Os crimes cibernéticos no Distrito Federal

Alexandre Paiva

Bacharel em Sistema de Informação pela Faculdade Anhanguera; defendendo através deste artigo acadêmico: **Os crimes cibernéticos no Distrito Federal**, apresentado à coordenação do curso como requisito básico para obtenção de aprovação, o título de Especialista em Segurança da Informação e Perícias em Crimes Cibernéticos pela UPIS – Faculdades Integradas, Brasília; Analista de Sistemas.

E-mail: alex.rcp@gmail.com

Evandro Lorens

Mestre em Ciência da Computação, Arquitetura da Informação e Segurança da Informação pela Universidade de Brasília; Especialização em Redes de Comunicações e Telecomunicações pela Universidade Federal do Espirito Santo; Graduado em Ciência da Computação pela Universidade Federal do Espirito Santo. Coautor.

E-mail: lorens@unb.br

Resumo

O objetivo deste artigo é apresentar a evolução dos crimes cibernéticos no Distrito Federal, Brasil. Traz uma revisão de literatura sobre crimes cibernéticos, explora a legislação nacional pertinente e analisa os números disponibilizados pela Delegacia Especial de Repreensão aos Crimes Cibernéticos – DRCC/PC/DF e Tribunal de Justiça do Distrito Federal e Territórios – TJDFT, com informações sobre os crimes cibernéticos no Distrito Federal.

Palavras-chave

Segurança da Informação; Crimes cibernéticos; Evolução crimes digitais no Distrito Federal.

Cybernetic Crimes in Distrito Federal

Abstract

The goal of this study is to present the evolution of cybernetic offenses in Distrito Federal, Brazil. It brings a review on the literature about cybernetic criminology, explores the national legislation pertaining to the subject and analyses numbers made available by the Agency for Reprimand to Cybernetic Crimes - DRCC/PC/DF and the Justice Court of Distrito Federal and Territories - TJDFT, and information on the cybernetic crimes in Distrito Federal.

Keywords

Information security; Cybercrimes; Evolution of digital crimes in the Federal District.

INTRODUÇÃO

Os crimes cibernéticos são quaisquer crimes existentes no meio físico ou virtual praticado por meio do uso de tecnologia. Esta definição abrange um espectro bem superior ao que se costuma ser o entendimento do senso comum. Nela são enquadrados, por exemplo, crimes de ódio e contra a honra perpetrados por meio das redes sociais e que têm o ciberespaço apenas como lugar ou local do crime, mantendo-se as condutas idênticas ao que ocorre no ambiente físico. Tal característica amplia significativamente o universo dos crimes cibernéticos. Com avanço crescente e desordenado, a Internet passou a ser universalmente um lugar comum para pessoas de todas etnias, crenças, idades e visões de mundo diferentes, uma poderosa infraestrutura de comunicação instantânea e mais do que nunca, um reflexo da sociedade tradicional. Neste universo podem ser encontrados serviços, lazer, comércio, entretenimento, educação, comunicação, relações interpessoais, informação, conhecimento, notícias, publicidade, pesquisas, ciência, religião, transações financeiras, causas sociais e até mesmo os crimes. Muito rapidamente os criminosos perceberam na Internet um lugar propício ou, no mínimo, um canal facilitador à perpetração de crimes financeiros, fraudes, estelionatos, crimes de ódio e contra a honra, acesso indevido a informações privilegiadas, espionagem comum e industrial, exploração sexual de crianças e adolescentes, pirataria, comércio de produtos ilegais (armas, drogas, medicamentos) entre outros, tudo isso usando plataformas e tecnologias relativamente

* Artigo apresentado à Diretoria de Ensino de Pós-graduação, Pesquisa e Extensão, da UPIS, em cumprimento à exigência para conclusão de Segurança da Informação e Perícias em Crimes Cibernéticos, sob orientação do mestre professor Evandro Lorens. *

simples e acessíveis, e com interessantes benesses: não ser necessário estar fisicamente no local do crime; e, aparentemente, um certo grau de anonimato. Novos tipos de crimes surgiram, caracterizados por apenas serem possíveis em ambientes informatizados, tendo sido denominados crimes puros ou próprios de Internet: invasão e danos de sistemas informatizados; inserção de dados falsos em sistema de informações; roubo de arquivos; sequestro lógico de computadores ou terminais com finalidade de produzir outros ataques coordenados contra alvos específicos.

