui o conjunto de normas, aplicações, processos, relações jurídicas que surgem como consequência da aplicação e desenvolvimento da informática...". PAIVA, Mário Antônio Lobato de. Os institutos do Direito Informático. **Âmbito Jurídico**, Rio Grande, VI, n. 14, ago 2003. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/%3C?n_link=revista_artigos_leitura& artigo_id=5487&revista_caderno=17>. Acesso em: out. 2017.

que ocasionou a formação de duas correntes bem delimitadas, tema este que sobrevive com aceitações e restrições de ambos os lados da doutrina.

Num primeiro ponto, os partidários do tradicionalismo negam sua existência em separado, enquanto outros da mesma corrente entendem que as novas práticas – de caráter penal, consumerista, civil, empresarial etc. – no âmbito da internet representam um meio e, por esse motivo, são meros reflexos de condutas antes reguladas.

Para a segunda corrente, porém, é indiscutível a necessidade de organizar legislativamente a atividade informática, que hoje tanto carece de proteção específica. Além disso, sustentam que o Direito Penal do século XIX restringe-se, em sua maioria, aos bens jurídicos advindos da primeira e da segunda geração de direitos fundamentais, isto é, aqueles relativos à liberdade e à igualdade.

2.2 Conceito de Delito Informático

É de grande importância frisar desde logo que também não há um conceito unívoco do que vem a ser delito informático, repetindo a discordância que ocorre com o ramo maior, que é o direito informático. Com base nas lições do festejado pesquisador Augusto Eduardo de Souza Rossini, há quem chame de "criminalidade do computador", "criminalidade da informática", "delitos cibernéticos", além dos já citados vocábulos.

Como é cediço, desde a década de 1980, o professor alemão Klaus Tiedemann fazia referência a um conceito de crime informático, relatando que se tratava de alusão a todos os comportamentos ilegais de acordo com a legislação vigente ou que eram socialmente prejudiciais, desde que praticados com o emprego de um equipamento automático de processamento de dados. Logo, o conceito, na concepção do professor germânico, abrange o problema da ameaça à esfera privada do cidadão mediante a acumulação, associação, arquivamento e, principalmente, divulgação irrestrita de dados por meio de computadores[6] (TIEDEMANN, 1985).

6 Con la expresión "criminalidad mediante computadoras" se alude a todos los comportamientos antijurídicos según la ley vigente (o socialmente perjudiciales y por eso punibles en el futuro) realizados merced al empleo de un equipo automático de procesamiento de datos. Dicho concepto, pues, abarca, por una parte, el problema de la amenaza a la esfera privada del ciudadano mediante la acumulación, archivo, asociación y divulgación de datos mediante computadoras; de hecho, sin embargo, hasta el momento en Alemania Federal solo se han conocido poços casos de violación de derechos personalisimos em razón del aprovechamiento abusivo de datos conservados em una computadora. TIEDEMANN, Klaus. Criminalidad **Mediante Computadoras**. Disponível em: <http://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/download/4315/3569/>. Acesso em: dez. 2017.

A *criminalidad mediante computadoras*, como opta por nomear o referido autor, em muito se relaciona com os problemas enfrentados pelo indivíduo em sua esfera privada, que, de certo modo, acaba ameaçada ou lesionada pela memorização, interconexão e transmissão informática de dados, bem como se relaciona com os atentados ao patrimônio cometidos por meio de sistemas informáticos.

Nas palavras do celebrado Tiedemann em seu ensaio intitulado *Poder Económico y Delito*, os crimes informáticos nada mais são senão

> [...] todos los actos, antijurídicos, según la ley penal vigente (o social perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos (TIEDEMANN, 1985).

Isso ratifica a ideia de que, enquanto outrora deveríamos falar no uso de computadores como privilégio reservado a poucos indivíduos da sociedade pré-moderna, hoje já se fala em novas modalidades de ilícitos penais, que contam com a utilização dos meios cibernéticos e eletrônicos para a prática de crimes já conhecidos da sociedade, desde a gênese das legislações compiladas na forma escrita, a positivação da norma.

Com o crescimento exacerbado do número de internautas, a rede mundial de computadores sofreu avassaladora invasão de crimes praticados por meio da rede, que cresceram em proporções catastróficas.

Nesse sentido, já se pronunciou a professora Ivete Senise Ferreira:

> A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução (FERREIRA, 2000).

É inegável o prejuízo que pode ser provocado por esse tipo de ferramenta, sendo possível, de uma determinada localidade, acessar um sistema de computadores situado do outro lado do mundo e manipular seus dados, tornando-se crimes "limpos", que não deixam quaisquer rastros (ROSA, 2005). Por isso, é certo que, pela juventude da matéria,

resta imensa discussão até mesmo no âmbito de sua conceituação, como visto, de quais seriam os alcances e limites da norma própria de Direito Informático.

De qualquer maneira, o Direito Informático decorre daquelas previsões legais já existentes no ordenamento jurídico, seja da legislação comum ou esparsa. A esse respeito, a doutrinadora Patrícia Peck Pinheiro explicita que "o Direito Digital [...] tem sua guarida na maioria dos princípios do Direito atual, além de aproveitar a maior parte da legislação em vigor" (PINHEIRO, 2009).

Sendo assim, a par das diversas definições já fornecidas no corpo do presente texto[7] e, independentemente dos muitos esforços erigidos na doutrina, parece-nos que a definição mais acertada, levando em consideração o objeto material e os meios de atuação dos crimes informáticos, é aquela fornecida pela Organização para a Cooperação Econômica e Desenvolvimento (OCDE) da ONU, segundo a qual o "crime de informática, ou *computer crime*, é qualquer conduta ilegal não ética, ou não autorizada que envolva processamento automático de dados e/ou transmissão de dados" (FERREIRA, 1992).

Qualquer que seja a definição adotada, fato é que a legislação ainda é bastante precária em termos de normas criminais que assegurem melhor proteção ao internauta durante sua navegação na internet[8]. Exemplo que bem demonstra um primeiro passo rumo a uma legislação mais rigorosa foi a promulgação da Lei nº 12.737, de 2012, que age sob a alcunha de "Lei Carolina Dieckmann".

A partir desse antecedente legal, o legislador brasileiro procurou punir quem invadisse dispositivo informático sem a devida autorização do proprietário, constituindo juridicamente a figura do conhecido *hacker*[9], seguindo uma novidade que outros países têm seguido, que, a propósito, bem explicita Augusto Eduardo de Souza Rossini:

> Contudo, os últimos episódios no mundo – "Setembro Negro", sistemática invasão de *hackers* e *crackers* a grandes computadores de empresas, disseminação de pedofilia etc. –, fizeram com que a crença na autorregula-

7 Em apertada síntese, os delitos de informática são todas as condutas típicas, antijurídicas e culpáveis, e, da mesma forma, antiéticas e não autorizadas, que utilizem meios automáticos de processamento e/ou transmissão de dados para serem cometidos.

8 O professor Tiedemann assevera que "...el legislador alemán, en la 'Ley Federal de Protección de Datos', reforzó la regulación con normas penales poco precisas." TIEDEMANN, Klaus. **Criminalidad Mediante Computadoras**. Disponível em: <http://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/download/4315/3569/>. Acesso em: dez. 2017.

9 Conforme o professor Henrique César Ulbrich, *hacker* é uma pessoa que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes para lidar com um computador. Ele sabe que nenhum sistema é completamente livre de falhas e sabe onde procurar por elas, utilizando-se de técnicas das mais variadas, acrescentando que o *hacker* é usualmente visto como um criminoso. Porém, quem realmente utiliza suas habilidades para o mal é o chamado *cracker*.

> mentação caísse por terra, de forma que o ramo do Direito chamado de *ultima ratio* não outro senão o Direito Penal, fosse instado a interferir. O fato é que o Estado teve que dirigir seus olhos para esse problema a fim de garantir a proteção a bens jurídicos preciosos para a sociedade (ROSSINI, 2002).

Foi justamente a partir do grande levante de invasões aos computadores mundiais que trouxe para o Estado a responsabilidade única de vigiar e, ao mesmo tempo, garantir a proteção dos bens jurídicos relevantes para o meio social que se encontrava em risco, além de punir aquele que transgredisse tais valores. De imediato, a preocupação se instalou nos Estados Unidos e, em seguida, alastrou-se para todo o mundo, de maneira uniforme. A internet é, desde muito tempo, uma realidade nos mais diversos países do globo terrestre e, indiscutivelmente, em todos são cometidos delitos informáticos.

A experiência brasileira, como já ressaltada, apresentava grave lacuna normativa que impedia a punição pela invasão a computadores. Porém, como explicita Cléber Masson em seu compêndio, "a legislação penal brasileira sempre possuiu arsenal para combater a imensa maioria dos crimes eletrônicos, algo em torno de 95%" (MASSON, 2015).

Deveras, há que se reconhecer a verdade nas falas do doutrinador. Por meio dos tipos penais previstos no Código Penal e em leis esparsas, era possível punir a criminalidade informática, adequando as normas às condutas perpetradas no âmbito do mundo virtual. Apenas a título exemplificativo, quem ofendesse a honra alheia incidiria nos crimes contra a honra; quem praticasse intimidações, recairia sobre o crime de ameaça; quem espalhasse vírus para inutilizar equipamentos seria responsabilizado pelo crime de dano, e assim por conseguinte.

Em resposta ao vácuo normativo e ao alargamento dos citados tipos penais a dimensões que chegavam a ser forçosas demais, computou-se aos demais crimes arrolados no Estatuto Repressivo o delito nomeado de "invasão a dispositivo informático alheio", cujos requisitos básicos são a necessidade de uma proteção – senha ou qualquer outro meio assecuratório – no aparelho e a carência de autorização do dono daquele objeto invadido, numa espécie de "ausência do consentimento do ofendido".

O delito, também conhecido como "intrusão virtual", está tipificado e enumerado no artigo 154-A do Código Penal, cuja redação de sua modalidade fundamental, *ipsis litteris*, é a seguinte:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computador, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagens ilícitas.
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

Numa breve análise do tipo em comento, o objeto jurídico penalmente tutelado, não se tem dúvidas, é a liberdade individual no que é pertinente com a inviolabilidade dos sigilos. A conduta invasora recai sobre o dispositivo informático alheio, que figura como objeto material, esteja ele conectado ou não à internet. O núcleo típico é o verbo "invadir", que significa, em apertada conceituação, ocupar determinado lugar[10] à força. Qualquer pessoa pode titularizar o polo ativo do crime, bem como pode ser qualquer um a vítima, desde que tenha um dispositivo informático, que pode ser celulares, câmeras, CDs, DVDs e computadores.

Entre diversas hipóteses de aumento de pena, o Brasil contemplou o seu primeiro tipo penal específico contra as problemáticas criminais do ambiente virtual. Entretanto, ainda não é e tampouco será o suficiente para erradicar tais práticas, como se verá.

2.3 A Questão dos Bens Jurídicos nos Crimes Informáticos

O objeto ou bem jurídico que é tutelado pela normal penal – representado nos dizeres do clássico penalista Francisco de Assis Toledo como todos os objetos materiais ou imateriais que são protegidos pelo Estado[11] – é todo valor ético-social que o direito seleciona, com o objetivo de assegurar a paz social, colocando-o sob sua proteção para que não seja exposto a perigo de ataque ou lesões efetivas (TOLEDO, 1994).

10 Apesar do substantivo "lugar" soar estranho, num primeiro momento, aos ouvidos daqueles que entendem cabível apenas quando se trata de local físico, situação que não se enquadra à internet, há que se lembrar de que alguns doutrinadores compreendem que o meio cibernético constitui não só um local de troca de informações, mas também uma nova modalidade de meio ambiente. Nessa esteira, Celso Antônio Pacheco Fiorillo, com fulcro no art. 215 da Constituição Federal, trata do meio ambiente digital como integrante do meio ambiente cultural, pois "todo bem referente à nossa cultura, identidade, memória etc., uma vez reconhecido como patrimônio cultural, integra a categoria de bem ambiental e, em decorrência, difuso". FIORILLO, Celso Antônio Pacheco. **Tutela jurídica do meio ambiente cultural como patrimônio normativo da denominada sociedade da informação no Brasil**. Disponível em: <https://www.cidp.pt/publicacoes/revistas/ridb/2012/10/2012_10_5959_5989.pdf>. Acesso em: dez. 2017.

11 "*Bem*, em um sentido muito amplo, é tudo o que se nos apresenta como digno, útil, necessário, valioso. É tudo aquilo 'que'est objet de satisfaction ou d'approbation dans n'importe quel ordre de finalité: parfait em son genre, favorable, réussi, utile à quelque fin...' [...] isto é, coisas materiais e objetos imateriais que, além de serem o que são, 'valem'. Por isso são, em geral, apetecidos, procurados, disputados, defendidos, e, pela mesma razão, expostos a certos perigos de ataques ou sujeitos a determinadas lesões." TOLEDO, Francisco de Assis. **Princípios básicos de Direito Penal**. 5. ed. São Paulo: Saraiva, 1994. p. 15.

Fernando de Almeida Pedroso fixa importante noção de objeto jurídico[12]:

> Bem representa tudo quanto satisfaça uma necessidade humana ou do agrupamento, despertando um interesse individual ou coletivo a ele endereçado. Quando esse bem interessa igualmente ao mundo do Direito, que o regulamenta e disciplina por meio de suas prescrições legais, recebe a denominação de bem jurídico. Se esta disciplina legal é, porém, feita a título de proteção, preservação e garantia do bem e é procedida dentro do ordenamento jurídico do Direito Penal, surge a figura do bem jurídico penalmente tutelado (PEDROSO, 2008).

O conceito de bem jurídico, além de se encontrar umbilicalmente relacionado à ofensividade da conduta, foi objeto de lenta progressão na história penal. A princípio, buscava-se um conteúdo material na lesão ou exposição a perigo de direitos subjetivos; após, na lesão ou exposição a perigo de interesses vitais para a sociedade; e, por fim, a lesão ou exposição de um bem jurídico (TOLEDO, 1994).

No tocante aos delitos informáticos, a problemática dos bens jurídicos tutelados se acirra na medida em que a melhor doutrina orienta-nos a relacioná-los com a natureza que é imposta ao respectivo delito. Num primeiro momento, admitindo se tratar de infração mista[13], a tutela continua recaindo sobre os bens jurídicos protegidos em crimes comuns, por exemplo, a honra na injúria e o patrimônio no furto e no estelionato. Porém, considerando-se tratar de infração pura[14], serão os mesmos, pois tais condutas não deixam de caracterizar o dano informático.

Acontece que, independentemente da classificação adotada, o bem jurídico permanente é a segurança informática, que existirá apesar da individualidade ou coletividade dos bens jurídicos. Hoje, a opção da *communis opinium doctorum* nos mostra que a me-

12 Há três teorias que buscam conceituar e justificar a existência dos bens jurídicos: a primeira, monista personalista, volta-se à defesa da pessoa, motivo pelo qual são os bens jurídicos individuais que estão protegidos pelo Direito Penal; a segunda, monista coletiva, garante a tutela penal aos interesses metaindividuais ou difusos; e a terceira, dualista, admite ambas as espécies de bens jurídicos, tanto os individuais quanto os coletivos, sendo a proteção deles de modo autônomo, conforme a necessidade em cada esfera de proteção. CUNHA, Rogério Sanches. **Manual de Direito Penal**: parte geral (arts. 1º ao 120). 4. ed. Bahia: JusPODIVM, 2017. p. 162-163.

13 Delitos informáticos mistos são aqueles "em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático". ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. **Caderno Jurídico**, Ano 2, n. 4, p. 139. jul. 2002.

14 Crimes informáticos puros, segundo a opinião de Augusto Eduardo de Souza Rossini, são "aqueles em que o sujeito visa especificamente ao sistema de informática em todas as suas formas, sendo que a informática é composta principalmente do *software*, do *hardware* (computador e periféricos), dos dados e sistemas e dos meios de armazenamento. A conduta (ou ausência dela) visa exclusivamente ao sistema informático do sujeito passivo". ROSSINI, Augusto Eduardo de Souza, *op. cit.*, p. 138.

lhor saída é entender os delitos de tal calibre como protetores de bem jurídico-penal de natureza difusa.

A esse respeito, escreve Gianpaolo Poggio Smanio, para quem

> os bens jurídico-penais de natureza difusa, que também se referem à sociedade em sua totalidade, de forma que os indivíduos não têm disponibilidade sem afetar a coletividade. Ocorre que os bens de natureza difusa trazem uma conflituosidade social que contrapõe diversos grupos dentro da sociedade [...] (SMANIO, 2000).

Portanto, em suma, os bens jurídicos tutelados pela norma penal quando da ocorrência de crimes informáticos são aqueles de natureza difusa, que alcançam toda a coletividade, sem especificar os sujeitos lesionados pela prática delitiva.

3 Do Projeto de Lei nº 5.555/2013

3.1 Antecedente Legislativo: Lei Carolina Dieckmann

No ano de 2012, cinco homens, inicialmente desconhecidos, mas posteriormente identificados e responsabilizados penalmente, invadiram o computador pessoal da atriz global e também modelo Carolina Dieckmann e subtraíram diversas fotografias íntimas, nas quais a vítima aparecia nua, passaram a extorqui-la, solicitando dinheiro em troca da não divulgação das imagens na internet. Os invasores informáticos foram punidos pelos delitos de furto, extorsão e difamação, mas de maneira alguma por algum crime relacionado à invasão de computadores.

Desde o ano anterior ao dos fatos, já se encontrava em discussão no Congresso Nacional o Projeto de Lei nº 2.793, apresentado pelo parlamentar Paulo Teixeira (PT/SP). Acontece que, em virtude dos acontecimentos, o projeto tramitou em regime de urgência e, em tempo recordista, foi promulgada a lei que, antes mesmo de publicada e sancionada, já era apelidada de "Lei Carolina Dieckmann", em razão da repercussão de sua experiência com os crackers que haviam subtraído suas imagens.

Diga-se de passagem, a lei, desde sua promulgação, sofre duras críticas por parte da doutrina jurídica e de profissionais que atuam no campo da segurança da informação,

uma vez que seus dispositivos são amplos o bastante para gerar dubiedade e interpretações subjetivas, o que pode ser utilizado contra a vítima numa suposta defesa de um acusado por crime informático, o que tornaria a lei ineficaz[15]. Junte-se a isso o fato de que a novel lei, em termos de crime informático puro, apenas acrescentou o aludido art. 154-A do Código Penal, que não pune a distribuição de imagens que desabonem a vítima.

Isso porque os crimes informáticos são verdadeiras "portas de entrada" para outras condutas criminosas, facilmente praticadas após a corrupção do computador e sua utilização como instrumento para o cometimento de crimes. Outrossim, é bastante criticável o fato de que o legislador não foi longe o suficiente para contemplar a invasão de sistemas por meio de novos métodos, como o *clouding computing*[16].

Muito além das imperfeições redacionais dos tipos penais, as penas são irrisórias se levada em consideração a especial gravidade de que se revestem tais crimes, de tal maneira que a Lei nº 12.737/2012 – embora avançada pelo acontecimento com Carolina Dieckmann – sequer pune aquilo que a vitimou e não consegue dar respostas satisfatórias à sociedade e àqueles que se servem das facilidades tecnológicas para o crime.

3.2 Conteúdo do Projeto de Lei

Em trâmite legislativo desde o ano de 2013, oriundo de proposta do deputado João Arruda, do PMDB/PR, o Projeto de Lei nº 5.555/2013 – que no estado atual já se encontra com substitutivo legislativo e em votação perante o Senado Federal, após aprovação na Câmara dos Deputados – visa incluir a comunicação no rol de direitos assegurados à mulher por intermédio da Lei Maria da Penha, além de reconhecer que a violação de sua intimidade nada mais é senão uma das várias formas de violência doméstica e familiar, notadamente na modalidade "pornografia de vingança" ou *revenge porn*. Ainda, subsidiariamente, o projeto alterará o Código Penal a fim de fazer constar em seu rol de condutas delitivas o crime de "exposição pública da intimidade sexual".

Nota-se que a proposta tem como fito dar uma proteção superior à mulher, levando-se em consideração as várias formas de violência a que está exposta. Na ocasião,

15 A posição doutrinária que é contra a tipificação de delitos informáticos sustenta que as penas não cumprem seu papel de intimidação, visto que são baixas e muitas vezes podem ficar apenas no âmbito dos Juizados Especiais, cujas consequências são as possibilidades de investigações simplórias e céleres, além da incidência dos chamados "institutos despenalizadores" da transação penal e suspensão condicional do processo, gerando pouco ou nenhum combate efetivo ao crime informático no Brasil.

16 Refere-se à "computação em nuvem", em que há utilização da capacidade de armazenamento por meio de servidores compartilhados e interligados por meio da internet.

caso o projeto seja finalmente aprovado, acrescentará um novo inciso ao art. 7º da Lei nº 11.340/2006, dando a necessária proteção aos direitos de comunicação[17].

