PROSPECÇÃO SOBRE A EVOLUÇÃO E O FUTURO DOS CRIMES CIBERNÉTICOS

FABRÍCIO RABELO PATURY
Coordenador

AUTORES

Aline Maria Proence Pereira Lopes
Bárbara Emily Ribeiro de Oliveira
Carlos César Carqueija Júnior
Daniela Santos Dias
Eloah Lucena Bicalho
Filipe Hamilton Zani
Guilherme Celestino Conceição Tadeu
Leandro dos Anjos Figueiredo
Livanilda Vieira Pereira Meneses
Maiara Cruz de Oliveira
Marcella Almeida Brandão Rebouças
Renata Lorena Almeida Brandão Rebouças

PROSPECÇÃO SOBRE A EVOLUÇÃO E O FUTURO DOS CRIMES CIBERNÉTICOS

2019

FACULDADE BAIANA DE DIREITO

P966 Prospecção sobre a evolução e o futuro dos crimes cibernéticos / coordenador, Fabrício Rabelo Patury. – Salvador : Faculdade Baiana de Direito, 2019.
185 p.

Vários autores.
Bibliografia.
ISBN 978-85-62756-75-7.

1. Crime cibernético. 2. Crime por computador. I. Patury, Fabrício Rabelo. II. Título.

CDD 345.0268

Diagramação: SO Editoração Eletrônica (soeditoracaoeletronica@gmail.com).
Capa: Salamandra

Conselho Editorial:

Profª Drª. Ana Carolina Fernandes Mascarenhas
Profª Drª. Ana Thereza Meirelles
Prof. Dr. Antonio Adonias Aguiar Bastos
Profª Drª. Cláudia Albagli Nogueira
Prof. Dr. Dirley da Cunha Jr
Prof. Dr. Fredie Didier Jr
Prof. Dr. Gabriel Marques da Cruz
Prof. Dr. Gamil Föppel el Hireche
Profª Drª. Maria Auxiliadora Minahim
Prof. Dr. Maurício Requião
Prof. Dr. Valton Dória Pessoa

Todos os direitos desta edição reservados à Faculdade Baiana de Direito.
Copyright: Faculdade Baiana de Direito.
É terminantemente proibida a reprodução total ou parcial desta obra, por qualquer meio ou processo, sem a expressa autorização do autor e da Faculdade Baiana de Direito. A violação dos direitos autorais caracteriza crime descrito na legislação em vigor, sem prejuízo das sanções civis cabíveis.

FACULDADE BAIANA DE DIREITO

Rua Visconde de Itaborahy 989,
Amaralina, Salvador – Bahia
(71) 3205-7700 / Fax: (71) 3240-3552
contato@faculdadebaianadedireito.com.br
www.faculdadebaianadedireito.com.br

SUMÁRIO

APRESENTAÇÃO

Fabrício Rabelo Patury[1]

É com enorme satisfação que apresento, como coordenador do Grupo de Estudos de Direito Digital da Faculdade Baiana de Direito, este importante trabalho, como resultado da dedicação e pesquisa extremamente qualificadas dos integrantes do primeiro ciclo.

Este livro é fruto de zelosa lapidação, esmero ímpar e esforço individual e coletivo dos integrantes, cabendo ao professor que subscreve esta apresentação a honra de orientar e coordenar os trabalhos do grupo.

A ideia de criar um Grupo de Estudos em Direito Digital nasceu da vertente inovadora da coordenação da Faculdade Baiana de Direito - ressaltando que a inovação é viga mestra dos princípios que regem esta Faculdade - que, debruçando-se sobre os desafios que a nova sociedade digital trouxe à evolução do Direito, vislumbrou a efetiva necessidade acadêmica em estudar, refletir e produzir conhecimento sobre a matéria.

No âmbito do imenso espectro de possibilidades de temas de Direito Digital, após profundas análises de teses polêmicas e palpitantes, elegeu-se como temática deste Primeiro Grupo de Estudos a "Prospecção sobre a Evolução e o Futuro dos Crimes Cibernéticos". Talvez o leitor esteja se perguntando: Mas porque este foi o eleito?

---

1 Promotor de Justiça do Estado da Bahia. Coordenador do Curso de Pós Graduação presencial em Direito Digital da Faculdade Baiana de Direito. Professor da disciplina Direito Digital na Faculdade Baiana de Direito. Especialista em Ciências Criminais pela UGF-RJ. Ex-coordenador do Núcleo de Combate aos Crimes Cibernéticos do MPBA.