A explosiva popularização do e-mail, das plataformas de comunicação executadas sobre a Internet e das redes sociais incluiu milhões de pessoas em conectividade e, simultaneamente, expôs aos criminosos milhões de potenciais vítimas. São pessoas comuns que passaram a usar a Internet como plataforma de serviços e de comunicação, sem nenhuma ou quase nenhuma preocupação com segurança de dados pessoais e transacionais. Essa exposição teve como consequência lógica o aumento crescente de crimes cibernéticos no Brasil e no mundo. De acordo com a SAFERNET (2017), no Brasil, no ano de 2016, foram recebidas e processadas por meio da CND (Central Nacional de Denúncias) mais de 115.000 denúncias de ocorrências de crimes de ódio como: racismo, apologia ao nazismo, homofobia, xenofobia, apologia ao crime, além de pornografia infantil e aliciamento de pessoas pela Internet. No Distrito Federal, os crimes relacionadas a fraudes bancárias somaram mais de 26.000 processos executados ou arquivados entre o ano de 2013 e julho de 2018, de acordo a Delegacia de Repressão aos Crimes Cibernéticos da Polícia Civil do Distrito Federal (DRCC/PCDF), e com o Núcleo de Estatística da Primeira Instância do Tribunal de Justiça do Distrito Federal e Territórios (NUEST/TJDFT). Os números revelam o grande interesse dos criminosos pelas plataformas digitais e, indiretamente, a dificuldade do poder público em prevenir e reprimir esses crimes, seja por falta de estrutura, e/ou por falta de pessoal qualificado para atuar nesse campo.

CRIMES CIBERNÉTICOS

Segundo BARRETO (2016), crimes cibernéticos são crimes praticados através ou por meio de "*tecnologias (computador, internet, caixa eletrônicos), sendo em regra, crimes meios – ou seja, apenas a forma em que são praticados é que é inovadora, ... onde, apesar de se concretizarem em ambientes virtuais, os delitos trazem efeitos no mundo real*". Ainda segundo o autor, "*os cibercrimes na grande maioria das vezes se caracterizam por serem plurilocais, quando vítima e agente estão em locais distintos, ou, ainda, quando a execução do delito se inicia em um lugar e a consumação ocorre em outro, mas no mesmo país*".

Para SHIMABUKURO (2017), "*apesar de o conceito de ciberespaço não abranger um corpo físico ou espaço geográfico, ele representa uma construção social feita à imagem e semelhança do mundo físico. O ciberespaço conecta redes, equipamentos e principalmente pessoas [...]*. A partir dessa visão reflexiva do ciberespaço em relação ao mundo físico, a autora sugere que os crimes cibernéticos atuais do cenário virtual brasileiro "*não chegam a ser tão sofisticados*". Para Adriana Shimabukuro, a baixa cultura em segurança da informação de grande parte da população usuária de sistemas informatizados e da Internet no Brasil é refletida na baixa complexidade das fraudes e golpes, que funcionam satisfatoriamente e com baixo risco de exposição ou captura para os criminosos. Em outras palavras, obter ganhos com atividades criminosas Internet no Brasil não demanda muito esforço, uma vez que os usuários não demonstram preocupação nem preservam a própria segurança no ambiente virtual. Muitas vezes, esses mesmos usuários não conseguem sequer perceber que foram vítimas de algum tipo de fraude ou golpe.