Pela eventual lei nova haverá agregação de um novo inciso no citado artigo, passando a vigorar com o seguinte texto:

> Art. 7º São formas de violência doméstica e familiar contra a mulher, entre outras:
> VI – violação de sua intimidade, entendida como a divulgação por meio da Internet ou em qualquer outro meio de propagação da informação, sem o seu expresso consentimento, de imagens, informações, dados pessoais, vídeos, áudios, montagens ou fotocomposições da mulher, obtidos no âmbito de relações domésticas, de coabitação ou de hospitalidade (BRASIL, 2013).

Não obstante, fato notório é a expansão da odiosa prática de violação da intimidade de diversas mulheres por intermédio da rede mundial de computadores, com a divulgação não autorizada de imagens, áudios, dados e informações pessoais, que a ela pertencem, motivo que bastou para o nascimento do citado projeto com o propósito de engrandecer a lista de formas de violência doméstica e familiar contra a mulher.

Sabe-se que isso abre espaço para a chamada "pornografia de vingança", também conhecida por *revenge porn*, que pode ser conceituada como uma das várias formas de violência moral, mas somada ao objeto sexual, pela qual alguém publica em redes virtuais e distribui por meio de outros aparelhos conectados à rede, sem o consentimento da vítima, fotos ou vídeos de conteúdo sexual explícito ou com nudez.

O ponto preocupante é que os supracitados atos criminosos são, na maior parte das vezes, praticados por cônjuges, companheiros e até mesmo ex-cônjuges, que se valem da posição de superioridade no contexto da coabitação ou da hospitalidade para conquistar os aludidos dados e, logo em seguida, lançá-los na rede a fim de causar constrangimento inestimável à vítima[18].

17 Conforme parecer exarado pela Comissão de Cidadania de Justiça (CCJ) da Câmara dos Deputados, assinado pela deputada Laura Carneiro, do PMDB-RJ, relatora do caso, "apesar da enumeração de grande parte dos bens jurídicos protegidos pela Constituição Federal, é importante frisar que a inclusão do direito à comunicação no aludido rol é medida que se mostra de rigor, haja vista que tem o condão de materializar todos os demais direitos das mulheres". Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra; jsessionid=F1EA5733FF70F9F9E56FFA204D964AAB.proposicoesWebExterno2?codteor=1527228&filename=Parecer-CCJC-21-02-2017>. Acesso em: dez. 2017.

18 Explica a Defensora Pública, Dulcielly Nóbrega, em entrevista concedida à ONG Compromisso e Atitude, que "[...] o relacionamento era mantido na base da confiança. Mas em uma cultura profundamente machista, os homens pensam que as mulheres são

Tecendo importante crítica à "pornografia de vingança", no sentido de que o discurso que prega que "caso não queira ter a intimidade violada, não registre a sua intimidade" constitui flagrante óbice ao livre exercício da sexualidade pelas mulheres, Mariana Giorgetti Valente, Natália Neliz, Juliana Pacetta Ruiz e Lucas Bulgarelli escrevem:

> Para além dos danos físicos e psicológicos causados pela ameaça, o perigo do ataque sexual passa a operar como uma lembrança do privilégio masculino, com o intuito de restringir o comportamento das mulheres. É isso que engendraria o discurso do *better safe than sorry* (melhor prevenir que remediar), e a vivência dos impulsos sexuais femininos como perigo: se os homens são vistos como desejantes, agressivos, impetuosos, cabe à mulher, nessas representações dominantes, o papel de custodiar o comportamento masculino, não lhe provocando desejos (VALENTE et al., 2016).

Ademais, frise-se que a realização de tal modalidade de violência contra a mulher no âmbito da internet possui elevada capacidade lesiva, uma vez que expõe a intimidade dela num espaço habitado por um número indeterminado de pessoas[19], revelando, como dito anteriormente, a natureza difusa dos crimes informáticos. Nesse sentido, fica evidente que a promulgação da nova e possivelmente vindoura lei tem por finalidade a proteção da dignidade sexual da mulher, notadamente no que toca à respeitabilidade sexual e da honra que ela desfruta perante o meio social em que vive.

A aprovação do projeto pela Câmara dos Deputados e, na esperança de votação favorável também no Senado Federal, veio em bom tempo. Sabe-se que as normas penais existentes já não são suficientes para conter tais avanços sociais, ainda que criminosos. Igualmente, a velocidade com que informações desse tipo são compartilhadas revelam o potencial danoso da internet e faz com que lesões irreversíveis à dignidade e à honra de quem sofre um ataque de pornografia vingativa sejam causadas, não restando qualquer alternativa ao Direito senão renovar o conteúdo legislativo acerca do tema.

sua propriedade e não aceitam o fim do relacionamento. É uma objetificação do corpo da mulher.". Disponível em: <http://www.compromissoeatitude.org.br/podeparar-mulheres-sao-principal-alvo -da-pornografia-de-vinganca/>. Acesso em: fev. 2017.

19 Em pesquisa realizada pela instituição SaferNet – organização de defesa dos direitos humanos na internet – constatou-se que, em 2016, cerca de 224 internautas procuraram o serviço virtual da organização para relatar acontecimentos que caracterizam a pornografia de vingança. Além disso, é manifesto que o fato atinge principalmente mulheres, que representam 81% dos casos denunciados, sendo, a cada quatro vítimas, uma criança ou adolescente. Disponível em: <http://www.huffpostbrasil.com/2015/07/06/revenge-porn-dados_n_7734660. html>. Acesso em fev. 2017.

3.3 Legislação Correlata

Até a década de 1990, a violência física (*vis absoluta*) ou moral (*vis compulsiva*) recebia tratamento penal único, pois, independentemente do tipo de conduta, sempre recaía nas disposições clássicas do Código Penal ou da Lei de Contravenções Penais (Decreto-Lei nº 3.688/1941), representando as modalidades de vias de fato, lesão corporal leve, grave ou gravíssima, e, na maior das hipóteses, homicídio.

A partir de então, a legislação, baseada em diversos estudos que demonstravam a falha do Código Penal em coibir toda forma de violência, começou a se especializar. Exemplo disso é a promulgação da Lei nº 8.069/1990, nomeada de Estatuto da Criança e do Adolescente, que criminaliza condutas de tratamento degradante ao menor.

No que diz respeito aos delitos contra a criança e o adolescente, o Estatuto traz tipos penais que em muito se aproximam daqueles objetivados pela promulgação do Projeto de Lei nº 5.555/2013. A título exemplificativo, cumpre aqui arrolar as condutas que se encontram presentes nos artigos 240 ao 241-D, que tipifica e pune as ações relacionadas à pornografia, sexo explícito ou exploração sexual de criança ou adolescentes.

Para fazer um paralelo do que pode vir a ser a nova tipificação oriunda do projeto em discussão, ainda que de forma superficial e meramente comparativa, atentemo-nos ao artigo 241-A, cuja redação é

> 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.

Os diversos núcleos do tipo, quais sejam, oferecer, trocar, disponibilizar, transmitir, distribuir, publicar e divulgar, seriam muito bem adequados à prática de *revenge porn* que antes foi descrita. Ousa-se dizer que o único diferencial aparente seria mesmo o sujeito passivo, que em um são apenas as crianças e/ou adolescente, e no outro seriam todos os absolutamente capazes, maiores de dezoito anos.

Dessa maneira, desde meados do ano de 2008, época em que sobreveio lei alteradora do Estatuto, o Brasil tem caminhado rumo a uma tipificação das práticas vingativas que envolvam pornografia, até porque se trata de delito muitas vezes praticado por via da

internet ou de outros meios eletrônicos, cuja única diferença está cravada nos sujeitos do delito.

4 Considerações Finais

Se de um lado a modernidade, marcada pelo uso em comum da internet e pelo início da era *homo digitalis*, trouxe elementos facilitadores ao desenvolvimento social, por outro também criou amplos desafios daqueles que têm por objetivo e função primordial a manutenção dos direitos e da paz social. O enfrentamento e a punibilidade dos chamados crimes informáticos – cometidos essencialmente por meio da internet ou de dispositivos eletrônicos vindos até a sociedade moderna, graças à evolução tecnológica – ainda representam grandes problemáticas ao Direito, que, em muito, encontra-se preso aos bens jurídicos edificados a partir das antigas revoluções.

O ordenamento jurídico brasileiro, apesar de carente de normas específicas sobre o tema, desde muito punia tais crimes praticados por meios virtuais de forma análoga aos tipos penais previstos no Código Penal ou nas legislações esparsas.

Porém, o momento presente não é mais o mesmo.

A criminalidade virtual tem sofrido imensurável crescimento, nos quais as condutas passam a ser dotadas de alta lesividade, com características típicas de crime plurilocal – isto é, realizado longe do local onde se dá o evento – e com delinquentes pertencentes ao ramo informático, o que dificulta demasiadamente a captura deles.

Justamente nesse contexto é que foi promulgada a batizada "Lei Carolina Dieckmann", criadora de modalidade de crime informático puro no ordenamento jurídico brasileiro, situação nunca antes vista no cenário brasileiro. Não obstante o fato de que a entrada em vigor de novas leis, regulamentando a situação jurídica nos meios virtuais, deu importantes subsídios para solucionar os impasses criados pelos delitos informáticos, ainda deficientes em vários pontos, especialmente por não preverem qualquer forma de violência moral praticada com o auxílio dos meios cibernéticos.

E quem mais sofre com essa modalidade de violência são as mulheres, que acabam vitimadas por seus companheiros e friamente expostas no mundo virtual, sem qualquer tipo de autorização, originando o fenômeno criminológico conhecido por "pornografia de vingança", e sequer podem recorrer às vias judiciais, visto que há um enorme vácuo legislativo, pois a temática não foi abordada por qualquer política.

Por isso, ao modificar a Lei Maria da Penha e acrescentar um novo delito ao Código Penal, o Projeto de Lei nº 5.555/2013 – hoje em trâmite perante o Senado Federal, aguardando votação – mostra-se essencial para assegurar às pessoas, em especial às mulheres, maior proteção no âmbito da moral subjetiva e no ambiente familiar, erradicando cada vez mais a violência doméstica.

A proposta tende a acrescentar valores indispensáveis à comunidade brasileira, que procura incessantemente instrumentos capazes de combater a criminalidade dos tempos modernos, sobretudo no que se refere aos direitos de dignidade das mulheres, além de incluir o direito à comunicação como condição fundamental para o nivelamento dos direitos femininos no Brasil.

Referências

ALMEIDA FILHO, José Carlos de Araújo. Direito Eletrônico ou Direito da Informática? **Informática Pública**, v. 7, 2005. Disponível em: <http://www.ip.pbh.gov.br/ANO7_N2_PDF/IP7N2_almeida.pdf>.

BARBAGALO, Érica Brandini. **Contratos Eletrônicos**. São Paulo: Saraiva, 2001. p. 39.

BRASIL. **Projeto de Lei nº 5.555, de 2013**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A1BA2446F9641AE675CD91B6C2FDE9D1.proposicoesWebExterno2?codteor=1528795&filename=REDACAO+FINAL+-+PL+5555/2013>.

CUNHA, Rogério Sanches. **Manual de Direito Penal**: parte geral (arts. 1º ao 120). 4. ed. Bahia: JusPODIVM, 2017.

FERREIRA, Ivete Senise. A criminalidade informática. In: De LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito e Internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

FIORILLO, Celso Antônio Pacheco. **Tutela jurídica do meio ambiente cultural como patrimônio normativo da denominada sociedade da informação no Brasil**. Disponível em: <https://www.cidp.pt/publicacoes/ revistas/ridb/2012/10/2012_10_5959_5989.pdf>. Acesso em: dez. 2017.

MASSON, Cléber. **Direito Penal Esquematizado** 7. ed. São Paulo: Editora Método, 2015. v. 2.

PAIVA, Mário Antônio Lobato de. Os institutos do Direito Informático. **Âmbito Jurídico**, Rio Grande, VI, n. 14, ago 2003. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/%3C?n_link=revista_artigos_leitura&artigoid=5487&revista_caderno=17>. Acesso em: out. 2017.

PINHEIRO, Patrícia Peck. **Direito Digital**. 3. ed. São Paulo: Saraiva, 2009.

ROSA, Fabrízio. **Crimes de Informática**. 2. ed. Campinas: BookSeller, 2005.

ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. **Caderno Jurídico**, Ano 2, n. 4, jul. 2002.

SMANIO, Gianpaolo Poggio. **Tutela Penal dos Interesses Difusos**. São Paulo: Atlas, 2000.
TIEDEMANN, Klaus. **Poder Económico y Delito**. Barcelona: Editorial Ariel, 1985.

_____. **Criminalidad Mediante Computadoras**. Disponível em: <http://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/download/4315/3569/>. Acesso em: dez. 2017.

TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal**. 4. ed. São Paulo: Saraiva, 1994.

VALENTE, Mariana Giorgetti; NERIS, Natália; RUIZ, Juliana Pacetta; BULGARELLI, Lucas. **O Corpo é o Código**: estratégias jurídicas de enfrentamento ao revenge porn no Brasil. São Paulo: InternetLab, 2016.

CRIMES CIBERNÉTICOS

11 ESTUPRO DE VULNERÁVEL SEM CONTATO FÍSICO

Fabiana Almeida de Jesus[1]

Resumo: Estupro de vulnerável sem contato físico é um tema complexo, não está tipificado na norma infraconstitucional. O objetivo da pesquisa será analisar a possibilidade de imputação concernente ao título dignidade sexual, uma vez que o Superior Tribunal de Justiça (STJ) passou a entender que o vulnerável, ao ser forçado à prática do ato libidinoso ou a qualquer prática sexual, ofende a dignidade da pessoa humana. Existe possibilidade jurídica de imputação ao crime de estupro de vulnerável sem contato físico? Foi utilizado para responder a pergunta o método pesquisa teórico-dogmática, no qual foram abordados estudos de doutrinadores, jurisprudências, noticiário jurídico, e entrevistas com autoridades judiciárias. Sendo assim, conclui-se que é possível imputar como crime no ordenamento jurídico o estupro de vulnerável sem contato físico em prol da dignidade da pessoa humana.

Palavras-chave: Estupro de vulnerável. Princípios constitucionais. Lacuna normativa. Humanização dos julgamentos. Imputação jurídica.

Abstract: *Rape of vulnerable without physical contact is a complex subject, not typified in the infraconstitutional norm. The objective of the research will be to analyze the possibility of imputation concerning the title sexual dignity, since the Superior Court of Justice (STJ) came to understand that the vulnerable to being forced to practice the libidinous act or any sexual practice, offends the dignity of the human person Is there a legal possibility of imputation to the crime of rape of vulnerable without physical contact? It was used to answer the question the theoretical-dogmatic research method, in which it was approached studies of doctrinators, jurisprudence, legal news, and interviews with judicial authorities. Thus, it is concluded that it is possible to impute as a crime in the legal system the rape of vulnerable without physical contact for the dignity of the human person.*

Keywords: Rape of vulnerable. Constitutional principles. Regulatory gap. Humanization of judgments. Legal attribution.

1 Introdução

A atual legislação penal brasileira, em seu art. 217-A, da Lei nº 12.015 de 2009, preleciona que só é caracterizado estupro de vulnerável com ato da conjunção carnal, o qual,

1 Acadêmica do 10º Período do Curso de Direito da Faculdade Doctum de Vitória, fabianadireitodejesus@gmail.com.

de acordo com dicionário informal significa intromissão do órgão genital masculino no interior da cavidade vaginal ou qualquer prática de ato libidinoso.

A pesquisa é questionável, apesar de tais condutas serem caracterizadas como ato libidinoso, o tema ainda é novo , raramente é discutido nos tribunais, nos centros acadêmicos e em sociedade de modo geral. Também, existem poucos doutrinadores que discutem o assunto.

Dessarte, far-se-á um paralelo utilizando o método bibliográfico e de análise de documentos, esclarecendo a distinção entre duas vertentes que se manifestam a respeito da necessária conjunção carnal para caracterização do crime, contrapondo parte da doutrina que apoia uma interpretação ampla do dispositivo, fundamentando não ser preciso o contato físico do agressor com a vítima, sendo irrelevante tal ação perante a violação sexual. Para entender a pesquisa, constata-se, então, ausência expressa no sentido de ser imputado como estupro de vulnerável sem contato físico, e não como satisfação de lascívia. Dessa forma, pretende-se verificar as possíveis mudanças na legislação penal e sua aplicabilidade nos crimes de dignidade sexual no que tange ao tema a ser pesquisado.

Sendo assim, a problemática do artigo será: existe possibilidade jurídica de imputação ao crime de estupro de vulnerável sem contato físico?

O objetivo geral da pesquisa é analisar a possibilidade de imputação no crime de dignidade sexual com relação ao estupro de vulnerável sem contato físico, uma vez que, o Superior Tribunal de Justiça passou a entender que o vulnerável ao ser forçado à prática do ato libidinoso ou a qualquer prática sexual que satisfaça a lascívia de terceiro, ofende a dignidade da pessoa humana, causando um dano físico e psíquico à vítima constrangida.

O tema deste artigo foi escolhido após a leitura de uma noticiá sobre um fato ocorrido em Mato Grosso do Sul, em que o Tribunal de Justiça considerou legítima a denúncia contra um homem acusado de contratar pessoas para levarem uma menina de dez anos a um motel, onde ela foi forçada a se despir para sua apreciação. Dessa forma, o Egrégio Tribunal de Justiça considerou o fato como estupro de vulnerável consumado sem contato físico.

A presente pesquisa apresenta grande relevância social, visto que as vítimas são pessoas vulneráveis que não possuem condições de se defenderem, e também por ferir princípios constitucionais, a dignidade da pessoa humana, a dignidade sexual e a liberdade sexual. Motivo pelo qual faz-se necessário mudar a tipificação penal em benefício

da sociedade, imputando como crime atos que deem prazer ao agente usando a pessoa do vulnerável para satisfazer a sua libido sexual.

Para elaborar o presente artigo, utilizou-se a pesquisa teórico-dogmática, sendo abordados estudos de doutrinadores, jurisprudências e matéria constitucional que indicam ser possível caracterizar estupro de vulnerável sem contato físico.

Teve como base de conhecimento caráter transdisciplinar, com incidência de investigações contidas entre searas distintas do Direito Penal, Direito Processual Penal, Direito Constitucional e no âmbito da Psicologia Jurídica. No Direito Penal o estudo será sobre a imputação jurídica da existência do crime de estupro de vulnerável sem contato físico. No Direito Processual Penal serão discutidas as possíveis mudanças na legislação, defendendo o posicionamento de ser punido como crime, e não como contravenção penal. No Direito Constitucional a pesquisa abrangerá direitos e princípios fundamentais. E na Psicologia Jurídica tratar-se-á a respeito dos danos e consequências que causam à vítima.

O primeiro capítulo deste artigo, intitulado: Estupro de vulnerável, trata sobre Lacuna normativa; Danos físicos e psíquicos à vítima; Princípios constitucionais violados; Importância da valorização da dignidade humana e o corolário da dignidade sexual. No segundo capítulo abordar-se-á a Constitucionalização do Código para atualização do Direito Penal, que consistirá na necessidade de atualizar esse ramo do direito por meio de penas mais severas para crimes que lesionam o bem jurídico protegido: a dignidade sexual e o confronto doutrinário em face da nova modalidade de estupro de vulnerável. O terceiro capítulo, tendo por título Imputação jurídica ao crime de estupro de vulnerável sem contato físico, no qual será discutida a importância da humanização dos julgamentos utilizando o direito como forma de promoção e justiça, bem como sobre a possibilidade de imputar o fato como crime e os benefícios desse ato para a sociedade.

2 Estupro de vulnerável

Estupro de vulnerável de acordo com art. 217-A do Código Penal só é consumado se o ato for caracterizado com a conjunção carnal ou a prática de outro ato libidinoso com menor de 14 (catorze) anos ou com alguém, que, por enfermidade ou deficiência mental, não tenha o necessário discernimento para praticar o ato ou que, por qualquer outra causa, não pode oferecer resistência (BRASIL, 1940).

Logo, verifica-se que o legislador especificou a caracterização de estupro de vulnerável somente a três grupos. Existe um rol taxativo de vulneráveis na legislação penal, mas há outros grupos, segundo entende a autora, que poderiam ser inseridos na referida lei como pessoas vulneráveis, visto que sua condição não a deixa ter forças para lutar em prol de sua defesa.

Assim, antes de mencionar quem poderiam ser esses vulneráveis, é importante falar sobre o conceito de vulnerabilidade.

> Vulnerabilidade é um conceito amplo, complexo, multidimensional e multideterminado; vulnerabilidade biológica: expressando pelo contínuo desequilíbrio das funções biológicas; vulnerabilidade psicológica: manifestada pelas funções psíquicas do indivíduo e ancorada pelos recursos emocionais e afetivos individuais; vulnerabilidade espiritual: ancorando-se em diferentes recursos simbólicos no enfrentamento de desafios e dos limites impostos pela realidade; vulnerabilidade cultural, social e ambiental: produzidas pelo entorno sociocultural e agenciadas pelas condições de desigualdade social, econômica e política, (JUNGES, 2007 apud SILVA; SILVA, 2012, p. 2).

Na mesma esteira, observa Victor Eduardo Rios Gonçalves: é necessário que o agente se aproveite do estado de incapacidade de defesa e que se demonstre que esse fator impossibilitava por completo a capacidade de a vítima se opor ao ato sexual (GONÇALVES, 2016, p. 678). Diante desses conceitos, podem-se encaixar em situação de vulnerabilidade os seguintes grupos:

Pessoa idosa: o Estatuto do Idoso afirma ser considerada idosas as pessoas com idade igual ou superior a 60 (sessenta) anos (BRASIL, 2003). Os idosos passam por mudanças contínuas em seu corpo, principalmente em seu estado emocional, e, devido a isso são considerados frágeis, pois a maior parte da população idosa tem sua saúde física e psíquica debilitada, sendo propícia a ser vitimada com enfermidades. São cons-

trangidos e agredidos facilmente em seu ambiente de convivência, não somente com agressões físicas, mas também com palavras, que os fazem ficar marcados ao longo da vida, por não conseguir expor ao próximo aquilo que lhes afligem e, sendo assim, preferem guardar para si. Outros vivem isolados sem apoio familiar, tendo que se desdobrar a cuidar dos afazeres domésticos ou vivem esquecidos por parentes em um leito de hospital e asilos.

Os ébrios habituais e viciados em tóxicos: tanto o uso de substâncias alcoólicas quanto o uso de drogas ilícitas altera o estado mental do sujeito, ou seja, a partir do momento em que usam demasiadamente esses ilícitos, perdem o controle da própria vida. O Código Civil (Lei nº 10.406/2002), em seu art. 4º, inciso II, preleciona a incapacidade relativa dos ébrios habituais e viciados em tóxicos, o que significa dizer que não podem exercer os atos da vida civil por completo, somente na dependência de outros, independentemente de a embriaguez ocorrer de forma voluntária ou involuntária, mesmo assim é considerado um ser vulnerável em consequência de não poder exprimir suas próprias vontades (BRASIL, 2002).

Da diversidade sexual: no momento atual, verifica-se a evolução da sociedade em todos os sentidos – comportamental, profissional, sentimental, sexual. Todavia, no que tange às questões de gênero, ainda existe intolerância por parte de muitos no sentido de não aceitá-los como diferentes da sociedade, e sendo assim, acabam por agredir fisica e psicologicamente esses indivíduos de forma brutal. A violência ao grupo LGBT (lésbicas, gays, bissexuais, travestis) existe desde os primórdios, a falta de respeito ao próximo prevalece nas atitudes de muitas pessoas, principalmente no convívio familiar, e isso faz com que o número de delitos às vítimas venha a crescer cada vez mais.

Mulher x homem no ambiente doméstico: no início da civilização, tinha-se a crença de que o homem era superior à mulher, de que esta devia obediência àquele, tinha seus direitos restringidos, deveria cumprir apenas com obrigações no ambiente doméstico, por exemplo, satisfazer aos prazeres sexuais do homem, que não dependia ao menos do consentimento desta para coabitação. Não bastasse isso, a agressão física e psicológica ainda faz parte do ambiente doméstico de muitas famílias, e isso inclui todos os tipos de violência, e não se pode duvidar que o sujeito seja capaz de cometer crimes contra o próximo, por muitas vezes não deixá-lo ter a liberdade que é sua por direito. Com o passar dos anos, a mulher conquistou seu espaço em sociedade, tendo seus direitos valorizados na seara profissional, vida íntima, política, religiosa e familiar. Apesar de grandes conquistas, ainda, tem sido alvo do machismo, tornando-se mais uma vítima para estatística de agressão. Sem embargos, é importante frisar, essa situação engloba

também homens que são violentamente agredidos por suas companheiras. E esses fatos também contribuem para o aumento da estatística de violência doméstica.

Para suprimir a violência contra a mulher, o legislador inseriu no art. 121, § 2º (homicídio qualificado) do Código Penal, o inciso VI, § 2º-A, da Lei nº 13.104/2015 (Feminicídio), como também está em vigor há 11 (onze) anos, a Lei nº 11.340/2006 (Violência Doméstica). As referidas leis têm como principal objetivo garantir direitos e trazer proteção às mulheres vítimas de agressões físicas, psicológicas praticadas por companheiros no ambiente doméstico, familiar e em sociedade. Por mais que a proteção às mulheres seja importante, não se pode passar despercebida a situação de homens vítimas de agressões praticadas por mulheres que estão na condição de companheira. Observa-se por meio da decisão interlocutória, dos autos de nº 1074/2008:

> [...]. Embora em número consideravelmente menor, existem casos em, que o homem é quem vem a ser vítima da mulher tomada por sentimento da posse e da fúria que levam a todos os tipos de violência, diga-se: física, psicológica, moral e financeira. No entanto, [...] para estes casos não existe previsão legal de prevenção à violência, pelo que requer a aplicação da lei em comento por analogia. [...]. É certo que não podemos aplicar a lei penal por analogia quando se trata de norma incriminadora, porquanto fere o princípio da reserva legal, firmemente encabeçando os artigos de nosso código Penal Art. 1º. [...]. Ora, se podemos aplicar a analogia para favorecer o réu, é óbvio que tal aplicação é perfeitamente válida quando o favorecido é a própria vítima de um crime. É possível a "aplicação da lei 11.340/06 para os homens, uma vez que não existe lei análoga a ser aplicado quando o homem é vítima de violência doméstica". Por algumas vezes me deparei com casos em que o homem era vítima do descontrole emocional de uma mulher que não media esforços em praticar todo o tipo de agressão possível contra o homem. Não é vergonha nenhuma o homem se socorrer ao Poder Judiciário para fazer cessar as agressões da qual vem sendo vítima. [...]. "E compete à justiça fazer o seu papel de envidar todos os esforços em busca de uma solução de conflitos, em busca de um a paz social". (CONJUR, 2008).

Assim, homem e mulher são considerados vulneráveis quando agredidos fisicamente, psicologicamente, financeiramente por seus companheiros(as) no seio familiar.

Conjuntamente, incluir como vulneráveis pessoas que vivem em condição de rua, profissionais do sexo (prostitutas), pessoas de identidade de gênero diversa, pessoas com deficiência física e mental, como aqueles que vivem e se sentem inferiores aos outros, de forma desigual e que na ocasião não conseguem adquirir forças para defesa própria.

2.1 Lacuna normativa

Ao analisar o art. 217-A do Código Penal, apesar de ser considerado um delito hediondo conforme dispõe a Lei nº 8.072/1990, nota-se a ausência de um dispositivo penal mais severo, devido a descrição do trecho legal iniciar com verbo "ter" conjunção carnal ou "praticar" outro ato libidinoso. Constata-se, então, a caracterização do crime tão somente com contato físico (conjunção carnal ou prática de libidinagem), isto é, o agressor precisa tocar na vítima para ser enquadrado como estupro de vulnerável (BRASIL, 1940).

A legislação penal valoriza a dignidade da pessoa humana, a dignidade sexual, e, ainda assim, faz-se necessário alterar a redação do dispositivo legal, com objetivo de caracterizar como crime o estupro de vulnerável sem contato físico, a fim de que possa trazer segurança jurídica às pessoas vulneráveis, como também a toda a sociedade que fica à mercê de tanta violência.

2.2 Danos físicos e psíquicos à vítima

Não dá para calcular os danos físicos e psíquicos que o vulnerável sofre ao ser vítima de estupro, muitas vezes o dano é irreparável, não há como esquecer os abalos sofridos durante o ato. O dicionário jurídico traz o conceito de dano no Direito Penal:

> Dano: (Lat. *Damno*.) mal que se faz a alguém; prejuízo ou ofensa material ou moral, resultante da culpa extracontratual ou aquiliana que importa em responsabilidade civil; prejuízo causado por alguém a outrem, cujo patrimônio seja diminuído, inutilizado ou deteriorado, qualquer ato nocivo, prejudicial, produzido pelo delito (CP. arts. 163, 165, 166, 181, 182, 259, e 346; CC. arts. 159 e 1092). Dano material: o mesmo que dano real; dano causado por lesões corporais (*coisa corpórea*) ou atentado à integridade física de alguém. Dano moral: aquele que atinge um bem jurídico de ordem moral ou

> pessoal, particular, como a honra, a dignidade, a consideração social. (CC. art. 7º), (SANTOS, 2001, p. 69).

Não existe dano maior ou menor, a dor da agressão física e psicológica é a mesma, as consequências podem ser para a vida toda, em muitos casos não há cura. A vulnerável quando vítima do estupro com conjunção carnal pode ser surpreendida com uma gravidez indesejada, com doenças sexualmente transmissíveis (DST). O constrangimento é inevitável, a vítima fica com o psicológico abalado, por causa do medo não consegue expor os momentos terríveis que vivenciou. Assim, optam por conviver com sentimento de angústia, vergonha e revolta ao saber que sua honra foi manchada. Ocorrem, assim, trauma físico e psicológico por não conseguirem ser igual aos outros em sociedade ou por não terem vida própria com saúde e bem-estar. Essas possíveis enfermidades podem induzir ao suicídio de muitos inocentes, que em vez de buscarem ajuda, acreditam que a solução é dar um fim a própria vida (GESSE, 2008).

O vulnerável pode ser vítima de estupro sem ter o contato físico no momento em que satisfaz à lascívia de outrem, o que pode ser caracterizado apenas com um olhar para satisfazer à libido do agressor. Na legislação atual não existe imputação para estupro de vulnerável sem contato físico, mas esse delito tem sua punição a partir do art. 218, do Código Penal, o que deveria ser mudado, pois quando a vítima é constrangida a participar de determinados atos que satisfaçam ao prazer sexual do agressor, deveria ser considerado como estupro de vulnerável sem contato físico.

2.3 Princípios constitucionais violados

A República Federativa do Brasil tem como fundamento a dignidade da pessoa humana, (BRASIL, CF 1988). É um princípio constitucional que valoriza o homem e a mulher como pessoa, não somente com valores morais, mas tão somente com valores éticos e espirituais. O ser humano deve ser tratado com respeito e ser protegido pelo Estado, apesar de este não ter condições de oferecer uma proteção individualizada, de outra sorte, cabe ao sujeito tentar se proteger das melhores formas possíveis.

Ao enfatizar a dignidade humana, Rodrigo César Rebello Pinho prescreve: “O valor da dignidade da pessoa humana deve ser entendido como o absoluto respeito aos direitos fundamentais, assegurando-se condições dignas de existência para todos” (PINHO, 2006, p. 63).

Dessa forma, quando o vulnerável for constrangido à prática do ato sexual ou libidinagem, além de ter sua dignidade humana violada, a sua dignidade sexual também sofre violação, tendo em vista que o art. 217-A do Código Penal (alterado pela Lei nº 12.015/2009) tutela este princípio (BRASIL, 1940).

Nesse ponto de vista, não se deve partir da presunção de que a pessoa vulnerável já tenha como prática diária a vivência sexual, é o que relata nos ensinos de Luiz Regis Prado:

> Configura o delito a conduta de ter conjunção carnal ou praticar ato libidinoso com pessoa menor de 14 (catorze) anos, ainda que a vítima tenha consentido no ato, pois a lei ao adotar o critério cronológico acaba por presumir *iuris et deiure*, pela razão biológica da idade, que o menor carece de capacidade e discernimento para compreender o significado do ato sexual. Daí negar-se existência válida a seu consentimento, não tendo ele nenhuma relevância jurídica para fins de tipificação, (PRADO et al., 2014, p. 1047-1048).

No mesmo sentido, o Superior Tribunal de Justiça publicou a Súmula nº 593:

> O crime de estupro de vulnerável se configura com a conjunção carnal ou prática de ato libidinoso com menor de 14 anos, sendo irrelevante eventual consentimento da vítima para a prática do ato, sua experiência sexual anterior ou existência de relacionamento amoroso com o agente" (BRASIL, 2017b).

Ao contrário, alguns magistrados entendem não haver crime se o ato for de consentimento da vítima:

> Namoro Precoce – Consentimento da família afasta tipificação de estupro de vulnerável: O artigo 217-A do CP diz, expressamente, ser estupro de vulnerável a prática de sexo ou ato libidinoso com menor de 14 anos, mas a 6ª Câmara do Tribunal de Justiça do Rio Grande do Sul entendeu que a idade não basta para a aplicação do dispositivo. Para o colegiado, também é preciso analisar o contexto dos fatos para se verificar a vulnerabilidade da menor. Por isso, manteve o trancamento de uma ação penal do MP contra um rapaz de 18 anos, seus pais e a mãe de sua namorada, uma menina de 12 anos. Nos dois graus de jurisdição, o entendimento predominante foi de que o convívio do rapaz com a menor na casa dele, com a ciência e coni-

> vência dos pais, está inserida em uma realidade social em que os jovens têm iniciação sexual mais precoce. A denúncia do MP-RS relata que o rapaz praticava sexo com a garota com o consentimento de seus pais da mãe da menor. Para a promotoria, a mãe da menina tinha o dever de impedir a convivência da filha com o namorado. [...]. O juízo da comarca de origem considerou atípica a conduta e, em decorrência, rejeitou a denúncia. Para o julgador, não basta o enquadramento do fato no dispositivo do Código Penal, sem levar em conta a evolução da sociedade. [...]. A decisão citou doutrina do penalista Guilherme de Souza Nucci: "O legislador brasileiro encontra-se travado na idade de 14 anos, no cenário dos atos sexuais, há décadas. É incapaz de acompanhar a evolução dos comportamentos na sociedade. Enquanto o ECRIAD proclama ser adolescente o maior de 12 anos, a proteção penal ao menor de 14 anos continua rígida. [...]." Conforme o juiz, as informações trazidas aos autos permitem relativizar a vulnerabilidade da vítima, o que leva à atipicidade da conduta narrada pelo MP-RS. Afinal, a menor disse à polícia que já namorava o indiciado, consentindo com as relações sexuais. Desde fevereiro de 2016, passou a morar na casa dos pais dele, sem abrir mão de frequentar à escola. ["...]:", [...]. A relatora da apelação-crime no TJ-RS, desembargadora Vanderlei Teresinha Kubiak observou que a menor e o indiciado mantêm um relacionamento afetivo duradouro. Logo, não se trata de uma situação de abuso sexual, mas de precocidade. Por este raciocínio, seria uma "hipocrisia" impor pesada pena aos denunciados, quando há nas novelas, filmes, seriados e programas de televisão todo um estímulo à sexualidade (MARTINS, 2017).

Não obstante, a Constituição Federal (1988) demonstra com clareza a proteção dos direitos e deveres individuais:

> Art. 5º, *caput*, X: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade. São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, CF 1988).

A inviolabilidade sexual não se dá apenas no citado inciso X, do art. 5º, da Constituição Federal, mas também têm-se um valor moral, os costumes individuais, a liberdade

sexual que, quando atingidos, precisam ser reparados. Os agressores devem ser penalizados para valorização do respeito mútuo em sociedade.

O vulnerável de forma genérica tem por direito a escolha de com quem deseja manter o relacionamento, assim como de se portar em sociedade, mesmo que já tenha como prática no dia a dia a vivência sexual deve ser respeitado o consentimento da vítima. O mero constrangimento, a grave ameaça e violência física e psíquica podem ser considerados como prática de estupro de vulnerável.

2.4 A importância da valorização da dignidade humana e o corolário da dignidade sexual

A dignidade humana é um princípio fundamental, abrange a todos sem nenhuma exceção, é um valor moral, intrínseco, ou seja, é personalíssimo do sujeito, e por isso, é necessário ter sua dignidade como pessoa protegida. Além disso, é um direito supremo, está acima dos direitos e garantias fundamentais, uma vez que não há como proteger a dignidade da pessoa humana, se os direitos fundamentais não são garantidos de forma a valorizar o ser humano como pessoa, conforme escreve Maria Celina Bodin de Moraes:

> [...] A Constituição consagrou o princípio e, considerando a sua eminência, proclamou-o entre os princípios fundamentais, atribuindo-lhe o valor supremo de alicerce da ordem jurídica democrática. Com efeito, da mesma forma que Kant com a ordem moral, é na dignidade humana que a ordem jurídica (democrática) se apoia e se constitui. Neste ambiente, de um renovado humanismo, a vulnerabilidade humana será tutelada, prioritariamente, onde quer que se manifeste. Terão precedência os direitos e as prerrogativas de determinados grupos considerados, de uma maneira ou de outra, frágeis e que estão a exigir, por conseguinte, a especial proteção da lei. Nestes casos estão às crianças, os adolescentes, os idosos, os portadores de deficiências físicas e mentais, os não-proprietários, os consumidores, os contratantes em situação de inferioridade, as vítimas de acidentes anônimos e de atentados a direitos da personalidade, os membros da família, os membros de minorias, entre outros. O Constituinte ao instituir a Constituição Federal de 1988, teve o cuidado de assegurar a todos os povos os direitos sociais, individuais, à liberdade, à segurança, o bem-estar, à igualdade, e a justiça como os valores supremos de uma sociedade fraterna, pluralista e sem preconceito (em todos os aspectos). Ao observar este

> preâmbulo, verifica-se o dever que o Estado tem em proteger e garantir a todos a segurança jurídica quando os direitos fundamentais são violados diariamente pelo mesmo ente estatal que ao invés de garantir proteção, muitas vezes viola direito de uma forma coletiva e individual (MORAES, 2006, p. 12).

No mesmo sentindo, afirma Fabiano Lepre Marques (2011): "A dignidade da pessoa humana passa a ser, assim, um valor essencial, reconhecido nos mais variados documentos nacionais e internacionais, constituindo-se naquilo que parece ser" (MARQUES, 2011, p. 10).

A Declaração Universal de Direitos Humanos (ONU, 1948) confirma, em seu art. 1º que todos os seres humanos nascem livres e iguais em dignidade e em direitos; dotados de razão e de consciência, devem agir uns para com os outros em espírito de fraternidade. Igualmente, a Constituição Federal, no art. 5º, declara a igualdade de direitos e garantias fundamentais. Não se pode olvidar que a pessoa vulnerável, assim como todos os cidadãos, merece ter sua liberdade respeitada, sendo esta a de ir e vir, liberdade de expressão, liberdade de escolha, liberdade sexual, como também de ter seus direitos sexuais protegidos. (BRASIL, CF 1988).

Noutras palavras, a pessoa não pode ter seu direito sexual invadido por agressores(as) que agem com dolo e intuito de destruir a vida da pessoa vulnerável por meio de toque físico, palavras ou, até mesmo, com o olhar. Sobretudo, aquilo que cause constrangimento, humilhação à sua vida privada e à sua intimidade.

Para os comentadores do Código Penal (2002), anteriormente, protegia-se o gênero "mulher", pois, em alguns artigos de lei, tinha-se transcrito a proteção da "mulher honesta", assim como a tipificação da sedução de "mulher virgem, menor de dezoito anos e maior que catorze anos", em que, à época, o objeto jurídico indicava integridade ou a virgindade da menor, a saber:

> Art. 213. (Estupro) – constranger mulher à conjunção carnal, mediante violência ou grave ameaça: Pena – reclusão, de seis meses a dez anos.
> Art. 215. Ter conjunção carnal com mulher honesta, mediante fraude: Pena: reclusão, de um a três anos [...].
> Art. 216. Induzir mulher honesta, mediante fraude, a praticar ou permitir que com ela se pratique ato libidinoso diverso da conjunção carnal: Pena – reclusão, de um a dois anos [...].

> Art. 217. Seduzir mulher virgem, menor de dezoito anos e maior de catorze, e ter com ela conjunção carnal, aproveitando-se de sua inexperiência ou justificável confiança. Pena: reclusão, de dois a quatro anos (DELMANTO et al., 2002, p. 458; 467; 469; 471).

Com a evolução da sociedade, o legislador instituiu a Lei nº 12.015/2009 em que passou a tratar, a partir do título VI, dos crimes contra a dignidade sexual, o qual a tutela da dignidade sexual foi valorizada, pois o Direito Penal não mais protege somente a mulher, mas também os homens, considerando que estes podem ser vítimas de estupro, isto é, homem e mulher incluem-se como sujeito passivo – sendo vítimas, assim como podem ser sujeito ativo – autores do delito. Dessa feita, o corolário da dignidade sexual valorizou a vítima em situação de vulnerabilidade com a junção dos atos libidinosos com a prática da conjunção carnal.

3 Constitucionalização do código para o Direito Penal

Ao perceber a vida do homem em sociedade, constata-se a falha que cometemos no dia a dia, sendo mau, desumano com o próximo, quer dizer, somos o retrato do que relata o filósofo inglês Thomas Hobbes ao afirmar em sua filosofia: o homem é lobo do homem por sua própria natureza, e devido a isso seria necessário as pessoas pactuarem um contrato entre si, em renúncia à própria liberdade em troca de tranquilidade (HOBBES apud SCHULTZ, 2007).