Além da "inconsciência" dos usuários brasileiros em relação aos riscos de se tornarem vítimas de cibercriminosos, um outro aspecto tem propiciado e potencializado as atividades criminosas na Internet brasileira: a superexposição dos usuários nas redes sociais, produzida pela ação dos próprios usuários que, ao compartilharem abertamente textos, fotos, vídeos e áudios, revelam seus hábitos, seu patrimônio, suas relações familiares e afetivas, seus ambientes de frequência, suas rotinas e também as suas fragilidades. Informações pessoais das vítimas são demandas óbvias dos criminosos, especialmente nos furtos de identidades para cometimento de fraudes comerciais e financeiras usando os dados dessas vítimas. Em uma outra obra BARRETO (2017), considera que "*com a popularização desses sites – mídias sociais -, os frequentadores passaram a postar fotografias, vídeos, informações pessoais, endereços e números de telefone – dados estes bastantes úteis e facilitadores para qualquer ação criminosa"*.

Numa outra vertente perniciosa da superexposição nas redes sociais são catalisados os crimes de exploração sexual de crianças e adolescentes, especificamente a prática da pornografia e abuso infantil. Abusadores dispõem, com facilidade, de farto material (fotos vídeos, locais, etc.) publicado inadvertidamente nas redes sociais pelas próprias crianças e adolescentes, e por seus familiares. A abundância e a riqueza de informações facilitam o encaminhamento de aproximação, abordagem e aliciamento das vítimas, explorando o seu próprio mundo, prévia e abertamente compartilhado nas redes sociais. De acordo com LOTUFO (2017), "*a Internet é o meio para arregimentação de organização criminosa, preparação de crime doloso, e, em muitos casos, como, por exemplo, nos arts. 241-A e 241-B do ECA, pode vir a ser o instrumento e o local de consumação dos delitos.*". Os caputs dos artigos 241, 241-A, 241-B e 241-C da Lei 8069/90 (Estatuto da Criança e do Adolescente – ECA) assim prescrevem como crimes:

> *Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)*
>
> *...*
>
> *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: (Incluído pela Lei nº 11.829, de 2008)*
>
> *...*
>
> *Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)*
>
> *...*
>
> *Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008)*

A irrealidade do suposto anonimato no ambiente da Internet tem demandado esforços dos criminosos na busca por técnicas que inviabilizem ou pelo menos dificultem o trabalho policial de investigação e perícia dos crimes cibernéticos. Nessa toada, sistemas complexos de criptografia disposta em camadas e configuradas em redes de computadores distribuídos têm sido empregados para ocultação do tráfego de dados e das informações trafegadas. Tais sistemas têm sido referenciados como componentes da *Dark Web*, cujo representante mais conhecido é o navegador Tor (*The Onion Router),* um projeto iniciado em 2002, financiado inicialmente pela marinha americana, com intuito de prover comunicação anônima na Internet, e atualmente mantido por voluntários. Por meio da comunicação na *Dark Web* são alcançados, por exemplo, ambientes virtuais de vendas de drogas ilícitas, vendas ilegais de armas, pornografia infantil, encomendas de assassinatos, tráfico de pessoas, venda de informações sigilosas, ações políticas

fundamentalistas voltadas ao terrorismo, espionagem industrial, entre outros. LOTUFO (2017) destaca que nesse contexto, a Internet, como reflexo do nosso mundo físico, pode ser usada para qualquer fim, "*...para o ser humano extravasar o que tem de pior dentro de si.*", e completa: "*apenas para citar algumas situações: tortura por encomenda, fóruns de canibalismo, pornografia grotesca, pedofilia, grupos extremistas, hitmans (contratação de assassinos), venda livre de drogas e vídeos snuffs (termo utilizado para filmagens de homicídios premeditados, geralmente feito próprio assassino com cenas de extrema brutalidade e violência)*". A figura 1 mostra um infográfico com as representações de ambientes de comunicação da Internet classificados por percentual de volume de conteúdo e por tipos de conteúdo de cada ambiente.