Corolariamente se pode comparar a Carta Magna com a filosofia de Hobbes, a qual, no momento em que transferiu a responsabilidade do povo que lutava por proteger seus direitos e deveres ao Estado por meio de um documento chamado contrato social, atribuiu poderes ao Estado a fim de regular e aplicar normas coercitivas a quem descumprisse alguma cláusula contratual. Em nossa República Federativa, no ano de 1988, foi promulgada, por meio de um Estado Democrático de Direito, a Constituição Federal, com objetivo de assegurar direitos e garantias fundamentais, impor normas e aplicar sanções impostas pelo Estado a quem descumpre ou viola direito do outro.

Todas as normas infraconstitucionais são embasadas pela Constituição Federal, isto é toda norma precisa ter como princípios os direitos e garantias fundamentais, é o que será estudado neste capítulo, a saber, a constitucionalização do Código Penal deve ser o exercício principal dos legisladores que editam a redação das normas penais que

tipificam um novo tipo penal. Assim, percebe-se que o Decreto-Lei nº 2.848/1940 "Código Penal" foi recepcionado pela Constituição Federal de 1988, como forma de proteção ao bem jurídico tutelado.

Nessa vereda, nos leva à lição de Nucci:

> Quando um bem jurídico é destacado como tal, surgem tipos penais incriminadores para protegê-los, indicando as condutas proibidas, sob pena de lesão ao referido bem jurídico tutelado. A Constituição Federal indica vários bens jurídicos, vários dos quais o Direito Penal chamou para si para a conveniente e proteção e amparo. Ilustrando, vêem-se os seguintes bens jurídicos fundamentais: vida, liberdade, igualdade, segurança, propriedade, intimidade, vida privada, honra, trabalho, dentre outros (NUCCI, 2013, p.74).

Em concordância, o doutrinador Capez, afirma:

> Toda ação humana está sujeita a dois aspectos valorativos diferentes. Pode ser apreciada em face da lesividade do resultado que provocou (desvalor do resultado) e de acordo com a reprovabilidade da ação em si mesma (desvalor da ação). Toda lesão aos bens jurídicos tutelados pelo Direito Penal acarreta um resultado indesejado, que é valorado negativamente, afinal foi ofendido um interesse relevante para a coletividade (CAPEZ, 2013, p. 19).

Sobretudo, o Código Penal sendo considerado o último recurso, deve ser aplicado quando não houver outros meios de solucionar o conflito e assegurar os bens jurídicos listados como princípios fundamentais, além disso o principal bem tutelado pelo Código Penal é a vida, e esta merece proteção em todos os sentidos. Se, por exemplo, ocorre violação do direito à liberdade sexual, o agente precisa ser punido a depender do caso concreto com restrição de sua liberdade a fim de manter a ordem pública e a paz em sociedade.

Portanto, o Código Penal está em consonância com a Constituição Federal à medida que obedece aos requisitos do art. 5º, em especial o inciso XLVIII "a pena será cumprida em estabelecimentos distintos, de acordo com a natureza do delito, a idade e o sexo do apenado". Logo, a constitucionalização do Direito Penal é importante para garantir que o direito seja posto em prática nas ordens da Constituição Federal.

3.1 Atualização do Direito Penal com penas mais severas para crimes que lesionam o bem jurídico protegido: a dignidade sexual

Inicialmente, antes de adentrar no tema em questão, é importante destacar que outrora, o capítulo VI do Código Penal tinha por denominação: Dos crimes contra os costumes, pois naquele tempo se ditava como as pessoas deveriam se comportar sexualmente em sociedade, o que nos leva a entender que a violação sexual era culpa da vítima, e não do agente violentador. A vítima quando deflorada, por exemplo, com ou sem o próprio consentimento era rejeitada muitas vezes por sua família e até mesmo pela sociedade. Entendia-se, à época, ser imoral a mulher perder a virgindade antes do casamento, de acordo com os costumes daquele tempo a mulher deveria ser honesta, não sensual a ponto de provocar a libido do agente.

Com a Lei nº 12.015/2009 foi alterada a denominação "Dos crimes contra os costumes" para "Dos crimes contra a dignidade sexual" em obediência ao princípio da dignidade humana previsto no art. 1º, inciso III, da Constituição Federal, de modo que muitos dispositivos que feriam a dignidade humana foram revogados do Código Penal, situação em que se deu margem à junção de dispositivo legal já existente no Código Penal com a criação de novos delitos. É bom frisar, em prol da dignidade sexual, alguns delitos tiveram a tipificação de pena aumentada (BRASIL, CF 1988).

Tecidas as considerações, a Lei nº 12.015/2009 incluiu na norma infraconstitucional a tipificação delitiva, o art. 217-A como estupro de vulnerável, acrescidas do aumento de pena se resultar lesão corporal de natureza grave e se a conduta resultar em morte da vítima. Ao caminhar pelo Código Penal, percebe-se que o aumento de pena ocorre apenas nas condutas de lesão corporal grave e se resultar em morte da vítima. Mas, em contrapartida, se a prática delitiva tiver como resultado lesão corporal de natureza leve, presume-se, então, que o agente é punido com pena branda, a saber, pelo *caput* do art. 217-A (BRASIL, 2009).

Por outro lado, existem práticas sexuais que constrangem a vítima, e não são considerados no Código Penal como estupro. Na doutrina, sobreleva a lição de Rogério Greco:

> O estupro pode ser caracterizado mesmo sem contato físico: Entendemos não ser necessário o contato físico entre o agente e a vítima para efeitos de reconhecimento do delito de estupro, quando a conduta do agente for diri-

> gida no sentido de fazer com que a própria vítima pratique o ato libidinoso, a exemplo do que ocorre quando o agente, mediante grave ameaça, a obriga a se masturbar (GRECO, 2013, p. 497).

Nesse sentido, importa dizer o quanto é significativo atualizar o Código Penal com relação aos delitos praticados contra pessoa vulnerável, seria sábio incluir na redação do art. 217-A como delito de estupro sem o contato físico, mesmo que seja uma imputação branda, mas será necessário para reprimir a sociedade criminógena, visto que só pode tipificar crimes por meio de lei, conforme descrito no art. 5º, inciso XXXIX, da Constituição Federal, ao passo que, em consonância com o princípio da legalidade está o art. 1º do Código Penal, em que ambos preveem: não há crime sem lei anterior que o defina; não há pena sem prévia cominação legal. Sendo assim, terá como resultado o respeito da moral, dos bons costumes, não somente estas, mas também para a tutela do bem jurídico, isto é, a dignidade sexual (BRASIL, CF 1988; BRASIL, 1940).

3.2 Confronto doutrinário em face da tipificação legal

O tema discutido é bastante controverso, é uma novidade para sociedade, pois não há tipificação legal, então quando ocorre um fato que poderia ser imputado como crime de estupro sem contato físico, passa-se despercebido por não haver toque entre a vítima e o agente violentador. Sendo que, na prática e na a maioria das vezes, a condenação do indivíduo é tipificada como um mero constrangimento ilegal (art. 146 do CP), como satisfação de lascívia própria ou de outrem (arts. 218, 218-A do CP), conforme se demonstra no julgado da 2ª Turma Criminal do TJDFT, em que se desclassifica o crime de estupro de vulnerável por mero toque corporal:

> DESCLASSIFICAÇÃO DO CRIME DE ESTUPRO DE VULNERÁVEL - MERO TOQUE CORPORAL: O toque íntimo de consequências menores e de censurabilidade pouco intensa não é suficiente para configurar o crime de estupro de vulnerável. Não se pode dar uma interpretação muito ampla ao conceito de ato libidinoso, equiparando os atos lascivos àqueles meramente ofensivos ao pudor, sob pena de se aplicar punições injustas e desproporcionais. Para o entendimento predominante, o toque superficial nas partes íntimas da vítima, de forma rápida e inesperada, embora reprovável, não caracteriza o crime de estupro de vulnerável, mas sim a contravenção penal de perturbação da tranquilidade. Dessa forma, o Colegiado, majoritariamente, desclassificou a conduta atribuída ao réu para o delito do artigo 65 da Lei

> de Contravenções Penais. Em sentido contrário, o voto minoritário entendeu que a conduta consistente em apalpar a genitália da vítima menor de idade, em contato direto com a pele, é fato que se amolda à figura típica do artigo 217-A do Código Penal. Acórdão n.º 793811, 20120110818353APR, Relator: ROBERVAL CASEMIRO BELINATI, Revisor: SILVANIO BARBOSA DOS SANTOS, 2ª Turma Criminal, Data de Julgamento: 08/05/2014, Publicado no DJE: 03/06/2014. p.: 253. (INFORMATIVO TJDFT DJE, 2014).

No mesmo entendimento, certifica Bintecourt (2011): "Passar as mãos nas coxas, nas nádegas ou nos seios da vítima, ou mesmo um abraço forçado, configura a nosso juízo, a contravenção penal do art. 61 da Lei Especial, quando praticados em lugar público ou acessível ao público" (BINTECOURT, 2011, p. 108).

Por outro lado, apesar de não estar descrito como estupro de vulnerável sem contato físico na legislação vigente, a doutrina majoritária defende que não necessariamente é caracterizado estupro com conjunção carnal ou ato libidinoso, basta apenas haver constrangimento que viole a dignidade sexual, afirma Rogério Sanches Cunha:

> De acordo com a maioria da doutrina, não há necessidade de contato físico entre o autor e a vítima, cometendo o crime o agente que, para satisfazer sua lascívia, ordena que a vítima explore seu próprio corpo (masturbando-se), somente para contemplação (tampouco há que se imaginar a vítima desnuda para a caracterização do crime – RT 429/380) (CUNHA, 2016, p. 460).

Nesse raciocínio, para Damásio de Jesus, pratica o crime de estupro aquele, que, com o emprego de violência ou grave ameaça, acaricia as partes pudendas de uma jovem por sobre o seu vestido (CASTRO, 2014).

Percebe-se que em toda história jurídica, teve-se apenas um julgamento procedente que condenou o réu por estupro de vulnerável sem contato físico, ao considerar "a dignidade sexual não se ofende somente com lesões de natureza física":

> Agressão emocional - estupro de vulnerável pode ser caracterizado ainda que não haja contato físico entre o agressor e a vítima. Com esse entendimento, a 5ª Turma do Superior Tribunal de Justiça confirmou decisão do Tribunal de Justiça de Mato Grosso do Sul que considerou legítima a denúncia contra um homem acusado de contratar, mais de uma vez, pessoas para levarem uma menina de dez anos a um motel, onde ela foi forçada a

tirar a roupa, por R$ 400 mais comissão para a irmã da vítima. No Recurso em Habeas Corpus, a defesa do acusado alegou que a denúncia é inepta, e, portanto, o réu deveria ser absolvido até porque não há provas de sua conduta. Para o defensor, não é possível caracterizar um estupro consumado sem contato físico entre as pessoas. Em seu voto, acompanhado pelos demais ministros da turma, o relator do processo, ministro Joel Ilan Paciornik, disse que, no caso analisado, o contato físico é irrelevante para a caracterização do delito. Para o magistrado, a denúncia é legítima e tem fundamentação jurídica em conformidade com a doutrina atual. "A maior parte da doutrina penalista pátria orienta no sentido de que a contemplação lasciva configura o ato libidinoso constitutivo dos tipos dos artigos 213 e 217-A do Código Penal, sendo irrelevante, para a consumação dos delitos, que haja contato físico entre ofensor e ofendido." Dignidade sexual: O relator lembrou que a dignidade sexual é passível de ser ofendida mesmo sem agressão física, como no caso da denúncia, em que uma criança foi forçada a se despir para a apreciação de terceiro. Segundo Paciornik, a denúncia descreve detalhadamente o crime, preenchendo os requisitos legais para ser aceita. Em seu parecer, o Ministério Público Federal opinou pela rejeição do pedido da defesa. O MPF considerou que o ato lascivo de observar a criança nua preenche os requisitos previstos na legislação brasileira para ser classificado como um caso de estupro, por se tratar de menor sem chances de defesa e compreensão exata do que estava ocorrendo. O ministro Jorge Mussi, ao acompanhar o voto do relator, disse que o contexto delineado revelou "uma situação temerária de se discutir se teve contato ou não", sendo suficiente, até o presente momento, a denúncia apresentada pelo Ministério Público. Para o ministro Ribeiro Dantas, o conceito de estupro apresentado na denúncia (sem contato físico) é compatível com a intenção do legislador ao alterar as regras a respeito de estupro, com o objetivo de proteger o menor vulnerável. De acordo com ele, é impensável supor que a criança não sofreu abalos emocionais em decorrência do abuso. O caso faz parte de investigação sobre uma rede de exploração de menores em Mato Grosso do Sul e envolve políticos e empresários de Campo Grande e região. Para o advogado do réu, José Trad, a decisão deste julgamento foi contra jurisprudência pacificada do STJ, principalmente pelas 5ª e 6ª turmas. Ele destaca que a corte sempre entendeu que o estupro só é consumado com contato físico. "Os ministros se impressionaram com a denúncia", justifica, destacando que compreende a preocupação dos ministros em tutelar a dignidade sexual dos menores de 14 anos. Trad

> ressalta ainda que apesar do entendimento da corte em considerar o crime como estupro de vulnerável, os ministros fizeram ressalvas ao voto do relator, destacando a importância do tema no debate doutrinário por haver divergência. "A questão não está definitivamente fechada." O advogado diz estranhar o fato de seu cliente ser enquadrado no crime de estupro de vulnerável (217-A do Código Penal) por contemplação lasciva mesmo havendo o artigo 218-A, que trata de satisfação de lascívia na presença de criança ou adolescente e traz condutas mais graves do que a contemplação. "Mesmo assim, ele está sujeito a uma pena muito mais severa", reclama. Afirma que ainda estuda se irá apresentar recurso ao STJ ou levar a questão ao Supremo. "Não há lógica ou razoabilidade em se punir a contemplação lasciva pelo artigo 217-A e punir condutas mais graves pelo artigo 218-A". "O precedente é perigoso", complementa. Na questão de mérito, onde a defesa alega falta de justa causa, José Trad destaca que há divergências entre a acusação e o depoimento prestado pela menina ao Ministério Público. "A história que a menor contou em depoimento no Ministério Público não foi bem assim. A história que ela conta dá a impressão de que esse encontro não se consumou por vontade do próprio acusado. Ela teria dito que, no motel, ele simplesmente olhou para a menina e ficou com medo ao ver que se tratava de uma menor de idade. Então ele teria mando a menina se vestir e ir embora", finaliza. (CONJUR, 2016).

Decisão justa pela 5ª Turma do Superior Tribunal de Justiça, embora não exista imputação expressa no Código Penal, o julgamento teve por base o princípio da dignidade humana e da dignidade sexual. Assim, percebem-se as controvérsias até mesmo perante as turmas dos Tribunais, quanto aos julgamentos de violação à dignidade sexual, uma vez que ainda não está pacificado, ou seja, não existe jurisprudência com relação à imputação de crime quanto a estupro de vulneráveis sem contato físico.

4 Imputação jurídica ao crime de estupro de vulnerável sem contato físico

Como já mencionado, na legislação brasileira não está tipificado como crime o estupro de vulnerável sem contato físico, dessa feita não há imputação legal. A tipificação do artigo 217-A, do Código Penal impõe como requisito para consumação do delito o contato entre vítima e o agente violentador, sendo praticada uma das duas condutas ou até

mesmo, se as duas condutas são praticadas no mesmo instante, o agressor responderá por crime único na modalidade hedionda, conforme dispõe a Lei nº 12.015/1990.

É importante frisar, a pena para esse delito é bem severa, desde o início o criminoso fica recluso, em regime inicial fechado, com pena mínima de 8 a 15 anos, se ainda resultar lesão corporal de natureza grave, a pena mínima passa a ser de 10 a 20 anos, quando há resultado em morte, a reclusão será de 12 a 30 anos. É um crime de ação pública condicionada à representação se a vítima for maior de idade. Sendo a vítima menor de 18 anos ou pessoa vulnerável, o crime passa a ser de ação penal pública incondicionada. Em ambos os procedimentos têm-se todo um rito a ser seguido no Código de Processo Penal e na Lei de Execução Penal (BRASIL, 1940).

Quando em sociedade acontecem cenas que violam a sexualidade do vulnerável, mesmo que essa violação não envolva toque, a autoridade policial ou até mesmo membros do Ministério Público, a partir do momento que tomam conhecimento do fato, muitas vezes caracterizam o delito como uma contravenção penal, em que a sanção é um pouco mais branda.

Para mudar essa realidade, e ainda com objetivo de trazer segurança jurídica às vítimas dessas atrocidades, é primordial uma nova imputação jurídica para que tais fatos sejam considerados crimes.

Segundo a teoria *tripartida*, criada pelo filósofo Hans Welzel, a qual é adotada por correntes majoritárias, crime é fato típico, antijurídico e culpável (MASSON, 2011, p. 175-176), isto é, para configurar crime é necessário que a conduta do meliante seja um ato reprovado pela sociedade e pelo ente estatal, visto que de nada adianta o sujeito cometer um fato que no momento pode ser incriminado por toda a sociedade, mas que não constitui crime.

Assim, só se pode imputar comportamentos como crime por meio de lei, pois é um princípio constitucional, conforme afirma o dicionário latino jurídico: "*nullum crimem, nulla poena sine lege poenale*" – Não há crime sem lei que o qualifique; não há pena sem lei penal. "*nullum crimem, nulla poena sine praevia lege*" – Não há crime, nem pena, sem lei prévia, (GUIMARÃES, 2012, p. 334). Sendo assim, o Estado agindo com seu poder, por meio de Lei, pode punir o homem quando este se enquadrar na violação das normas.

Nesse sentido, afirmam os doutrinadores Copobianco e Santos: a norma jurídica tem o poder para determinar condutas, tolher ações ou responsabilizar omissões. Em natu-

reza específica de Direito Penal, temos a legalidade em sentido estrito, baseado no dispositivo constitucional que afirma não existir crime sem lei que o defina (COPOBIANCO; SANTOS, 2014, p. 26).

A Lei de Introdução ao Código Penal, art. 1º preceitua:

> Considera-se crime a infração penal a que a Lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa, contravenção, a infração penal a que a Lei comina, isoladamente, penas de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente (BRASIL, 1941).

Para não ser desproporcional aos direitos da pessoa acusada, ao ser imposta a nova lei com dispositivo "estupro de vulnerável sem contato físico", o legislador precisará observar o princípio da proporcionalidade, em outras palavras, assevera Lima:

> Por força do princípio da proporcionalidade em sentido estrito, entre os valores em conflito o que demanda a adoção da medida restritiva e o que protege o direito individual a ser violado deve preponderar o de maior relevância. Há de se indagar, pois, se o gravame imposto ao titular do direito fundamental guarda relação de proporcionalidade com a importância do bem jurídico que se pretende tutelar (LIMA, 2016, p. 78).

A Constituição Federal expressa direitos constitucionais em prol do apenado, um deles está no art. 5º, inciso XLVI: "A lei regulará a individualização da pena e adotará, entre outras, as seguintes medidas: a) privação ou restrição de liberdade; b) perda de bens; c) multa; d) prestação social alternativa; e) suspensão ou interdição de direitos" (BRASIL, CF 1988).

O Código de Processo Penal traz a possibilidade da condenação ser cumulada com a reparação indenizatória, é o que descreve o art. 387, inciso IV: "O juiz, ao proferir a sentença condenatória: fixará valor mínimo para a reparação dos danos causados pela infração, considerando os prejuízos sofridos pelo ofendido" (BRASIL, 1941).

Percebe-se, em alguns estados, que a indenização por danos morais à vítima de estupro tem feito parte de muitas sentenças proferidas pelos magistrados:

> A 2ª Câmara Criminal do Tribunal de Justiça do Estado de Goiás (TJGO) condenou um homem a oito anos de reclusão, em regime fechado, por

> constranger uma garota de 09 (nove) anos de idade a praticar sexo oral com ele. O homem também deverá pagar R$ 3 mil à vítima, como indenização por danos morais. O relator do voto foi o desembargador Leandro Crispim. O réu foi enquadrado no artigo 217 do Código Penal, que dispõe sobre os atos libidinosos diversos e conjunção carnal com menores de 14 anos. O colegiado manteve, sem reformas, a sentença proferida pelo juiz auxiliar Pedro Paulo de Oliveira, da 2ª Vara Criminal de Anápolis. [...] Nos crimes de cunho sexual, a palavra da vítima tem relevado valor probante. [...]. Consta da denúncia que o acusado era amigo da família da menina e, como ele tem netos de idades próximas, a garota foi convidada um dia para dormir em sua casa. Num momento em que as outras crianças se afastaram, ele teria se valido da confiança da garota para levá-la a um local afastado e cometer a violência sexual. [...]. Após alguns meses, a criança relatou o acontecido e a mãe procurou uma Delegacia Policial para registrar queixa. [...] O professor da escola também prestou depoimento a respeito do comportamento da menina, que mudou drasticamente após o crime. O desembargador Leandro Crispim ressaltou que "as declarações da vítima, junto às demais provas colacionadas aos autos, constituem elemento probatório suficiente para justificar a condenação" (CURY, 2015).