FIGURA 1 – REPRESENTAÇÃO DOS AMBIENTES DE COMUNICAÇÃO DA INTERNET
(elaborado pelo autor)

LEGISLAÇÃO BRASILEIRA

O senso comum costuma designar "crime" toda conduta que confronta um determinado arcabouço ético estabelecido de um grupo social. Com os crimes cibernéticos não é diferente, e qualquer conduta que represente algum desvio ético é classificada pelo cidadão comum como crimes cibernético. Entretanto, a rigor, crime é tão somente toda conduta ilícita tipificada em legislação própria. No caso da República Federativa do Brasil, crimes são as condutas tipificadas no Código Penal Brasileiro. BARRETO (2016), relaciona os principais como crimes cibernéticos tipificados na legislação brasileira, sendo os próprios aqueles que só podem ser cometidos por usuários de sistemas informatizados e os impróprios são aqueles em que o computador é usado como instrumento para a execução do crime, porém não há ofensa ao bem jurídico "*... inviolabilidade dos dados ou informações".* VIANA (2003):

> "***Puros e próprios:*** *Art. 154-A - Invasão de dispositivo informático; Art. 163 – Dano; Art. 266 – Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública; Art. 313-A – Inserção de dados falsos em sistemas de informações; Art. 313-B – Modificação ou alteração não autorizada de sistema de informações. ". "****Impuros ou impróprios:*** *Arts. 241 e ss. Do E.C.A; Art. 20 da Lei nº 7.716/89 – Preconceito ou discriminação de raça, cor, etnia, etc.; Art. 122 do CPB – Induzimento, instigação ou auxilio a suicídio; Art. 138 do CPB – Calúnia; Art. 139 do CPB – Difamação; Art. 140 do CPB – Injúria; Art. 147 do CPB – Ameaça; Art. ". BARRETO, Alessandro Gonçalves (2106).*

A legislação brasileira prevê em vários dispositivos*"... princípios e garantias do uso da tecnologia pelos cidadãos em suas diversas relações e para o desenvolvimento do país ...*" (BARRETO, 2016). Em contrapartida, também há previsão em outros tantos dispositivos legais para enquadramento dos crimes cibernéticos. Considerada a competência da legislação federal para tratar dos crimes cibernéticos, podemos relacionar os seguintes diplomas legais do arcabouço legal brasileiro com pertinência nessa temática:

- Código Penal Brasileiro (CPB) Del nº 2.848, de 07.12.1940;
- Código de Processo Penal (CPP) Del nº 3.689, de 03.10.1941;
- Código de Processo Civil (CPC) Lei nº 13.105, de 2015;
- Código de Defesa do Consumidor (CDD) Lei nº 8.078, de 11.09.1990;
- Código Brasileiro de Telecomunicações (CBT) Lei nº 4.117, de 27.08.1962;
- Estatuto da Criança e do Adolescente (ECA) Lei nº 8.069, de 13.07.1990;
- Lei 9.983, de 14.07.2000, que acrescenta no CPB os Art. 313-A e Art. 313-B;
- Lei 12.737 de 30.11.2012, mais conhecida como Lei Carolina Dieckmann acrescentando ao CPB os artigos Art. 154-A e Art. 154-B, e alterando a redação dos artigos Art. 266 e Art. 298;
- Lei 12.965, de 23.04.2014, conhecida como Marco Civil da Internet.

Especificamente a Lei 12.965/2014, conhecida como Marco Civil da Internet, se propôs a regulamentar o uso da Internet no Brasil, provisionando princípios, garantia, direito e deveres para todo usuário e qualquer sistema que utilize a rede, e determinando as diretrizes para atuação do Estado. Não trata de tipificação criminal, mas estabelece direitos e deveres dos usuários da Internet brasileira. É composta por 32 (trinta e dois) artigos, divididos em 5 (cinco) capítulos: *Disposições preliminares; Dos direitos e garantias dos usuários; Da provisão de conexão e aplicações da Internet; Da atuação do poder público; e Disposições Finais.* Um dos conceitos mais importantes estabelecidos pela Lei 12.965/2014 é o Princípios da Neutralidade da Rede que estabelece igualdade de prioridade de tráfego a todos os serviços de rede comerciais

hospedados em território nacional, o que significa que não se pode exercer cobranças diferenciadas por serviços com base em prioridade de tráfego comercial que, na prática, não pode existir.

MATERIAIS E MÉTODOS

O desenvolvimento deste trabalho pautou-se primariamente na pesquisa do tipo bibliográfica, conforme classificam (PRODANOV e FREITAS, 2013). As fontes constituem-se primordialmente de material previamente publicado: livros, periódicos, artigos científicos e legislação brasileira. Os recortes essenciais desses materiais contribuíram para a exposição abrangente da temática Crimes Cibernéticos, depois de revisada e analisada sob várias óticas literárias complementares.

A focalização dos dados de crimes cibernéticos do Distrito Federal deu-se a partir da análise dos dados solicitados pelo autor aos órgãos de segurança pública e de justiça do Distrito Federal e fornecidos com base na Lei 12.527/2011 (LAI – Lei de Acesso à Informação).

A finalidade do trabalho é discutir os crimes cibernéticos e contextualizar o Distrito Federal nesse universo, evidenciando as informações obtidas por meio da análise dos dados coletados, e oferecendo uma visão específica para o contexto geográfico e político local. Baseou-se no método científico dedutivo, assim classificado por GIL (2008), adotando uma abordagem de natureza qualitativa para dados quantitativos e qualitativos previamente consolidados.

RESULTADOS: OS CIBERCRIMES NO DISTRITO FEDERAL

O Distrito Federal é a menor unidade da federação brasileira em área territorial, com 5,802 km², e ocupa a vigésima posição em contingente populacional com quase três milhões de habitantes em 2018 ou 1,4% da população brasileira. (IBGE, 2018). Em termos de rendimento nominal mensal per capita da população residente, ocupa a primeiro lugar entre as unidades da federação com R$ 2.548 no ano de 2017, aproximadamente o dobro da média nacional de R$ 1.268. (IBGE2, 2018). A liderança neste quesito diferencia o Distrito Federal, entre outros aspectos, como unidade com alta oferta e consumo de serviços de conectividade à Internet: é a unidade da federação que mais utiliza a internet no Brasil. Segundo dados da Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad), divulgada em 2018 pelo Instituto Brasileiro de Geografia e Estatística (IBGE), 85,3% da população local acessou a web no último trimestre de 2016, quando os dados foram coletados. O índice superou a média do país, de 64,7%, em mais de 20 pontos percentuais (IBGE3, 2018). Como a unidade da federação mais conectada, por uma população de poder aquisitivo acima da média, é natural que apareça como um campo fértil para os crimes cibernéticos, especialmente aqueles contra pessoas, no contexto da honra ou financeiro.

De acordo com os dados da Secretaria de Segurança Pública do DF (SSP/DF) e da Polícia Civil do Distrito Federal, quase metade das ocorrências de crimes cibernéticos são aqueles praticados contra a honra (Arts. 138, 139 e 140 do CPB). Em segundo lugar, aparecem os estelionatos virtuais e as ameaças. Em franco e preocupante crescimento, destacam-se as técnicas de *phishing*, usadas para furtar dados pessoais e credenciais de usuários de sistemas bancários, e-mails, redes sociais, sites de comércio eletrônico, entre outros. Grosso modo, os criminosos enviam por mensagens eletrônicas (SMS, WhatsApp, e-mail, etc.) com mensagens falsas com algum

tipo de apelo e links que apontam para páginas falsas, a partir das quais os dados dos usuários são coletados e/ou sistemas de *malware* instalados nos equipamentos desses usuários, viabilizando os golpes.