Não obstante, além de o agressor ter a responsabilidade de indenizar a vítima, estados e municípios têm esse dever quando não cumprem com seu papel de zelar, fiscalizar e promover a segurança da sociedade.

> Em 22/02/2017, a Prefeitura de Uberlândia/MG foi condenada por danos morais e deverá indenizar uma vítima de violência sexual em R$ 30 mil, sujeitos a correções monetárias. A criança era estuprada pelo pai e, mesmo após as denúncias, voltou a morar com o suspeito e continuou sendo abusada. A decisão proferida no mês passado pela Vara da Infância e Juventude da comarca de Uberlândia leva em consideração que o Município foi omisso quanto aos trabalhos desempenhados pelo Conselho Tutelar no acompanhamento da vítima e da família. O promotor de Justiça da Vara da Infância, Epaminondas da Costa, esclareceu que desde 2004 o Conselho Tutelar recebia denúncias de negligência por parte dos pais da criança em relação à higiene e alimentação. [...]. A primeira constatação do estupro de vulnerável ocorreu em 2010, quando a vítima estava com seis anos de idade, durante uma consulta no Hospital de Clínicas da Universidade Federal de Uberlândia (HC-UFU). Ela foi encaminhada para um avô, porém 30

> dias depois o responsável não quis mais cuidar da neta e a devolveu para o pai. "Em hipótese alguma essa criança deveria ter voltado a morar com o pai. Nesse momento era necessária a interferência, o acompanhamento dos conselheiros tutelares e o pedido de destituição do poder familiar", [...]. A segunda denúncia veio à tona um ano e meio depois. Questionada por funcionários da escola sobre o comportamento retraído, a aluna acabou relatando que era violentada pelo pai com frequência. O Conselho Tutelar foi novamente acionado e a vítima, junto ao irmão de oito anos, foi levada para uma instituição de acolhimento da cidade. Ao tomar conhecimento do caso, a Promotoria de Justiça de Defesa dos Direitos da Criança e do Adolescente ingressou com ações pedindo punições aos envolvidos que foram acatadas pelo Judiciário. Além do pedido de destituição dos pais sobre a criança, a Justiça deferiu o pedido de pagamento de pensão alimentícia por parte da mãe e do pai, cujos valores representam 25% do salário mínimo e são depositados em conta judicial no nome da criança. Outro deferimento foi referente à condenação dos pais na esfera criminal. O Ministério Público solicitou que o pai da criança fosse condenado pelo crime de estupro de vulnerável, cuja pena varia de oito a 15 anos de prisão. A mãe da vítima também deveria ser penalizada em caso de comprovação da conivência dela com os abusos. [...]. Por enquanto, os réus respondem em liberdade. O quarto e último pedido da Promotoria foram quanto à responsabilização do Município em virtude da má atuação do Conselho Tutelar em realizar ações protetivas em função da criança, que hoje está adolescente. "Não tenho conhecimento de nenhum outro município brasileiro que foi condenado em casos dessa natureza. A Administração tem o dever de fiscalizar a atuação de seus conselheiros tutelares e esse pedido foi uma forma de alertar os municípios a terem mais cuidado na seleção e fiscalização do trabalho dos conselheiros tutelares. [...]. (ALEIXO, 2017).

Dessa feita, para que o legislador insira no Código Penal uma nova imputação jurídica, como o estupro de vulnerável sem contato físico, seria preciso instituir uma pena um pouco mais branda, como a privação de liberdade e a reparação de forma indenizatória por danos causados à vítima. Devem ser observados pelo magistrado a dosimetria da pena, conforme dispõe o art. 59 do Código Penal, visto que não pode ser injusto com o infrator, e por mais que este tenha abusado do direito de terceiro ele merece ser protegido pelo princípio da dignidade humana.

4.1 A importância da humanização dos julgamentos utilizando o direito como forma de promoção e justiça

A sociedade não está mais acreditando no Poder Judiciário devido à desumanização por parte de alguns magistrados que, ao realizarem julgamentos, violam direitos, ao invés de exercerem seu papel de cumprir a lei, solucionar conflitos com seriedade, igualdade, espírito fraterno, social, e moral. Sendo assim, antes de sobressair ao assunto, faz-se necessário destacar o conceito de Justiça.

Segundo Francisco Mafra (2005), Justiça expressa uma maneira pessoal de perceber e avaliar aquilo que é direito, que é justo. Por justiça pode-se entender um princípio moral pelo qual o respeito ao direito é observado, é o poder de fazer valer o direito de alguém ou de cada um.

No mesmo contexto, declara Croucher: cada ser humano é feito à imagem de Deus. Assim, sustentamos o direito de cada pessoa viver em liberdade, em dignidade, em paz e com saúde,bem como de conhecer e experimentar plenitude de vida (CROUCHER, 1989, p. 15).

De todo modo, para que todos tenham essa vida plena, os representantes do povo, ao elaborarem projetos de lei, precisam observar que os projetos devem atender ao bem-estar social, e não ferir direitos e garantias fundamentais, que por sinal são princípios constitucionais para proteger a vida do homem, conforme preleciona a Constituição Federal em seu art. 3º:

> Constituem objetivos fundamentais da República Federativa do Brasil: I – Construir uma sociedade livre, justa e solidária; II – Garantir o desenvolvimento nacional; III – Erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; IV – Promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. (BRASIL, CF 1988).

Além disso, afirma um grupo de juristas:

> O fundamento desses direitos, a sua razão de ser está na própria viabilidade da existência do ser humano, uma existência assegurada em todas as suas dimensões, garantida através do oferecimento de condições essenciais

> e inerentes à pessoa, tais como a vida, a liberdade de expressão, o trabalho, a saúde, a alimentação, a moradia, a educação e ao meio ambiente preservado. A nossa Constituição Federal de 1988 é um marco na história dos direitos humanos no Brasil, porque nela podemos encontrar praticamente todas as gerações de direitos fundamentais reconhecidas nas normas do direito internacional. (AATR-BA, 2002, p. 3-11).

Por outro lado, se o Judiciário entender que, em determinado caso, não existe uma lei justa para solucionar tal conflito, o juiz, apesar de não poder julgar com seus próprios convencimentos, mas com fundamentos legais, deverá agir com espírito humano, ético, moral e social em respeito à dignidade humana.

Nessa esteira, Carlos Sánchez Viamonte (MORAES, 1998, p. 52) reitera o ofício da Justiça:

> [...] sua função não consiste somente em administrar a Justiça, pura e simplesmente, sendo mais, pois seu mister é ser o verdadeiro guardião da Constituição,com a finalidade de preservar os direitos humanos fundamentais, mais especificamente, os princípios da legalidade e igualdade, sem os quais os demais tornariam-se vazios (VIAMONTE apud MORAES, 1998).

Com efeito, declara Monica Rodrigues Moraes sobre os efeitos positivos que a sociedade terá com a humanização da Justiça:

> Com a humanização da Justiça, as decisões judiciais certamente buscarão a efetiva justiça porque devem levar em conta não apenas o texto da lei, mas também as condições sociais dos envolvidos, e, serão sempre fundamentadas na Paz e direcionadas à busca da Paz e justiça social, pois, vale registrar que atualmente, a paz logrou a dignidade teórica de um direito, foi elevada à categoria de direito positivo, sendo o mais verdadeiro axioma da democracia. (MORAES, 2008).

Desse modo, a decisão do Superior Tribunal de Justiça em condenar o réu pela prática de estupro de vulnerável sem contato físico foi importante para humanizar os julgamentos, visto que esse tipo de decisão foi a primeira a ser realizada no Brasil.

O Egrégio Tribunal foi além dos seus limites em trazer para o mundo jurídico um fato que ainda está em abstrato, ou seja, um a dois doutrinadores discutem o assunto que

não possui imputação jurídica, e ainda por não ser do conhecimento da sociedade. Enquanto isso não ocorre, o ideal é que todo operador do Direito tenha o bom senso em contribuir para uma sociedade com a humanização dos julgamentos, utilizando seus conhecimentos jurídicos como forma de promoção e justiça. Retirando do papel os direitos humanos e garantias fundamentais como um dever social a ser aplicado na vida prática de cada indivíduo, estando ela em situação de vulnerabilidade ou não.

4.2 Possibilidade de imputar o fato como crime em benefício da sociedade

A todo instante existem ao nosso redor pessoas, vítimas dessa barbaridade, mas infelizmente muitos casos chegam a ficar impunes devido à morosidade da Justiça ou até mesmo por decisão da própria vítima que tem medo do que possa ocorrer após a denúncia. E assim suportamo sofrimento ao longo da vida. Em uma das pesquisas, realizada pelas pesquisadoras citadas a seguir, foi comprovado que esses tipos de violências ficam gravados na memória, o estrago emocional pode até mesmo comprometer o futuro dessas pessoas. É o que relata Taciana Feitosa de Melo, Anaysa Câmara de Souza, Isabella Queiroga R. Floering e Lucilayne Maria da Silva (2015):

> As vítimas de abuso podem ser afetadas de diferentes formas, ou seja, enquanto algumas apresentam efeitos mínimos, outras desenvolvem severos problemas de ordem emocional, social e psiquiátrica. O impacto vai depender de fatores intrínsecos (vulnerabilidade e resiliência) e extrínsecos à criança (recursos sociais e emocionais, funcionamento familiar, condições financeiras. Este tipo de maus-tratos traz às suas vítimas consequências negativas ao longo do seu desenvolvimento cognitivo, comportamental, afetivo e social, (MELO et al., 2015).

À vista disso, imputar como crime o fato "estupro de vulnerável sem contato físico" será para a sociedade um grito de vitória. Isso é perceptível por meio do resultado de enquete realizada pela pesquisadora, no dia 25 de maio de 2017, em que 84,4% dos que votaram afirmaram ser a favor da imputação jurídica (FERENDUM, 2017).

No mesmo campo, segundo a participação da comentarista Wanna Paula Barros: “Com certeza trará benefícios para a sociedade, pois, mesmo sem nenhum contato físico, a criança é frágil, e, com isso ela estará mais protegida. O estuprador consegue

deixar uma criança fragilizada com o olhar, com gestos sem a necessidade de toque" (BARROS, 2017).

Em entrevista com o delegado titular da Delegacia de Proteção à Criança e ao Adolescente, Dr. Lorenzo Pazolini (informação verbal)[2], para saber sobre seu posicionamento a respeito do caso em estudo, este afirmou:

> [...] sem dúvida nenhuma é possível imputar como crime estupro de vulnerável sem contato físico, considerando salutar, porque, sobretudo se forem analisar os reflexos constitucionais, o art. 227, CF traz a proteção da criança e do adolescente e do estatuto, o qual tudo que está na Constituição foi replicado no ECRIAD, considerando ser a hipossuficiência em grau máximo. Não há dúvida nenhuma que o legislador pretendeu preencher os requisitos subjetivos, o que tem que quebrar o o dogma desse contato porque durante muito tempo as condenações se baseavam nesse contato, e hoje, claro, por exemplo, eu pensei em outro caso aqui, o autor que induz a prática dos atos sexuais, por exemplo, ele pede para a vítima se masturbar na frente dele e com contraprestação ou não, sendo a vítima, menor de 14 anos, esse caso nós já tivemos aqui no DPCA, não envolvendo pagamento, contraprestação onerosa, prostituição, exploração de terceiro; no nosso caso aconteceu o seguinte, a pessoa não tinha relação sexual com conjunção carnal, coito anal e nem toque, mas ele induzia a vítima a ser masturbar na frente dela e a vítima era menor de 14 anos, o qual se enquadraria como estupro de vulnerável, pois se tem a presunção legal, menor de 14 anos e indícios de atos libidinosos diversos da conjunção carnal, é considerado estupro de vulnerável (PAZOLINI, 2017).

O advogado, mestre em Direitos e Garantias Fundamentais, Dr. Paulo Sérgio Rizzo, em entrevista (via *e-mail*) esclareceu ser a favor do combate à referida conduta, que certamente terá um retorno à sociedade na proteção dos direitos humanos (RIZZO, 2017).

Dessarte, autoridades do ramo jurídico e da sociedade estão em consonância com parte dos doutrinadores no sentido de imputar o fato como crime.

2 Entrevista concedida por Lorenzo Pazolini, delegado titular da DPCA, a Fabiana Almeida de Jesus em 31 de maio de 2017.

5 Considerações Finais

Durante o processo de pesquisa, observou-se que tribunais, autoridades jurídicas, assim como operadores do Direito terão que enfrentar grandes desafios concernentes ao tema pesquisado, pois, se futuramente passarem a entender que o fato se enquadra como crime de estupro de vulnerável sem contato físico, será muito difícil para a sociedade captar esse novo conceito de delito. Outro desafio é não existir legislação sobre o assunto.

Na doutrina majoritária há pouco respaldo, porém, em prol da dignidade da pessoa humana, é necessário mudar a legislação, em especial o art. 217-A, sobre essa cultura do estupro, que para a sociedade só é caracterizado se houver contato físico entre vítima e agressor.

A violência sexual ocorre em todos os ambientes, mas definir essa caracterização na prática é difícil, pois muitos podem confundir com o princípio *bis in idem*, porém, levando em consideração a proteção humana, na prática, a dignidade sexual tem sido violada. A sociedade não sabe distinguir o que pode ser considerado estupro de fato, mas tão somente aquilo que está expresso como crime na legislação penal e o que é informado todos os dias nos noticiários.

Assim, constatou-se durante a pesquisa que todas as pessoas são consideradas vulneráveis, ao contrário daquele rol taxativo previsto no art. 217-A, pois, quando violentada, sofre traumas físicos e psicológicos, e dessa maneira sua dignidade humana, dignidade sexual e os princípios constitucionais são brutalmente violados.

Em vista dos argumentos apresentados, é primordial a atualização da legislação penal em respeito à Carta Magna, uma vez que o Superior Tribunal de Justiça já decidiu favoravelmente sobre o assunto, assim, como as autoridades que fazem parte do meio jurídico, no estado do Espírito Santo.

De todo o exposto, conclui-se que a possibilidade jurídica de imputar como crime o estupro de vulnerável sem contato físico trará segurança jurídica para toda a sociedade, principalmente, às vítimas. No entanto, é importante ressaltar que essa imputação jurídica não poderá de maneira alguma ferir a integridade física do agente violentador, e deverá ser levada em consideração com todos os princípios constitucionais e penais. Sendo assim, ambos terão sua dignidade humana preservada.

Referências

ASSOCIAÇÃO DE ADVOGADOS DE TRABALHADORES RURAIS NO ESTADO DA BAHIA – AATR-BA. **Direitos Humanos Fundamentais**. 2002. p. 3-11. Disponível em: <http://www.dhnet.org.br/dados/cursos/aatr/a_pdf/01_aatr_dh_fundamentais.pdf>. Acesso em: 10 maio 2017.

AGRESSÃO emocional: Estupro de vulnerável não exige contato físico entre agressor e vítima. **Revista eletrônica Consultor Jurídico**, São Paulo, 4 ago. 2016, 14h01m. Disponível em: <http://www.conjur.com.br/2016-ago-04/estupro-vulneravel-nao-exige-contato-entre-agressor-vitima>. Acesso em: 17 nov. 2016.

ALEIXO, Caroline. **Município é condenado a indenizar criança violentada pelo pai em MG**. G1 on-line, Minas Gerais, 22 fev. 2017 às 13h08m. Disponível em: <http://g1.globo.com/minas-gerais/triangulo-mineiro/noticia/2017/02/municipio-econdenado-indenizar-crianca-violentada-pelo-pai-em-mg.html>. Acesso em: 8 maio 2017.

BARROS, Wanna Paula. **Comentário participativo à enquete Possibilidade de imputar como crime a prática de estupro de vulnerável sem contato físico em benefício da sociedade**. 25 maio 2017. Disponível em: <http://www.ferendum.com/pt/PID74117PSD 64993>. Pesquisa encerrada em: 26 maio 2017, às 17h59m.

BINTECOURT, Cezar Roberto. **Tratado de Direito Penal**: Parte Especial 2 – Dos crimes contra a pessoa. 6. ed. rev. e ampl. São Paulo: Saraiva, 2012.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial [da] República Federativa do Brasil**, Rio de Janeiro, DF, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm>.

_____. Decreto-lei nº 3.914, de 9 de dezembro de 1941. Lei de introdução do Código Penal (decreto-lei n. 2.848, de 7-12-940) e da Lei das Contravenções Penais (decreto-lei n. 3.688, de 3 outubro de 1941). **Diário Oficial [da] República Federativa do Brasil**, Rio de Janeiro, DF, 9 dez. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm>.

_____. Decreto-lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Diário Oficial [da] República Federativa do Brasil**, Rio de Janeiro, DF, 13 out. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>.

_____. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

_____. Lei nº 10.406, 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 11. jan. 2002. Disponível em: <http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm>.

_____. Lei nº 10.741, 1º de outubro de 2003. Dispõe sobre o Estatuto do Idoso e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 3 out. 2003. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm>. Acesso em: 15 mai. 2017.

_____. Lei nº 11.340, de 7 de agosto de 2006. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8o do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal; e dá outras providências. **Vade Mecum Saraiva**: edição federal, 23. ed. São Paulo: Saraiva, 2017.

_____. Lei nº 12.015, de 7 de agosto de 2009. Altera o Título VI da Parte Especial do Decreto-Lei no 2.848, de 07 de dezembro de 1940 – Código Penal, e o art. 1º da Lei no 8.072, de 25 de julho de 1990, que dispõe sobre os crimes hediondos, nos termos do inciso XLIII do art. 5º da Constituição Federal e revoga a Lei no 2.252, de 1o de julho de 1954, que trata de corrupção de menores. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 10 ago. 2009. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12015.htm>. Acesso em: 15 mar. 2017.

_____. Lei nº 13.104, de 9 de março de 2015. Altera o art. 121 do Decreto-Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal, para prever o feminicídio como circunstância qualificadora do crime de homicídio, e o art. 1º da Lei nº 8.072, de 25 de julho de 1990, para incluir o feminicídio no rol dos crimes hediondos. **Diário Oficial [da] República**

Federativa do Brasil, Brasília, DF, 3 mar. 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/lei/L13104.htm>. Acesso em: 15 mai. 2017.

_____. Superior Tribunal de Justiça. **Súmula nº 593**. O crime de estupro de vulnerável configura-se com a conjunção carnal ou prática de ato libidinoso com menor de 14 anos, sendo irrelevante o eventual consentimento da vítima para a prática do ato, experiência sexual anterior ou existência de relacionamento amoroso com o agente. Terceira Seção, julgado em 25 out. 2017, Dje 6 de nov. de 2017. Disponível em: <http://www.stj.jus.br/SCON/sumanot/toc.jsp>. Acesso em: 3 nov. 2017.

CAPEZ, Fernando. **Curso de Direito Penal**. 17. ed. São Paulo: Saraiva, 2013. v. 1.

CASTRO, Leonardo. **Legislação Comentada**: artigo 213 do Código Penal – estupro. In: JUSBRASIL, publicado em 12 jan. de 2014, às 00h:28m: 30s. Disponível em: <https://leonardocastro2.jusbrasil.com.br/artigos/121943503/legislacao-comentada-artigo-213-do-cp-estu pro>. Acesso em: 7 abr. 2017.

CONJUR. Lei Maria da Penha é aplicada para proteger homem. **Revista Consultor Jurídico**. São Paulo, 30 out. 2008, 16h05m. Disponível em: <http://www.conjur.com.br/2008-out-30/lei_maria_penha_aplicada_proteger_homem>. Acesso em: 5 abr. 2017.

COPOBIANCO, Rodrigo Julio; SANTOS, Vauledir Ribeiro (Coord.). **Como se preparar para o exame de Ordem**: Direito Penal. 11. ed. Rio de Janeiro: Forense; São Paulo: Método, 2014. v. 5.

CROUCHER, Rowland. **Justiça e espiritualidade**: em busca de uma vida cristã criativa. Belo Horizonte: Missão Editora, 1989. (Coleção Justiça e Espiritualidade I).

CURY, Lilian. Confirmada condenação e indenização por estupro de vulnerável. **Notícias do TJGO**: Centro de Comunicação Social do TJGO, 25 fev. 2015, 13h15m. Disponível em: <http://tjgo.jus.br/index.php/home/imprensa/noticias/119-tribunal/8702-condenado-estupro-vulneravel>. Acesso em: 5 maio 2017.

CUNHA, Rogério Sanches. **Manual de direito penal**: parte especial (arts. 121-361). 8. ed. rev., amp. e atual. Salvador: JUSPODIVM, 2016.

DELMANTO, Celso; DELMANTO, Roberto; JUNIOR, Roberto Delmanto; DELMANTO. Fábio M. de Almeida. **Código Penal Comentado**: Legislação Complementar. 6. ed. atual. e ampl. Rio de Janeiro: Renovar, 2002.