Considerando os crimes contra a honra, ainda de acordo com a SSP/DF, as ocorrências de crime de Injúria Racial, tipificado no art. 140, §3º, do CPB, e que consiste em ofender a honra utilizando elementos referentes à raça, cor, etnia, religião e/ou origem, tiveram um crescimento de 3,4% no DF, em comparação com o mesmo período em 2017. As ocorrências aparecem em todas as 31 regiões administrativas, sendo o Plano Piloto o líder em números absolutos. No total, os crimes de racismo no DF, em 2014 foram 299 crimes registrados e em 2018, só no primeiro semestre, já foram registrados 211. (GDF/GAB/SSPDF – COOAFESP/SGI, 28, ago., 2018).

É também digna de nota a quantidade de crimes cibernéticos perpetrados e registrados contra mulheres no Distrito Federal. No grupo dos crimes de assédio moral e psicológico (injuria, difamação, ameaça, etc.), de janeiro a junho de 2018, foram registradas 4.968 ocorrências com vítimas mulheres. Os crimes de danos, violação e furto de dados contra elas, no mesmo período, totalizaram 805. De 2010 até 2018, a ocorrência desses crimes cibernéticos contra mulheres mais do que triplicou. (GDF/GAB/SSPDF–COOAFESP/S GI, 23, jul., 2018).

Os números alarmantes dos últimos anos, levaram o Governo do Distrito Federal a criar, em 19 de maio de 2017, a Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC), que funciona desde então, dentro do Departamento de Polícia Especializada (DPE) no Parque da Cidade. O principal objetivo é dar apoio, esclarecer casos de crimes cibernéticos registradas por autoridades e pelo público em geral. Da data de sua criação até 21 de agosto de 2018, somente na DRCC foram registradas 196 (102 em 2018) ocorrências que se desdobraram em 80 inquéritos relacionados a diversas condutas. De acordo com a DRCC, esses números ainda são baixos, pelo fato de a população desconhecer a Delegacia Especializada, e ainda, por muitas pessoas sequer saberem que foram vítimas de um crime cibernético (PCDF/DGI/DATE/SE/Polaris, 2018).

Pela ótica da justiça, é possível avaliar os números de processos relacionados aos crimes cibernéticos no Distrito Federal. De acordo com o Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), por meio do Núcleo de Estatística da 1º Instância – NUEST/TJDFT, entre 2013 e junho de 2018, foram abertos 39.273 processos, sendo que em alguns processos pode haver mais de um crime relacionado, de modo que a soma de crimes é maior que números de processos. Em ordem decrescente, os números de processos, por assunto ou crime principal são os seguintes:

- 35.264 processos relacionados a fraudes bancárias e financeiras pela Internet;
- 3.988 processos relacionados a propriedade intelectual;
- 15 processos sobre inserção de dados falsos em sistemas de informação;
- 6 processos relacionados a falhas ou danos em software.

É importante ressaltar que não são contabilizados como processos relacionados a crimes cibernéticos os processos referentes a crimes impróprios, como por exemplo, os crimes contra a honra. Também não aparecem os processos relacionados a pornografia infantil, de competência da Justiça Federal (BRASIL, TJDFT, 2018).

Outro dado do TJDFT que denota a complexa relação da justiça com as demandas judiciais relacionadas à tecnologia é o número de peritos judiciais privados cadastrados como habilitados para atender às demandas dos magistrados. No TJDFT são apenas 162,

número incompatível com a demanda atual de casos em andamento naquele tribunal.

No âmbito de atuação da Polícia Federal no Distrito Federal, merecem destaque operações nacionais frequentes relacionadas a crimes cibernéticos, que incluem alvos também no Distrito Federal. São operações sobre pornografia infantil, fraudes bancárias, fraudes fiscais, notícias falsas, racismo, ameaça e incitação ao crime, praticados via internet pela Internet (BRASIL, Polícia Federal, 2018). De acordo com o Instituto Nacional de Criminalística (INC-PF, 2018), localizado no Distrito Federal, o número de laudos periciais elaborados no Distrito federal relacionados a crimes de pornografia infantil pela Perícia Criminal Federal, de outubro de 2017 a setembro de 2018, foi de 132.