DESCLASSIFICAÇÃO DO CRIME DE ESTUPRO DE VULNERÁVEL: mero toque corporal. **Informativo Tribunal de Justiça Distrito Federal e Territórios**. DJE: 3 jun. 2014. Disponível em: <http://www.tjdft.jus.br/institucional/jurisprudencia/informativos/2014/informativo-de-jurisprudencia-n-o-284/desclassificacao-do-crime-de-estupro-de-vulneravel-2013-mero-toque-corporal>. Acesso em: 18 maio 2017.

FERENDUM. **Enquete**: Possibilidade de imputar como crime a prática de estupro de vulnerável sem contato físico em benefício da sociedade. 25 de maio 2017. Disponível em: < http://www.ferendum.com/pt/PID74117PSD64993>. Pesquisa encerrada dia: 26 maio 2017, às 17h59m.

GESSE, Claudia Maria Camargo. **As consequências físicas e psíquicas da violência no crime de estupro e no de atentado violento ao pudor**. 63f. (Trabalho de Conclusão de Curso Bacharel em Direito) – Faculdades Integradas Antonio Eufrásio de Toledo de Presidente Prudente, São Paulo, 2008. Disponível em: <http://intertemas.toledoprudente.edu.br/revista/index.php/ETIC/article/viewFile/1669/1595>. Acesso em: 16 maio 2017.

GONÇALVES, Victor Eduardo Rios; LENZA, Pedro (Coord.). **Direito Penal Esquematizado**: Parte Especial. 6. ed. São Paulo: Saraiva, 2016. (Coleção Direito esquematizado).

GRECO, Rogério. **Curso de Direito Penal**: Parte especial. 10. ed. Rio de Janeiro: Impetus, 2013. v. 3.

GUIMARÃES, Deocleciano Torrieri. **Dicionário Universitário Jurídico**. 17. ed. São Paulo: Rideel, 2013.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**. 4. ed., rev., ampl. e atual. Salvador: Ed. JusPODIVM, 2016.

MAFRA, Francisco. O Direito e a Justiça. **Âmbito Jurídico**. Rio Grande, n. 20, fev. 2005. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista _artigos_leitura&artigo_id=870>. Acesso em: maio 2017.

MASSON, Cleber Rogério. **Direito Penal Esquematizado**: parte especial. 7. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: Método, 2011.

MARQUES, Fabiano Lepre. A dignidade humana: uma análise hermenêutica de seus contornos. In: ENCONTRO NACIONAL DO CONPEDI, 20., 2011,Vitória. **Anais...** Florianópolis: Boiteux, 2011.

MORAES, Alexandre de. **Direitos Humanos Fundamentais**: teoria geral, comentários aos arts. 1º- 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. São Paulo: Atlas, 1998. v. 3. (Coleção Temas Jurídicos).

MORAES. Maria Celina Bodin de (Coord). **Princípios do Direito Civil Contemporâneo**. Rio de Janeiro: Renovar, 2006. Disponível em: <https://www.researchgate.net/publication/ 28770373_Principios_do_direito_civil_contemporaneo>. Acesso em: 17 mai. 2017.

MORAES, Monica Rodrigues Campos. **Humanização da Justiça**: uma abordagem conceitual. Jurisway Sistema Educacional on-line. Publicado em: 11 mar. 2008. Disponível em: <https://www.jurisway.org.br/v2/dhall.asp?id_dh=576>. Acesso em: 10 maio 2017.

MARTINS, Jomar. Namoro Precoce: Consentimento da família afasta tipificação de estupro de vulnerável. **Revista Consultor Jurídico**. São Paulo, 6 maio 2017, 07h51m. Disponível em: <http://www.conjur.com.br/2017-mai-06/consentimento-familia-afasta-tipificacao-estupro-vulneravel#author>. Disponível em: <http://s.conjur.com.br/dl/acordao-modificado-6a-camara-criminal.pdf>. Acesso em: 15 maio 2017.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**: parte geral e parte especial. 9. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2013.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Declaração Universal dos Direitos Humanos**. Disponível em: <http://www.mp.go.gov.br/portalweb/hp/7/docs/declaracao_universal _dos_direitos_do_homem.pdf>. Acesso em: 17 mar. 2017.

PINHO, Rodrigo César Rebello. **Teoria Geral da Constituição e Direitos Fundamentais**. 6. ed. São Paulo: Saraiva, 2006. v. 17.

PRADO, Luiz Regis; CARVALHO, Érika Mendes de; CARVALHO, Gisele Mendes de. **Curso de Direito Penal Brasileiro**: parte geral, parte especial. 13. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014.

RIZZO, Paulo Sérgio. **Entrevista com Paulo Sérgio Rizzo**. Advogado e consultor jurídico, Professor universitário, Mestre em direitos e garantias constitucionais fundamentais. 1 jun. 2017. Entrevista concedida a Fabiana Almeida de Jesus, por meio do e-mail: fabianadireitodejesus@gmail.com.

SANTOS, Washington dos. **Dicionário jurídico brasileiro**: terminologia jurídica, com algumas notas, observações e comentários,brocardos latinos (jurídicos e forenses). Belo Horizonte: Del Rey, 2001.

SCHULTZ, Célia. O homem é lobo do homem. **Blog Filosofia em Casa**. São Paulo, 27 de dez. 2007 às 6h49m. Disponível em: <http://auladefilosofiacelia.blogspot.com.br/2007/12/thomas-hobbes-o-homem-o-lobo-do-homem.html>. Acesso em: 4 mar. 2017.

SILVA, Henrique Salmazo; SILVA, Thais Bento Lima. **Vulnerabilidade e aspectos biopsicossociais e velhice, Revista Temática Kairós Gerontologia**, São Paulo, dez. 2012., p. 1-5. ISSN 1516-2567. Disponível em <https://revistas.pucsp.br/index.php/kairos/article/viewFile/ 17289/12829>. Acesso em: 15 mar. 2017.

12 PROJETO "MINISTÉRIO PÚBLICO PELA EDUCAÇÃO DIGITAL NAS ESCOLAS"

Neide M. C. Cardoso de Oliveira[1]
Marcia Morgado[2]

Resumo: O projeto "Ministério Público pela Educação Digital nas Escolas", elaborado pelo Ministério Público Federal em parceria com a ONG SaferNet Brasil, busca, por meio da educação, proporcionar que crianças e adolescentes se tornem cidadãos conscientes de seus direitos e deveres no uso da internet, a fim de que cresçam sabendo se prevenir de eventuais crimes no ambiente virtual, assim como evitar que sejam futuros agressores. Mostrar como surgiu o embrião do projeto e como ele se desenvolveu no ambiente ministerial visa incentivar ideias simples e inovadoras dentro da Instituição, que, para além de órgão de persecução penal, deve se preocupar com a prevenção de crimes, entre eles, os cibernéticos.

Palavras-chave: Projeto. Educação. Crianças e adolescentes. Instituição. Prevenção. Crimes cibernéticos.

Abstract: *The project "Prosecution Service in favor of Digital Education in Schools", prepared by the Federal Prosecution Service in partnership with the NGO SaferNet Brazil, seeks, through education, to provide children and adolescents with citizen awareness of their rights and duties in the use of the Internet, so that they grow knowing how to prevent possible crimes in the virtual environment, as well as prevent them from being future aggressors. Showing how the project's archetype emerged and how it developed in the prosecution environment aims to encourage simple and innovative ideas within the institution, which, besides being a criminal prosecution service, should be concerned with crime prevention, including cybernetics.*

Keywords: Project. Education. Children and adolescents. Prevent. Institution. Cybercrimes.

1 Procuradora Regional da República da PRR da 2ª Região. Membro do Núcleo de Combate à Corrupção da PRR2. Coordenadora do Grupo de Apoio no Combate aos Crimes Cibernéticos da 2ª Câmara de Coordenação e Revisão (matéria criminal) do MPF. Coordenadora do Projeto "Ministério Público pela Educação Digital nas Escolas". Especialista em Direitos Humanos pela UFRJ.

2 Procuradora Regional da República da PRR da 2ª Região. Coordenadora do Projeto "Ministério Público pela Educação Digital nas Escolas". Membro do GT Comunicação Social da PFDC. Membro do GT Inclusão para pessoas com deficiência da PFDC. Membro do GT Criança e Adolescente da PFDC. Coordenadora do Núcleo de Apoio Operacional – NAOP da PRR da 2ª Região. Membro titular da Copeij (Comissão Permanente da Infância e da Juventude) do GNDH (Grupo Nacional dos Direitos Humanos) do CNPG (Conselho Nacional dos Procuradores Gerais).

1 Histórico

Qualquer pessoa, em qualquer lugar do mundo, desde que conectada à rede mundial de computadores – internet, o mais poderoso meio de comunicação da atualidade – pode acessar o conteúdo de páginas publicadas por um criminoso. E, como é cada vez mais precoce o uso da rede, as crianças e os adolescentes, dada a sua maior vulnerabilidade, ficam expostos ao assédio de pessoas que utilizam o mundo virtual para a prática de ilícitos.

De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE), metade dos brasileiros estão conectados à rede mundial, ou seja, aproximadamente 107 (cento e sete) milhões de pessoas, colocando o Brasil como o quinto país do mundo em número de usuários de internet[3].

O Brasil é um dos quatro maiores polos de divulgação de pornografia infantil do mundo, concorrendo com os EUA, a Coreia do Sul e a Rússia (ONG *Rainbow Phone*)[4]. Nesse quadro assustador, a internet é um facilitador do contato entre os criminosos (a maioria, pedófilos), possibilitando-os de se organizarem em comunidades virtuais, trocando informações, fotos e vídeos.

Uma vez postados os mais diversos conteúdos na rede, tais como dados pessoais, informações e fotos, perde-se o total controle sobre a sua destinação. O conselho, que outrora ouvíamos como "pense antes de falar", deve ser adaptado, nos dias de hoje, para "pense antes de postar", justamente porque qualquer conteúdo, uma vez colocado na internet, pode ser visto por qualquer pessoa no mundo, reproduzido e até maliciosamente modificado quantas vezes se puder imaginar.

O Ministério Público Federal, diante da moderna criminalidade que ocorre por meios virtuais, associada à universalização da internet no País e, em consonância com a ratificação pelo Brasil da Convenção dos Direitos da Criança (ONU) e da Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial[5], criou, em 2003 e 2006, respectivamente, nas Procuradorias da República nos Estados de São Paulo e do Rio de Janeiro, grupos de trabalho especializados no combate aos crimes cibernéticos.

3 Segundo o IBGE, um em cada dez domicílios brasileiros com conexão à internet, acessam a rede por meio de celular ou *tablet*. Segundo o órgão, 85,6 milhões de brasileiros acima de 10 anos de idade (49,4% da população) tinham usado a internet, pelo menos uma vez, no período de referência dos últimos três meses (últimos 90 dias que antecederam o dia da entrevista) em 2013.

4 Fonte: Disponível em: <http://www.safernet.org.br/site/noticias/mpf-safernet-assinam-termo-para-prevenir-crimes-internet-0>.

5 Ratificada pelo Brasil em 24 de setembro de 1990 – Decreto nº 99.710, de 21 de novembro de 1990 e ratificada em 27 de março de 1968 – Decreto nº 65.810, de 8 de dezembro de 1969, respectivamente.

Tais grupos são integrados por procuradores da República, que recebem a distribuição de processos, notícias de fatos e inquéritos policiais relacionados aos crimes referentes à divulgação de pornografia infantojuvenil e racismo na internet.

A preocupação com a navegação segura no mundo virtual surgiu como consequência dos trabalhos de investigação de crimes realizados pelo Núcleo Técnico de Crimes Cibernéticos da Procuradoria da República de São Paulo[6]. Percebeu-se que muitas pessoas eram – e são – vitimadas por desconhecimento de medidas de segurança básicas e cuidados simples.

Por entender que só a repressão é insuficiente e que a prevenção é o melhor caminho a seguir na conscientização das pessoas, em especial das crianças e dos adolescentes, principais vítimas desses delitos, as Procuradorias da República nos Estados de São Paulo e Rio de Janeiro, por incentivo de seus aludidos grupos especializados de combate a crimes cibernéticos, firmaram convênios com a Organização Não Governamental SaferNet Brasil[7] [8], para atuação conjunta na área de prevenção a tais crimes. Assim, o Ministério Público Federal começou a promover, em parceria com a referida ONG, desde 2009, na sede da Procuradoria da República em São Paulo e, a partir de 2010, também na sede da Procuradoria da República no Estado do Rio de Janeiro, as Oficinas denominadas "*Promovendo o uso responsável e seguro na internet*", destinadas aos professores das redes pública e privada de ensino nos respectivos estados. Essa iniciativa ocorreu, à época, também nas Procuradorias da República em João Pessoa, na Paraíba; em Manaus, no Amazonas; em Belém, no Pará e em Fortaleza, no Ceará.

A primeira Oficina foi realizada pela Procuradoria da República em São Paulo[9], por intermédio do seu Grupo de Combate a Crimes Cibernéticos, no Dia da Internet Segura, em 2009. O *Safer Internet Day* – que costuma ocorrer no dia 9 de fevereiro – é uma iniciativa mundial da ONG *InHope*[10] e do Conselho da Europa, que objetiva divulgar práticas de navegação segura na internet em diversos países do mundo. Como um dos eventos

6 Criado pela Portaria PR/SP n. 500, de 6 de março de 2010.

7 ONG SaferNet Brasil é uma associação civil sem fins lucrativos e econômicos, sem vinculação político partidária, religiosa ou racial, fundada em 20 de dezembro de 2005, por um grupo formado por cientistas da computação, professores universitários, pesquisadores e bacharéis em Direito. Oferece um serviço de recebimento de denúncias anônimas de crimes e violações de direitos humanos na internet, assim como oferece um help desk com apoio psicológico para apoio a vítimas de delitos cibernéticos.

8 Termo de Mútua Cooperação Técnica, Científica e Operacional entre a ONG SaferNet Brasil e as Procuradoria da República no Estado de São Paulo, em 29 de março de 2006 e Procuradoria da República no Estado do Rio de Janeiro, em 13 de novembro de 2006. Também firmados com as Procuradorias da República no Estado do Rio Grande do Sul, em 25 de outubro de 2006; no Estado de Goiás, em 12 de março de 2007 e no Estado do Paraná, em 14 de junho de 2007.

9 Disponível em: <http://www.prsp.mpf.gov.br/>.

10 Disponível em: <https://www.saferinternetday.org/> e <http://www.inhope.org/gns/home.aspx>.

para divulgação da data e conscientização quanto ao tema, foi realizada palestra na Secretaria de Educação do Estado de São Paulo, em parceria com a ONG SaferNet Brasil, por meio de seu diretor de educação, o psicólogo e educador, Rodrigo Nejm, a qual foi presenciada por dezenas de professores e transmitida ao vivo, via rede, para centenas de outros professores de várias escolas do estado de São Paulo.

A partir dessa primeira experiência, iniciou-se um ciclo periódico de oficinas "*Promovendo o Uso Responsável e Seguro da Internet*"[11], nas quais foram realizadas palestras na sede da Procuradoria da República em São Paulo, dirigidas aos coordenadores e professores das redes pública e privada de ensino, que receberam, também, material didático e treinamento para serem multiplicadores do aprendizado.

As palestras ficavam disponíveis na internet e eram de uso livre por qualquer interessado. Também foi disponibilizado treinamento com material desenvolvido pela ONG SaferNet Brasil, com sugestões de atividades pedagógicas para abordagem do assunto em sala de aula, a fim de que os professores dispusessem de meios para levar o que aprenderam à sua unidade escolar.

No Rio de Janeiro, a primeira oficina foi realizada em 18 de maio de 2010 e baseou-se em uma pesquisa realizada pela ONG SaferNet Brasil naquela cidade, sobre os riscos e hábitos on-line com 514 estudantes fluminenses de 10 a 17 anos[12], e constatou-se que:

64% vão para as *lan houses* acessar a internet;
34,14% ficam mais de 3 horas diárias navegando na internet;
as atividades preferidas são sites de relacionamento (74,12%) e jogos (51,56%);
47% dizem que os pais não impõem limites para navegação;
57,2% se consideram mais habilidosos com a web do que os pais;
48% dizem ter mais de 30 amigos virtuais (conhecidos apenas pela internet);
16,5% dos alunos admitem já ter publicado fotos suas íntimas na internet;
29,77% dos participantes têm um amigo que já sofreu cyberbullying ao menos uma vez.

Em 2011, ocorreu a entrega, com sucesso, de material pedagógico para todas as escolas da rede municipal de ensino da cidade do Rio de Janeiro, que contava, à época,

11 Foram realizadas cinco oficinas "Internet Segura" na PR/SP no ano de 2009, nos meses de abril, maio, junho, agosto e outubro, bem como uma palestra no ano de 2011. Além dessas atividades, foram realizados três debates no "Safer Internet Day", na Secretaria de Educação, em 2009; no Comitê Gestor de Internet, em 2010; e na Procuradoria Regional da República da 3ª Região, em 2012.

12 Pesquisa constante no site da safernet.org.br.

com 1.080 (mil e oitenta) unidades escolares[13]. Em 2012, foi realizada uma oficina, desta vez em parceria com o Ministério Público do Estado do Rio de Janeiro, destinada aos conselheiros tutelares – que têm contato direto com as crianças e os adolescentes em seus lares e são ouvintes/testemunhas de inúmeros casos de abuso infantojuvenil, praticados também por meio da internet. A participação dos conselheiros tutelares na oficina visou capacitá-los para identificar e para lidar com o tema com criança/adolescente e seus familiares, bem como para denunciar eventual notícia de crime sofrido por criança ou adolescente no meio virtual.

2 Projeto

Diante do sucesso da experiência nos estados de São Paulo e Rio de Janeiro, as subscritoras deste artigo, com o apoio da Procuradoria Federal dos Direitos do Cidadão e das 2ª e 3ª Câmaras de Coordenação e Revisão do Ministério Público Federal, submeteram à Procuradoria Geral da República a ideia de expandir a realização das oficinas para todo o Brasil, surgindo, em decorrência, o Projeto "Ministério Público pela Educação Digital nas Escolas", aprovado no âmbito da Instituição, por meio da Portaria PGR/MPF nº 753/2015.

O mencionado Projeto, realizado pelo Ministério Público Federal em parceria com a Organização Não Governamental SaferNet Brasil e o Comitê Gestor da Internet no Brasil (CGI.br)[14], é coordenado pela Procuradoria Federal dos Direitos do Cidadão (PFDC), por meio do Grupo de Trabalho Comunicação Social – com auxílio do Grupo de Apoio no Combate aos Crimes Cibernéticos (2ª Câmara de Coordenação e Revisão do MPF) e do Grupo de Trabalho Tecnologia da Informação e Comunicação (3ª Câmara de Coordenação e Revisão do MPF) – e tem por objetivo contribuir para a capacitação de educadores no tema, formando agentes multiplicadores em instituições públicas e privadas de ensino.

O Grupo de Trabalho Comunicação Social da Procuradoria Federal dos Direitos do Cidadão tem por objetivo

13 Disponível em: <http://rioeducaideias.blogspot.com.br/2011/09/safernet-entrega-1080-kits-para-as.html>.

14 O Comitê Gestor da Internet no Brasil tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (Internet Protocol) e administração pertinente ao Domínio de Primeiro Nível ".br". Também promove estudos e recomenda procedimentos para a segurança da internet e propõe programas de pesquisa e desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no uso da internet (Decreto nº 4.829, de 3 de setembro de 2003).

> promover e garantir o respeito aos princípios da comunicação social delineados no capítulo V da Constituição Federal de 1988, por meio de constantes debates entre sociedade civil, setor privado e poder público, a fim de elaborar subsídios fundamentados e traçar metas para atuação dos membros do Ministério Público Federal no tema. Com isso, pretende-se que as diversas plataformas da comunicação pública no Brasil sejam ambientes de respeito e promoção dos direitos humanos, especialmente aqueles inerentes ao cidadão em situação de vulnerabilidade[15].

O Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão do Ministério Público Federal (temática criminal) é responsável por buscar implementar uma política institucional de atuação e capacitação para os membros voltada para a efetiva repressão aos crimes cibernéticos. Visa, entre outros objetivos, ao aprimoramento no que diz respeito ao enfrentamento a esses crimes, por meio de cursos de treinamento para novos procuradores (Curso de Ingresso e Vitaliciamento)[16]; bem como para os membros já integrantes na carreira[17], abrangendo também membros da magistratura federal[18].

Uma importante atribuição desse grupo vem a ser o acompanhamento da legislação nacional e internacional sobre o tema, com apresentação de Notas Técnicas[19]; organização e atualização do "Roteiro de Atuação sobre Crimes Cibernéticos", distribuído para o MPF e Judiciário Federal; bem como a representação internacional (em diversos eventos) e nacional do grupo (CGI.br e grupos de discussão on-line sobre crimes cibernéticos)[20].

O Grupo de Trabalho Tecnologias da Informação e da Comunicação da 3ª Câmara de Coordenação e Revisão do MPF (temática Consumidor e Ordem Econômica) tem por objeto os aspectos diversos das tecnologias modernas, como proteção de dados pes-

15 Disponível em: <pfdc.pgr.mpf.mp.br/insittucional/grupos-de-trabalho/gts>.

16 Em 2012, 2013, 2014 e 2015, com o curso sobre a "Atuação do MPF no Combate aos Crimes Cibernéticos", ministrado pelas procuradoras da República, Melissa Blagitz, Fernanda Domingos e Priscila Schreiner.

17 Cursos organizados pela Escola Superior do Ministério Público da União (ESMPU), em 2012, 2013, 2014 e 2015.

18 Curso "**Os crimes cibernéticos e a atuação do Ministério Público Federal, do Judiciário Federal e da Polícia Federal**", realizado na PR/SP, de 20 a 22 de outubro de 2015, promovido pela Escola Superior do Ministério Público da União. E a palestra – "Os Aspectos Internacionais no Combate ao Crime Cibernéticos", ministrada pela procuradora regional da República, Neide Cardoso e o professor Carlos Affonso de Souza, organizada pela Emarf/RJ, em 14 de agosto de 2015.

19 Notas Técnicas nº 1, sobre o regulamento do Marco Civil da Internet e nº 2, sobre o projeto Internet.org e o princípio da neutralidade da rede, elaboradas em conjunto com o GT de Tecnologia da Informação e Comunicação, da 3 CCR e o GT de Comunicação Social da PFDC.

20 CGI.br – Comitê Gestor da Internet no Brasil – disponível em: <http://cgi.br/pagina/camara-de-seguranca-e-direitos-na-internet/70>.

soais, registro de identidade civil, divulgação indevida de produtos restritos no comércio eletrônico e dados abertos governamentais.

O aspecto da prevenção no tema relativo ao uso seguro da internet, com foco em crianças e adolescentes, traz a afinidade necessária que justifica a atuação integrada entre os grupos de trabalho citados.

O projeto "Ministério Público pela Educação Digital nas Escolas" se alinha às diretrizes estabelecidas pela Lei nº 12.965/2014 – também conhecida como Marco Civil da Internet – que, em seu art. 26[21] destaca o dever constitucional do Estado na prestação da educação para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, para a promoção da cultura e para o desenvolvimento tecnológico.

As crianças e os adolescentes da geração Y enfrentam novos desafios ao se conectarem à internet, como reforça o professor e educador Rodrigo Nejm:

> [...] Se nos primeiros momentos da Internet as interações estavam baseadas no anonimato, favorecendo a manifestação de comportamentos até então inexplorados, na atualidade, os adolescentes usam intensamente os contextos digitais com seus nomes verdadeiros, expondo voluntariamente detalhes sobre suas vidas que incluem endereços de onde estão, o que estão pensando, com quem estão em relacionamento, quais as preferências gerais, além de expressarem suas opiniões sobre diferentes temas sociais e políticos pelos quais se interessam. No caso das exposições intencionais, podemos dizer que há uma antecipação, uma oferta sob risco, de conteúdos mais íntimos como tentativa de ampliar os laços sociais e as trocas, mesmo antes de haver o retorno positivo na relação, [...][22].

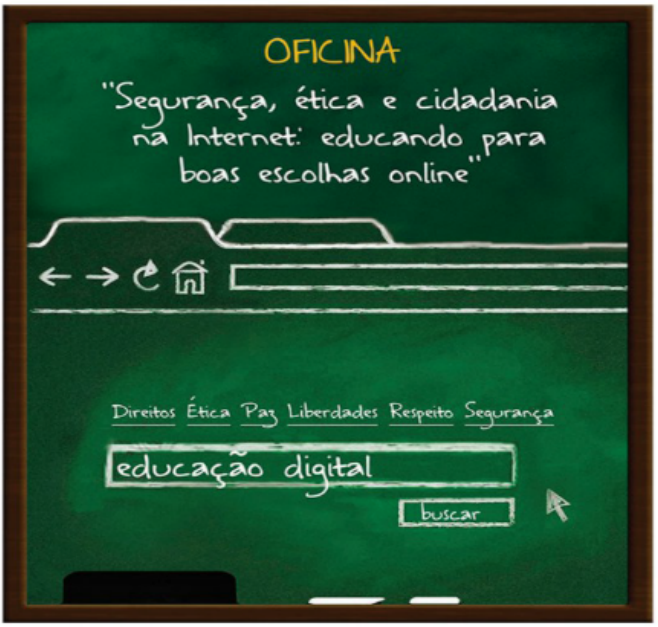
Contribuir em todos esses aspectos é o objetivo do projeto, por meio da oficina "Segurança, ética e cidadania na internet: educando para boas escolhas on-line". A proposta é oferecer a professores e demais operadores do sistema de direitos subsídios para

21 Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

22 NEJM, Rodrigo. Minha privacidade, nossas regras: aspectos comportamentais e sociais do compartilhamento de informações privadas entre adolescentes. In: DA SILVA, Ângelo Roberto Ilha (Org.). **Crimes Cibernéticos**: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2018, p. 71-72.

o desenvolvimento de atividades pedagógicas acerca dos desafios para o uso seguro e cidadão da rede mundial de computadores, abordando temas como *ciberbullying, sexting*, aliciamento e uso excessivo da rede.

A oficina é agendada, em regra, pelo procurador regional dos Direitos do Cidadão[23] da capital do estado, em reunião prévia com as Secretarias Municipais e Estaduais de Educação e de Assistência Social, os Institutos Federais de Ensino e o Sindicato das Escolas Privadas e tem, por dinâmica, o seguinte formato: na parte da manhã, iniciam-se os trabalhos com uma palestra do procurador da República que organiza a oficina na sua cidade, na qual é explicado aos presentes o papel do Ministério Público relacionado ao tema, seja no âmbito criminal, seja no âmbito da cidadania. Em seguida, o psicólogo e educador da ONG SaferNet, Rodrigo Nejm, inicia a capacitação dos educadores, demonstrando os mais diversos tipos de violações aos direitos humanos que ocorrem no mundo virtual e dos quais as crianças e os adolescentes podem ser vítimas ou agentes.



23 O procurador regional dos Direitos do Cidadão é um procurador da República, escolhido entre seus pares, e que representa a PFDC em seu estado de lotação, exercendo as funções inerentes ao PFDC, regionalmente. As oficinas também podem ser organizadas por procurador da República com atuação na área criminal na respectiva capital.

Na parte da tarde, em continuação, são distribuídos materiais pedagógicos (cartilhas, cartazes e *folders* didáticos) para a introdução do assunto em sala de aula. É oportunizado tempo para perguntas pelos participantes e para a discussão de situações práticas, cada vez mais vivenciadas no ambiente escolar, bem como são demonstrados os meios existentes para o adequado encaminhamento às autoridades das notícias de crimes que venham a ter conhecimento.

O objetivo desse material pedagógico é estimular os brasileiros, principalmente as crianças e os adolescentes, a aproveitar todo o potencial da rede, sem se esquecer de adotar os cuidados necessários nesse novo espaço público, observando as dicas de segurança, ética e cidadania. Orientação, diálogo e conscientização continuam sendo as melhores "tecnologias" para promover boas escolhas on-line.

Após a realização da oficina, ficam disponibilizados às escolas participantes do projeto, na sede da Procuradoria da República local, cerca de 3 mil exemplares da cartilha "Diálogo Virtual 2.0: preocupado com o que acontece na Internet? Quer conversar?" – cuja versão digital pode ser acessada no site da PFDC (www.pfdc.pgr.mpf.mp.br). A referida cartilha foi elaborada pela equipe da SaferNet Brasil, com o propósito de contribuir para a promoção do uso ético, responsável e seguro da internet no Brasil. Com uma linguagem simples, ilustrações inéditas e diagramação lúdica, a publicação pretende atingir públicos de diferentes faixas etárias e níveis socioeducacionais. Para retirada do material, a escola interessada deve preencher um formulário on-line, no qual informa o tipo de atividade que pretende realizar com o material em sua escola. Tal informação também é utilizada como um dos indicadores de resultado do projeto.

Desde o ano de 2015, foram realizadas mais de 20 (vinte) oficinas, no Distrito Federal e nos seguintes estados: Amazonas, Bahia, Ceará, Espírito Santo, Mato Grosso, Minas Gerais (duas vezes), Pará, Paraíba, Pernambuco, Rio de Janeiro (duas vezes), Rio Grande do Sul, Rondônia, Santa Catarina, São Paulo (para comunidades indígenas também, a pedido da Funai local), Tocantins e Mato Grosso do Sul, tendo-se por meta alcançar os demais estados até o final do ano 2017, o que de fato, ocorreu, com a realização da última oficina, na cidade de Natal, no mês de dezembro de 2017. Em relação às primeiras 20 oficinas já realizadas, extraem-se os seguintes dados estatísticos, colhidos do site mapa.safernet.org.br (ainda não incluídos os dados relativos a Mato Grosso do Sul):

Educadores capacitados – 2.887 pessoas
Municípios alcançados – 280
Alunos beneficiados – 155.004

Também, no mencionado período, têm-se os seguintes dados estatísticos de avaliação[24]:

AVALIAÇÃO DO PÚBLICO SOBRE A RELEVÂNCIA DO TEMA E DOS CONTEÚDOS:

MUITO BOM: 93,37%
BOM: 5,44%
REGULAR: 00,44%
INSUFICIENTE: 00,75%

AVALIAÇÃO DO PÚBLICO SOBRE A APRENDIZAGEM DO TEMA:

MUITO BOM: 78,68%
BOM: 20,81%
REGULAR: 00,31%
INSUFICIENTE: 00,06%

AVALIAÇÃO DO PÚBLICO SE RECOMENDA A ATIVIDADE:

SIM:99,87%
NÃO: 0,12%

Sempre que possível, visando dar o máximo de visibilidade às oficinas, a Coordenação e a Assessoria do Projeto na PFDC vêm promovendo sua divulgação por meio de palestras, como a realizada para promotores da Infância e Juventude, em evento orga-

24 Disponível em: <mapa.safernet.org.br>.

nizado pelo Copeij[25], no *Internet Governance Forum* (em Workshop da Unesco)[26] e para a Fiscalía General de Ecuador[27], entre outros.

Todas as informações sobre o Projeto constam do site <www.pfdc.pgr.mpf.mp.br>. Sobre as oficinas já realizadas, também constam maiores detalhes no *link* <http://midia.pgr.mpf.gov.br/pfdc/hotsites/diversos/MPEducacaoDigital/relatorioMPEducacaoDigital.pdf>.

Em paralelo, outros países também desenvolvem políticas públicas voltadas à informação de professores, como o Reino Unido, cujo *Cyber Security Challenge* desenvolveu um "plano de aula" e um jogo interativo para instruir os professores sobre a *Computer Misuse Act*[28].

Igualmente, aulas de *cyber-ethics*, isto é, em tradução livre, ética no *cyberespaço*, são sugeridas pelo especialista em segurança na internet Stephen Cobb, que as vê como parte essencial para deter o crime cibernético. Para ele, a adição de aulas de ética no *cyberespaço* no currículo escolar elementar pode ser vista como um grande acerto em curto e longo prazos[29].

Outro destaque é a *Common Sense*[30], organização sem fins lucrativos dedicada a auxiliar o desenvolvimento de crianças e adolescentes em um mundo em rápida evolução, pelo empoderamento de educadores e estudantes por meio de sua instrução à profícua utilização das ferramentas educativas presentes nos dispositivos tecnológicos; por sua vez, a *UK Safer Internet Centre*[31] é o resultado da parceria de instituições de caridade britânicas, com o objetivo de auxiliar crianças e adolescentes a permanecerem seguros on-line.

25 Comissão Permanente da Infância e da Juventude (Copeij) – Evento realizado de 5 a 7 de agosto, na sede do MP-MG em Belo Horizonte.

26 O Fórum de Governança da Internet (IGF) é um fórum multissetorial, democrático e transparente, que viabiliza debates sobre questões de políticas públicas relativas a elementos importantes da governança da internet. O IGF fornece uma plataforma facilitadora para discussões entre todos os setores do ecossistema de governança da internet, incluindo as entidades credenciadas pela Cúpula Mundial sobre a Sociedade da Informação (CMSI), bem como outras instituições e indivíduos com especialidade comprovada e experiência em assuntos relacionados à governança da internet. O último evento IGF ocorreu em João Pessoa/PB, de 10 a 13 de novembro de 2015.

27 "Taller Internacional de Capcitación de fiscales, investigadores Y técnicos informáticos em materia de delitos cibernéticos (ciberdelitos)" – 24 a 25 de novembro de 2015.

28 Disponível em: <http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people--from-getting-involved>.

29 Disponível em: <https://www.welivesecurity.com/2015/01/20/cybercrime-deterrence-6-important-steps/>.

30 Disponível em: <https://www.commonsense.org/>.

31 Disponível em: <https://www.saferinternet.org.uk/>.

3 Conclusão

O objetivo do projeto é a união de esforços na prevenção e no combate à pornografia infantil, ao racismo e a outras formas de discriminação veiculadas na internet. E, para tal intento, o Ministério Público Federal conta com a parceria da ONG SaferNet Brasil e o patrocínio do Comitê Gestor da Internet no Brasil, a fim de que os professores das redes pública e privada de ensino fundamental e médio ensinem e orientem seus alunos a usarem de forma saudável e responsável a internet, a se protegerem de criminosos e a não se tornarem futuros agressores.

O projeto também tem por objetivo o estabelecimento de parceria com o Ministério da Educação, a fim de que as respectivas diretrizes, o conteúdo e o material pedagógico das o ficinas sejam adotados pelo Poder Público, em complementação às políticas de educação em direitos humanos já realizadas, o que possibilitará alcançar o maior número de educadores de escolas públicas e privadas. Para tanto, está em vias de se assinar um Termo de Cooperação Técnica com o Ministério da Educação, por meio da Procuradoria Federal dos Direitos do Cidadão (PFDC), para disponibilizar o material produzido em plataformas acessadas por professores de todo o País.

Por meio do projeto "Ministério Público pela Educação Digital nas Escolas" busca-se o incentivo à educação, pela prevenção, para que crianças e adolescentes aprendam a usar a internet de forma cidadã, segura e ética, bem como para que torne possível o adequado encaminhamento às autoridades, por qualquer pessoa, de notícias sobre a ocorrência de crimes cibernéticos, visando à devida apuração e punição dos autores de tais ilícitos.

Com a realização de todas as oficinas propostas, o projeto parte para sua terceira fase, ainda em estudos, sobre a possibilidade de sua implementação no ambiente universitário, a fim de que os alunos dos cursos de pedagogia, psicologia e serviço social sejam preparados para lidar com esses temas virtuais profissionalmente na sala de aula ou no atendimento de crianças e adolescentes.

As crianças e os adolescentes, por meio da educação nas escolas, devem crescer conscientes de seus atos para que, com a exata noção do que é o mundo virtual, não só não sejam vítimas de crimes pela internet, como também, ao se tornarem adultos, não os pratiquem, tornando-se cidadãos ciosos de seus direitos e deveres. A noção de que a internet não é apenas uma rede mundial de computadores, mas, na verdade, uma rede mundial de pessoas conectadas por computadores, é importantíssima e deve ser

a cada dia difundida, para que, a partir da compreensão da sociedade, redobrem-se os cuidados com a veiculação de conteúdos que não sejam apropriados a pessoas cuja vulnerabilidade deflui da sua própria condição de ser em formação.

Referências

COBB, Stephen. **Cybercrime deterrence**: 6 important steps. 2015. Disponível em: <https://www.welivesecurity.com/2015/01/20/cybercrime-deterrence-6-important-steps/>.

NEJM, Rodrigo. Minha privacidade, nossas regras: aspectos comportamentais e sociais do compartilhamento de informações privadas entre adolescentes. In: DA SILVA, Ângelo Roberto Ilha (Org.). **Crimes cibernéticos**: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção de provas digitais, nova lei antiterrorismo, outros temas. Porto Alegre: Livraria do Advogado, 2018, p. 71-72.

13 JUSTIÇA RESTAURATIVA: UMA NOVA PERSPECTIVA PARA O ENFRENTAMENTO DOS CRIMES CIBERNÉTICOS RELACIONADOS À PORNOGRAFIA INFANTIL

Cristina Scalabrin[1]

Resumo: Este artigo pretende ser um instrumento de reflexão acerca da complexidade e dos desafios envolvidos na temática dos crimes cibernéticos relacionados à pornografia infantil que expõem a fragilidade do cuidado com a infância e a adolescência, engendrada em uma sociedade marcada por uma revolução tecnológica que produz novas formas de subjetivação, valores, relações e, consequentemente, novas modalidades criminais. O crescente número de URLs únicos denunciados, bem como o aumento do número de ações criminais relacionadas ao tema, desafia o Sistema de Justiça a construir novas possibilidades de enfrentamento aos crimes cibernéticos relativas ao Estatuto da Criança e do Adolescente que possibilitem a construção de um processo restaurativo dos danos gerados pelo crime, rompendo ciclos de violência, transformando as relações e promovendo a pacificação social.

Palavras-chave: Crimes cibernéticos. Pornografia infantil. Justiça restaurativa.

Abstract: *The current article has the aim to be an instrument upon which we think about the complexity and challenges concerning cybercrimes related to child pornography.. These crimes illustrate the fragility of child and adolescent care, conveyed in a society marked by a technological revolution which produces new ways of subjectivation, values, relationships and consequently new criminal modalities. The growing number of reported single URLs, as well as the increase in lawsuits related to this topic, challenge the Criminal Justice to create new possibilities to fight cybercrimes involving the Child and Adolescent Statute that enable the construction of a process in order to restore the damage caused by these crimes, breaking hence cycles of violence, changing relationships and promoting social pacification.*

Keywords: Cybercrimes. Child pornography. Restorative justice.

1 Introdução

Sobre enfrentar o não enfrentável, Bauman nos diz:

> Agora, afinal, "estamos de pé, firmes, a enfrentar o caos". Nunca fizemos isso antes. Apenas enfrentar o caos já seria desconcertante e incômodo

1 Psicóloga, facilitadora de Círculos de Construção de Paz, consultora do Projeto de Justiça Restaurativa da Justiça Federal do Rio Grande do Sul.

> o suficiente. Mas a novidade do ato – a total ausência de qualquer antecedente pelo qual passar, pelo qual ser confirmado, pelo qual ser guiado – torna a situação enervante. As águas em que nos lançamos não são apenas profundas, nunca foram mapeadas. Não estamos ainda numa encruzilhada: para uma encruzilhada ser uma encruzilhada primeiro deve haver estradas. Agora sabemos que fazemos as estradas – as únicas estradas existentes e que podem ser construídas –, e fazemos simplesmente por nelas *caminhar*". (BAUMAN, 2011)

As novas tecnologias produziram uma modificação na relação de espaço e tempo em um território sem fronteiras. A existência do ciberespaço oportunizou a disponibilização de informação em volume sem precedentes na história. A conexão de pessoas em todo o mundo em tempo real constituiu novas formas de relação, mas também deu visibilidade a temáticas complexas, como a questão da pornografia infantil, fazendo com que informações que se restringiam apenas a um grupo específico fossem acessíveis a todas as pessoas que, de alguma forma, estão inseridas no ciberespaço. A substituição progressiva das relações do meio ambiente para o ambiente tecnológico e midiático produz outras formas de subjetivação e, consequentemente, relações pessoais e sociais na medida em que o sujeito é constituído, como nos aponta Foucault, a partir do momento histórico em que vive. Não há uma condição natural, e sim, uma condição histórica e social.

> Se alguém se move com rapidez suficiente e não se detém para olhar para trás e contar ganhos e perdas, pode continuar comprimindo um número cada vez maior de vidas no tempo de duração da existência mortal, talvez tantas quantas a eternidade permitir. (BAUMAN, 2005)

O impacto das novas tecnologias na subjetividade do sujeito pós-moderno, bem como as novas formas de expressão do conflito com a justiça, desafia-nos à escuta e compreensão do sentido que existe nos novos confrontos com a lei, tanto para o sujeito que pratica o crime como também para a sociedade que produz novas formas de violência. E então, faz-se necessário, a partir dessa escuta, criar novas possibilidades para que o sofrimento pessoal e social implicados nesse processo possam ser restaurados, e os ciclos de violência rompidos.

Nesse contexto, faz-se o convite à reflexão acerca dos limites e possibilidades de atuação do Sistema de Justiça. Se, por um lado, há um ideário social de justiça que entende a punição como uma possibilidade imediata de banir o mal como se fosse algo alheio à própria sociedade, ao longo da história essa lógica se mostrou ineficaz: "O ideal de

que, a toda a violação do sistema jurídico-penal, o Estado reagiria aplicando ao infrator a devida e justa retribuição fracassa no intento de responsabilizar os ofensores e coibir o crime, frustrando os anseios da sociedade" (FERREIRA; SEMERARO; SCALABRIN, 2017).

Em contraponto, uma possibilidade de reflexão e diálogo é aberta pelo paradigma restaurativo, que entende o crime como uma violação de pessoas e relações que, por meio do processo de responsabilização a partir de uma metodologia autocompositiva, compreende a vítima, o ofensor e a comunidade na construção de soluções que promovam reparação das pessoas e das comunidades envolvidas na situação de conflito com a justiça.