CONSIDERAÇÕES GERAIS

Observando toda a fundamentação teórica relacionada a crimes cibernéticos pesquisada, em confronto com os números oficiais dos órgãos de segurança pública e tribunais do Distrito Federal, verifica-se que muito se trabalha para solucionar tais crimes. Todos os anos, são milhares de ocorrências registradas, investigadas, denunciadas, processadas e periciadas. Na contramão desses números de combate ao crime, percebe-se um aumento consistente ano após ano das ocorrências dos crimes cibernéticos, ressalvados aqueles que se reduzem pela migração dos criminosos para outras modalidades de crime, motivados por fatores externos ou por melhores oportunidades de ganhos surgidas.

Uma outra análise dos dados, com viés mais social, demonstra o quanto a sociedade do Distrito Federal como um todo ainda não se dá conta de quão prejudiciais à nossa sociedade, e à economia são os crimes cibernéticos e, além, toda a sociedade perceber a importância da formação permanente de profissionais qualificados, nas searas pública e privada, que possam lidar com os crimes cibernéticos para preveni-los, combate-los, fazer cumprir a lei e efetivamente produzir justiça.

Nosso arcabouço jurídico precisa ser modernizado em todo o tempo, para enfrentar, com desenvoltura, os novos desafios impostos pelos avanços tecnológicos que, infelizmente, também se tornam disponíveis aos criminosos enquanto integrantes da nossa sociedade.

Investimentos em infraestrutura, em equipamentos, sistemas e treinamentos também são componentes essenciais para reversão do quadro apresentado pelos números dos crimes cibernéticos no Distrito Federal.

Por fim, outra abordagem social nos remete ao fato de que precisamos investir em educação digital, com foco sério em segurança da informação, de modo a reduzir a facilidade encontrada pelos criminosos para atuar e consequentemente, reduzir a incidência de crimes cibernéticos, em números absolutos e relativos. A forma adequada de lidar com os meios digitais e a capacidade de preservar informações pessoais a salvo de superexposição têm real potencial para ajudar a reduzir a criminalidade cibernética no Distrito Federal. Tais competências só serão possíveis quando as pessoas, as empresas, as organizações, os governos e toda a sociedade civil fizerem opção pela educação digital, cada qual em seu nicho de atuação, fortalecendo a maturidade dos usuários no trato com a tecnologia.

Artigo apresentado à Diretoria de Ensino de Pós-graduação, Pesquisa e Extensão, da UPIS, em Segurança da Informação e Perícias em Crimes Cibernéticos.

EFERÊNCIAS BIBLIOGRÁFICAS

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. 2016. **Manual de investigação cibernética:** à luz do Marco Civil da Internet. Brasport, Rio de Janeiro, Brasil, 2016.

BARRETO, Alessandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme. 2017. **Investigação Digital em fontes abertas**. Brasport, Rio de Janeiro, Brasil, 2017.

BRASIL. **Presidência da República Casa Civil:** Códigos. Disponível em <http://www.planalto.gov.br/ccivil_03/Codigos/quadro_cod.htm>. Acessado em 27, set., 2018.

BRASIL. **GDF: Polícia Civil do Distrito Federal: Departamento de Gestão da Informação:** Inquérito Policiais instaurados, Delegacia de Repressão aos Crimes Cibernéticos. Período, 2017 e 2018.

BRASIL. **Presidência da República Casa Civil: Lei nº 9.983, de 14 de julho de 2000**. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/L9983.htm>. Acessado em 27, set., 2018.

BRASIL. **Presidência da República Casa Civil: Lei nº 12.737, de 30 de novembro de 2012**. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acessado em 27, set., 2018.

BRASIL. **Presidência da República Casa Civil: Lei nº 12.965, de 23 de abril de 2014**. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em 27, set., 2018.

BRASIL. **Governo do Distrito Federal**: **Secretaria de Estado de Segurança Pública e Paz Social: Subsecretaria de Gestão a Informação, Informações Estatísticas nº 077/2018**. Disponível em <http://www1.ssp.df.gov.br/wp-conteudo/uploads/2018/03/Estat%C3%ADstica-077_2018-Inj%C3%BAria-racial-e-Racismo-no-DF_1%C2%BA-semt_18-e-%C3%BAltimos-anos.pdf>. 28, de agosto de 2018. Acessado em 28, de set., 2018.

BRASIL. **Governo do Distrito Federal**: **Secretaria de Estado de Segurança Pública e Paz Social: Subsecretaria de Gestão a Informação, Análise de Fenômenos de Segurança Pública nº. 072/2018**. Disponível em <http://www.ssp.df.gov.br/violencia-contra-a-mulher/>. 23, de junho de 2018. Acessado em 28, de set., 2018.

BRASIL. **Polícia Federal**: **Agência de Notícias**. Disponível em <http://www.pf.gov.br/agencia/noticias/2015/12/operacao-ufrap-combate-cri mes-ciberneticos-no-df-e-no-goias>. Acessado em 04, de out., de 2018.

BRASIL. **Tribunal Regional Federal da 3ª Região. Escola de Magistrados: Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017. 352p. (Cadernos de estudos; 1).

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 1999.

GLOBO.COM: **G1, PF combate em GO, DF e mais três estados fraudes bancárias na web**. Disponível em <http://g1.globo.com/goias/noticia/2017/03/pf-combate-crimes-ciberneticos-em-goias-df-e-mais-tres-estados.html>. Acessado em 04, de out., de 2018.

IBGE, **Projeção da população do Brasil e das Unidades da Federação**, disponível em <https://www.ibge.gov.br/apps/populacao/projecao/>. Acessado em 01, de nov., de 2018.

IBGE2, **Valores dos rendimentos domiciliares per capita referentes a 2017 para o Brasil e Unidades da Federação, calculados com base na Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua)**, disponível em <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20154-ibge-divulga-o-rendimento-domiciliar-per-capita-2017>; Acessado em 01, de nov., de 2018.

IBGE3, **Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua – Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal**. Disponível em <ftp://ftp.ibge.gov.br/Trabalho_e_Rendimento/Pesquisa_Nacional_por_Amostra_de_Domicilios_continua/Anual/Acesso_Internet_Televisao_e_Posse_Telefone_Movel_2016/Analise_dos_Resultados.pdf>. Acessado em 01, de nov., de 2018.

INC-PF – **Instituto Nacional de Criminalística** – **Dados do Sistema Criminalística**, 2018.

INTERNET WORLD STATS. ***Usage and Population Statistics***: Estatísticas sobre uso e população da Internet para a América do Sul, 31 de dezembro de 2017. Disponível em: <https://www.internetworldstats.com/south.htm#top>. Acessado em 26, set., 2018.

LOTUFO, Renata Andrade. **Crimes cometidos contra a vulnerabilidade sexual de crianças e adolescentes no ECA e no Código Penal: a Internet como forma de cometimento e aproximação do sujeito ativo e vítima**. São Paulo: EMAG, 2017. p. 255 (caderno de estudos; 1).

POZZEBOM Rafaela. **Quais são os crimes virtuais mais comuns?** Disponível em <https://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns>. Acessado em 27, de set., de 2018.

PRODANOV, Cleber Cristiano.; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico [recurso eletrônico]: métodos e técnicas da pesquisa e do trabalho acadêmico**. – 2. ed. – Novo Hamburgo: Feevale, 2013.

SAFERNET. **Indicadores de crimes denunciados**. Disponível em: <http://indicadores.safernet.org.br/indicadores.html>. Acessado em 21, de mai., de 2018.

SALVADORI, Fausto. **Revista Galileu: Tecnologia / Internet:** Crimes virtuais. Disponível em <http://revistagalileu.globo.com/Revista/Common/0,,EMI110316-17778,00-CRIMES+VIRTUAIS.html>. Acessado em 27, de set., de 2018.

SHIMABUKURO, Adriana. **Cibercrime: quando a tecnologia é aliada da lei**. São Paulo: EMAG, 2017. p. 17 (cadernos de estudos; 1).

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003