A partir da aprovação da Resolução nº 225/2016[2] do Conselho Nacional de Justiça, que dispõe sobre a Política Nacional de Justiça Restaurativa no âmbito do Poder Judiciário, abre-se campo dialógico interdisciplinar que pode construir novos caminhos para o enfrentamento das questões criminais, por meio do resgate da cidadania e da justiça como valor.

2 A Pornografia Infantil Como uma Questão Social

Até o final da década de 1960, o aparecimento de crianças em material pornográfico era algo raro. Entretanto, com a legalização de todas as formas de pornografia, em julho de 1969, na Dinamarca, foi iniciado um período conhecido como "década da liberalização". Como nos aponta Landini (2007), no final da década de 1970, estima-se que entre 300 e 600 mil crianças com menos de 16 anos estivessem participando da produção desse tipo de material.

A legislação contra a produção e distribuição de material contendo pornografia infantil começou a entrar em vigor, na maioria dos estados norte- americanos, em 1977, e no Brasil apenas em 1990, com a promulgação do Estatuto da Criança e do Adolescente (ECA) (LANDINI, 2007). No âmbito das relações internacionais, a Assembleia Geral das Nações Unidas adotou, em maio de 2000, o Protocolo Facultativo para a Convenção sobre os Direitos da Criança, que aborda as questões referentes à pornografia infantil, tendo sido ratificado pelo governo brasileiro em janeiro de 2004, entrando em vigor no país em fevereiro do mesmo ano.

2 Disponível em: <http://www.cnj.jus.br///images/atos_normativos/resolucao/resolucao_225_31052016_02062016161414.pdf>.

Ao mesmo tempo em que se constituiu um movimento para legislar sobre a temática da pornografia infantil, a internet, que até 1979 era utilizada apenas para fins militares e acadêmicos, começou a ganhar espaço no mundo comercial. Segundo Abreu (2009), a expansão desse mercado foi realizada por empresas norte-americanas e alemãs até a criação da rede mundial de computadores, a *World Wide Web*, em 1989 por Tim Berners-Lee. Essa rede possibilitou que todas as informações arquivadas nos computadores do mundo pudessem se conectar. Dessa maneira, também se constituiu uma nova dimensão da vida e das relações humanas, que se expandiu com grande velocidade, chegando ao ano de 1993 com 3,5 milhões de assinantes (ABREU, 2009). Segundo o relatório da União Internacional de Telecomunicações (UIT), agência da ONU especializada em tecnologias de informação e comunicação, divulgado em julho de 2017, até o final desse mesmo ano o número de assinaturas de banda larga móvel deve atingir o patamar de 4,3 bilhões de assinantes em todo o mundo.

Com a massificação do acesso à internet, os conteúdos que eram compartilhados apenas entre pessoas com interesse específico de imagens de pornografia infantil puderam ser acessados por qualquer pessoa que estivesse conectada à rede mundial de computadores. "Em suma, com a Internet, a pornografia infantil deixou de ser algo conhecido apenas pelo restrito grupo dos pedófilos e adquiriu visibilidade." (LANDINI, 2007).

Segundo dados disponibilizados pelo Inhope[3] (International Association of Internet Hotlines), no ano de 2012 foram confirmadas 33.821 denúncias de URLs únicos com conteúdo de abuso sexual infantil; em 2013 foram 48.910 URLs únicos; e no ano de 2014 esse número chegou a 83.644 URLs. No Brasil, os dados disponibilizados pela Safernet[4] informam que, ao longo de 11 anos, a organização confirmou a existência de 668.288 URLs distintos envolvendo conteúdo de abuso sexual infantil em 98 países dos cinco continentes. Esses dados nos trazem a dimensão da velocidade com que as conexões acontecem no ciberespaço e convidam à reflexão sobre o impacto pessoal, social, histórico e cultural, bem como à relação com a justiça.

De acordo com dados levantados na 2ª Câmara de Coordenação e Revisão Criminal do Ministério Público Federal, datados de outubro de 2017, atualmente no Brasil existem 2.077 inquéritos em andamento, 368 processos tramitando em primeira instância e 135 em 2ª instância, referentes aos crimes previstos no Estatuto da Criança e do Adolescente, que são de competência da Justiça Federal, entre os quais estão incluídas algumas

3 Disponível em: <http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx>.

4 Disponível em: <http://indicadores.safernet.org.br/indicadores.html>.

condutas previstas nos arts. 241, 241-A, 241-B, 241-C e 241-D, que versam sobre a temática da pornografia infantil.

Considerando-se o crescimento do número de denúncias, de operações policiais, de processos criminais e, por consequência, de execuções penais em crimes dessa natureza, e, ainda, cientes de que a realidade e a configuração atual do Sistema Penal mostram-se ineficazes no intento de transformar a situação conflitiva que é objeto deste artigo, bem como ante o reconhecimento de que as relações sociais e as práticas delitivas atualmente também operam por meio de uma nova arquitetura tecnológica, somos desafiados a pensar em uma outra lógica de fazer justiça que possibilite efetivamente a transformação dos conflitos. Por certo, a manutenção desse *modus operandi* fatalmente aumentará a demanda sobre um Sistema Judiciário que já sofre com a sobrecarga e judicialização cada vez maior dos conflitos de toda ordem.

> Se estamos justamente a tratar de como solucionar os conflitos de outro modo, o primeiro dever de honestidade que temos de ter para conosco é de considerar os próprios conflitos como o foco de ocultamento e apagamento operado pela história das ideias. Então, em vez de negligenciá-los como reveladores apenas daquilo que há de negativo, haveríamos de procurar encará-los como emergência de tentativas de dação de sentidos outros à vida, ao modo como a estruturamos, e interpretamos aquilo que vimos vivendo. Se o lograrmos, a própria justiça haveria de ser vista em meio a estes embates de interpretações, em meio às construções e desconstruções de equilíbrios possíveis entre modos distintos de se viver, de sentir, de desejar, de perceber suas próprias fraquezas e potencialidades, permitindo-nos, então, um modo distinto de considerar as respostas que damos a estes conflitos. (MELO, 2005)

3 A Justiça Restaurativa como Possibilidade de Transformação

> A dimensão restaurativa desafia a sociedade a superar o modelo fragmentado diante de situações complexas, sendo fundamental a interlocução entre saberes e instituições através da aproximação, da cultura de cooperação e do diálogo entre as diversas áreas de intervenção. Fazer justiça pressupõe restaurar, reconstruir o tecido social promovendo a pacificação social. (FERREIRA; SEMERARO; SCALABRIN, 2017)

A partir da regulamentação das práticas restaurativas no Brasil por meio da Resolução nº 225/2016 do Conselho Nacional de Justiça, o Poder Judiciário é instrumentalizado, no âmbito institucional, para a construção de novos caminhos, a partir de um conjunto de princípios, métodos, técnicas e atividades próprias que viabilizam a qualificação das respostas às demandas da sociedade no que tange à temática da violência, pela conscientização dos aspectos relacionais, institucionais e sociais implicados nas situações de conflito e violência, objetivando a pacificação social.

A ampliação da perspectiva sobre o fenômeno criminal nos traz a percepção de que o crime é uma violação cometida por alguém que também pode ter sido vítima de violações. Como aponta Zehr (2008) "trata-se de uma violação do justo relacionamento que deveria existir entre indivíduos", e também da justa relação na sociedade, no acesso a educação, saúde, assistência social e cultura, oportunizando possibilidades de existência favoráveis à vida.

Howard Zehr (2008) faz um contraponto acerca do entendimento do crime entre o paradigma retributivo e o restaurativo, no qual na "Justiça Retributiva o crime é uma violação contra o Estado, definida pela desobediência à lei e pela culpa. A Justiça determina a culpa e inflige dor no contexto de uma disputa entre ofensor e Estado, regida por regras sistemáticas". Em contrapartida, na "Justiça Restaurativa o crime é uma violação de pessoas e relacionamentos. Ele cria a obrigação de corrigir os erros", obrigação essa que nasce no processo de responsabilização a partir do entendimento dos fatores que levaram ao delito, construindo um desejo íntimo de reparação do dano e de estabelecer novas formas de relação interpessoal, comunitária e social.

A perspectiva restaurativa na abordagem às questões criminais abre um espaço de diálogo com o Outro, transcendendo as representações associadas ao crime, por meio de um vínculo estabelecido. Na perspectiva do filósofo Emmanuel Levinas, esse vínculo acontece por dois eixos: o reconhecimento da alteridade do Outro e a impossibilidade de definir a sua existência a partir do meu entendimento sobre ele; e a minha responsabilidade sobre este Outro, mediante um vínculo não violento, acolhendo esse sujeito na sua integral diferença. A partir da possibilidade do entendimento e elaboração dos fatores pessoais, interpessoais, sociais e culturais que levam ao conflito, abre-se um espaço de construção de ações restaurativas para os envolvidos na situação conflitiva: ofensores, familiares e sociedade.

Os princípios norteadores da Justiça Restaurativa são a corresponsabilidade, a informalidade, a voluntariedade, a consensualidade, a confidencialidade, a imparcialidade,

a participação, o empoderamento, o atendimento às necessidades de todos os envolvidos, a reparação dos danos, a celeridade e a urbanidade. Considerando a pluridimensionalidade humana, a operação dos princípios demanda ações de caráter interdisciplinar e intersetorial, agregando saberes e ações de diversas áreas ao tratamento das situações conflitivas e integrando as políticas públicas do âmbito da segurança, assistência, educação e saúde.

Para que exista a possibilidade de reparação dos danos e para que as necessidades dos envolvidos possam emergir, faz-se necessário um espaço de diálogo por meio de metodologia autocompositiva e consensual, com facilitadores habilitados para tal atividade. Os objetivos norteadores são a superação dos conflitos associados ao delito, bem como a construção de um entendimento sobre ele, a identificação das necessidades, e a compreensão da responsabilidade no conflito, buscando formas de atendimento das necessidades e reparação dos danos causados, criando condições para a não reincidência. A metodologia deve propiciar o direito igualitário à palavra, promovendo a responsabilização dos sentimentos e percepções, convidando ao entendimento da percepção do outro.

A criação de um espaço de reflexão e diálogo empodera pessoas e comunidade. Oportuniza que a pessoa vítima de violência não seja reduzida a testemunha em um processo criminal, mas tenha a possibilidade de que o dano sofrido seja reparado e que a situação vivida seja passível de ressignificação. Em relação ao ofensor, é favorecida a transposição da condição de culpa que cristaliza a situação na ordem do irreparável, para a possibilidade de responsabilização, reparação do dano causado e construção de novas formas de existência na sociedade, que promova o compromisso íntimo com a não reincidência criminal.

Do ponto de vista restaurativo, a comunidade, as instituições e a sociedade contribuem para o surgimento dos fenômenos de violência e também são afetadas por eles de maneira que essas instâncias devem ser consideradas, implicadas no processo de entendimento e reparação dos danos, por meio de novas possibilidades de atuação que promovam inclusão, pacificação e exercício da cidadania.

> A toda esta teia complexa, com vistas à correção da responsabilidade do "eu", Lévinas chamou, novamente, de justiça (LÉVINAS, 1988: 81). Ou seja, justiça é a moderação da responsabilidade que o "eu" tem sobre si, a qual só é possível a partir da multiplicidade dos homens e da presença do terceiro ao lado de outrem. Veja-se assim que, a rigor, a palavra justiça é usada

> em dois sentidos: como a responsabilidade em relação a outrem e como a correção da assimetria a partir da inserção do terceiro. (PIMENTA, 2010)

Ferreira Neto (2004) sinaliza que "um dos objetivos da genealogia foucaultiana do sujeito de desejo moderno foi efetuar a desnaturalização dessa versão de subjetividade por meio de sua formação historicamente datada". Assim, considerando-se que não há naturalidade no processo de subjetividade humana e ela é constituída e emerge conectada aos processos históricos e culturais ao mesmo tempo em que os produz; e a velocidade e a fragilidade dos laços estabelecidos pelo sujeito pós-moderno como repercussão de uma cultura cibernética que substituiu a cidade do meio ambiente pelos mecanismos tecnológicos e virtualização das relações, conclui-se que o resgate da dimensão humana por meio da promoção de espaços de inclusão e de direito à palavra pode ser um caminho para produção de alternativas que entendam e contemplem as necessidades não atendidas do tecido social, bem como um caminho de restauração dos laços pessoais, comunitários e sociais rompidos pelas situações de crime e violência.

No que tange aos resultados dos processos restaurativos, é importante salientar que, na medida em que aborda pessoas e relações, valorizando a experiência pessoal, conclui-se que a métrica quantitativa ou qualitativa analisada sob a ótica *simplesmente* retributiva não tem condições de registrar o que é da ordem subjetiva e relacional. Uma outra abordagem é sugerida, a da investigação transformadora, que, segundo Konzen (2007), parte dos seguintes princípios: ter como objeto de análise a ação social, em vez do conhecimento puro; reconhecer que grande parte do conhecimento é subjetivo, construído e inter-relacional; reconhecer a natureza complexa e limitada das descobertas; considerar a dinâmica do poder existente em todas as análises; respeitar os sujeitos como participantes do estudo; definir o papel dos pesquisados como sendo o de um facilitador, entendendo a impossibilidade da neutralidade; valorizar tanto o processo quanto o resultado; reconhecer as realidades do outro e estar aberto à possibilidade de ser pessoalmente afetado por essa relação; estar ciente das imprevisibilidades e dos danos em potencial nas situações atendidas; buscar equilíbrio entre objetividade e subjetividade; e, por último, lançar mão de métodos de obtenção de informações e de apresentação de resultados que façam sentido aos resultados obtidos, utilizando dispositivos verbais, visuais, artísticos e científicos.

4 Conclusão

Ainda que seja o momento de concluir, o desafio que está posto é o da reflexão. A temática trabalhada neste artigo diz respeito não só às crianças vítimas de violência, mas também a quem produz, reproduz, armazena e distribui material relacionado à pornografia infantil. Estamos diante de uma sociedade que cada vez mais se relaciona a partir da referência do ciberespaço, construindo e desconstruindo relacionamentos na velocidade em que se digita uma palavra nos dispositivos eletrônicos conectados na rede mundial de computadores.

Se por um lado a velocidade com que uma informação de violência é transmitida, reproduzida e replicada é passível de gerar uma onda proporcional à dimensão da rede, ações de prevenção, educação, fortalecimento de vínculos saudáveis, por outro lado, têm a mesma potencialidade desde que estejamos abertos ao entendimento de que há uma nova ordem nas relações, novas formas de subjetivação e que é necessário dar ao sujeito pós-moderno o acesso à palavra para que as ações de enfrentamento à violência na sociedade cibernética façam sentido para essa mesma sociedade.

É possível compreender, a partir do que foi exposto ao longo deste artigo, que na medida em que se amplia o acesso à rede mundial de computadores, mais pessoas são expostas à pornografia infantil, produzindo novas formas de subjetivação e relação em uma perspectiva macro. O conteúdo que antes do advento da rede mundial de computadores era restrito aos grupos fechados, torna-se material de consumo em potencial, operando como uma droga ilícita de fácil acesso a qualquer momento.

A possibilidade de compreender o crime como expressão dispara um processo de entendimento acerca das dimensões humanas e relacionais envolvidas nessa forma, ainda que trágica e violenta, de manifestação. A partir do diálogo entre saberes, outros entendimentos se tornam possíveis, viabilizando a construção conjunta e partilhada de estratégias e ações que possam operar de forma efetiva no processo de restauração das relações pessoais e sociais afetadas pelo delito.

A temática da pornografia infantil é algo rejeitado de forma intensa pela sociedade, ainda que paradoxalmente ela mesma faça parte do sistema que gera esse tipo de delito. Isso nos sinaliza a necessidade de falar, problematizar, discutir e compreender a dinâmica que desencadeia esse movimento para que sejam construídos caminhos de restauração legítimos das pessoas envolvidas direta e indiretamente com o crime, bem como criar relações sociais mais fortalecidas, que oportunizem a reparação das con-

sequências dos delitos relacionados com a vulnerabilidade, exposição e abandono da infância na nossa sociedade.

A oportunidade de diálogo com ofensores em processos ligados aos crimes do Estatuto da Criança e do Adolescente, bem como com as instituições de proteção à infância, pode trazer, a partir do processo restaurativo, informações fundamentais para que se possa pensar em ações intersetoriais de cuidado e prevenção desse tipo de conflito com a lei. As temáticas que envolvem os crimes contra a infância e de ordem sexual expõem a fragilidade da infância, a violação do corpo e da intimidade, a negligência e a dificuldade de falar sobre os assuntos que ainda são, paradoxalmente, tabus em nossa sociedade. Se, por um lado, a questão do sexo e da erotização é algo largamente difundido nos meios de comunicação e entretenimento entendidos como legítimos, o diálogo sobre violência e sexualidade buscando cuidado e prevenção é ainda uma temática que necessita de construção. Há um longo caminho a ser trilhado para que os crimes sexuais que acontecem na dimensão do ciberespaço possam ser enfrentados de maneira eficaz, produzindo a pacificação e restauração do tecido social.

E, por fim, cabe salientar que estamos diante de um desafio intersetorial, no qual se faz indispensável a construção, a articulação e o fortalecimento das redes de saúde, assistência social, educação, tecnologia e justiça em um compromisso de empreender, em conjunto, o resgate da cidadania por meio de projetos que fomentem uma cultura de cidadania, restauração, cuidado e inclusão.

Referências

ABREU, Karen Cristina Kraemer. **História e usos da Internet**. 2009 Disponível em: <http://chile.unisinos.br/pag/abreu-karen-historia-e-usos-da-internet.pdf>.

ALVES, Priscila Pires; MANCEBO Deise. Tecnologias e subjetividade na contemporaneidade. **Estudos de Psicologia**, v. 11, n. 1, p. 45-52, 2006. Disponível em: <http://www.scielo.br/pdf/%0D/epsic/v11n1/06.pdf>. Acesso em: 24 out. 2017.

BAUMAN, Zygmunt. **Vida líquida**. Rio de Janeiro: Zahar, 2005.

_____.**Vida em fragmentos**. Rio de Janeiro: Zahar, 2011.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8069.htm>. Acesso em: 24 out. 2017.

_____. Conselho Nacional de Justiça. **Resolução nº 225, de 31 de maio de 2016**. Dispõe sobre a Política Nacional de Justiça Restaurativa no âmbito do Poder Judiciário e dá outras providências. Disponível em: <http://www.cnj.jus.br/atos-normativos?documento=2289>. Acesso em: 24 out. 2017.

FERREIRA NETO, João Leite. Processos de subjetivação e novos arranjos urbanos. **Revista do Departamento de Psicologia – UFF**, v. 16, n. 1, p. 111- 120, 2004. Disponível em: <http://200.229.43.1/documentos/processos_subjetivacao.pdf>. Acesso em: 24 out. 2017.

FERREIRA, Roberto Schaan; SEMERARO, Luisanna; SCALABRIN, Cristina. Nova Perspectiva para a Execução Penal. In: BRASIL. Justiça Federal. Seção Judiciária do Rio Grande do Sul. **Justiça Federal no RS**: memória e futuro: 1967-2017. Porto Alegre, 2017.

FOUCAULT, Michel. **História da sexualidade 2**: o uso dos prazeres. Rio de Janeiro: Graal, 1984.

KONZEN, Afonso Armando. **Justiça restaurativa e ato infracional**: desvelando sentidos no intinerário da alteridade. Porto Alegre: Livraria do Advogado Editora, 2007.

LANDINI, Tatiana Savoia. Envolvimento e distanciamento na produção brasileira de conhecimento sobre pornografia infantil na Internet. **São Paulo em Perspectiva**, São Paulo, v. 21, n. 2, p. 80-88, jul./dez. 2007. Disponível em: <http://produtos.seade.gov.br/produtos/spp/v21n02/v21n02_07.pdf>. Acesso em: 24 out. 2017.

MELO, Eduardo Rezende. Justiça restaurativa e seus desafios histórico-culturais. Um ensaio crítico sobre os fundamentos ético-filosóficos da justiça restaurativa em contraposição à justiça retributiva. In: BRASIL. Ministério da Justiça – PNUD. **Justiça restaurativa**. Brasília, 2005.

PIMENTA, Leonardo Gulart. Justiça, alteridade e Direitos Humanos na teoria de Emmanuel Lévinas. **Revista USCS – Direito**, ano XI, n. 19, jul./dez. 2010. Disponível em: <http://seer.uscs.edu.br/index.php/revista_ direito/article/view/1104>.

PINTO NETO, Moysés. O Caso Pierre Rivière Revisitado por uma Criminologia de Alteridade. **Revista de Estudos Criminais**, Porto Alegre, v. 30, p. 55-68, 2003.

ZEHR, Howard. **Trocando as lentes**: um novo foco sobre o crime e a justiça. São Paulo: Palas Athena, 2008.

MPF
Ministério Público Federal

ISBN 978-85-85257-32-3