Nesta nova sociedade digital, ciberataques de grandes proporções mundiais, como o WannaCry e o Petya, reafirmaram a urgência em se preparar para a expansão do cibercrime. Dia a dia, a hiperconexão tem incrementado de forma exponencial o número, a forma e os tipos de delitos. Os cibercriminosos atualizam continuamente suas técnicas para incorporar as mais recentes tecnologias em sua forma de agir - estão sempre à frente, em constante evolução. As forças de segurança, sobrecarregadas com o combate à criminalidade tradicional, acabam por retardar a evolução na capacitação de seus integrantes e na estruturação para o enfrentamento nova criminalidade cibernética, sendo que esta demora - mais cedo ou mais tarde (provavelmente mais cedo) - se tornará insustentável e colocará em xeque o modelo de persecução estatal.

É fato que caminhamos para uma sociedade hiperconectada, onde os fatos e condutas da vida estarão praticamente todas - de alguma forma - vinculadas a dispositivos informáticos. E quanto mais conectamos nossas vidas, por meio de *smartphones*, mídias sociais, internet das coisas, carros autônomos, entre outros, mais vulneráveis nos tornamos.

Crackers profissionais ou mesmo criminosos com pouco conhecimento (mas que adquirem as ferramentas de cibercrime na grande rede mundial) estão migrando para a ilicitude no âmbito digital. Cientes de como as tecnologias funcionam, passam explorar as vulnerabilidades técnicas e humanas dos cidadãos comuns, que se limitam ao uso da tecnologia, sem terem sido devidamente educados digitalmente para fazer frente a esta nova realidade.

Basta um olhar atento para o futuro que verificaremos como a ubiquidade da computação em nossas vidas, bem como a nossa crescente dependência dos dispositivos informáticos e da internet, estão efetivamente nos deixando vulnerabilizados. Embora as vantagens do mundo *online* sejam inegáveis, toda esta hiperconectividade está nos colocando de forma digitalmente exposta, seja nas mais simples tarefas realizadas em uma casa inteligente, seja nos dados pessoais sensíveis lançados em redes sociais, seja até mesmo nas robustas tarefas executadas por plataformas digitais de estruturas críticas para o funcionamento da sociedade (entre elas as redes elétricas, redes de controle de tráfico aéreo, empresas petroquímicas, etc.).

O uso massivo de redes sociais, mensageiros instantâneos e aplicativos de funcionalidades levou o conceito de privacidade e intimidade na Internet a uma flexibilização extremamente perigosa. O usuário não é o cliente: é o produto. Paga o uso do serviço com a entrega de seus dados pessoais sensíveis que o transformam em objeto de monetização. Para além dos riscos de roubos de dados, perfis fakes, entre outros, é fato que a superexposição provocada pela evasão voluntária da vida pessoal é uma "tempestade perfeita" para a proliferação de stalkers, cyberbulling, pedófilos, estelionatários, racistas, homofóbicos, entre outros.

E se já não bastasse o enorme desafio que já é atual, a cada dia surgem novas tecnologias – tais como a robótica, inteligência artificial, DPA, nanotecnologia, computação ubíqua - que levam para o futuro um potencial sem precedentes de novas fronteiras para o crime. Um verdadeiro arsenal de ameaças a segurança marcha em ritmo acelerado. Há uma nova civilização profundamente interligada sendo construída, mas, ao mesmo tempo, tecnologicamente vulnerável. É este paradoxo que está sendo explorado por cibercriminosos usuais, pelo crime organizado cibernético e pelo submundo digital (que não se restringe à Deep Web).

Afinal, tempos modernos fazem nascer crimes modernos...

Lastreado nestes pensamentos, caro leitor, é que a temática "Prospecção sobre a Evolução e o Futuro dos Crimes Cibernéticos" foi escolhida pelo Primeiro Grupo de Estudos de Direito Digital. Identificou-se a necessidade de uma produção acadêmica que se debruçasse sobre estudos amplos e profundos da evolução da cibercriminalidade para compreender e revelar os riscos que representam e como devemos – cidadão e Estado – nos preparar para a enfrentar. Este livro se consolida como contribuição acadêmica que a Faculdade Baiana de Direito oferece à sociedade, neste tema tão importante.

O projeto-base foi construído com bastante apuro. Após sua convalidação pela Faculdade, foram efetuados os trâmites de edital e chamamento dos integrantes. Durante 01(um) ano, foram realizadas reuniões quinzenais, quando então materiais audiovisuais, artigos, livros, filmes, entre outros materiais que pudessem estar vinculado ao tema, foram trazidos para sala de aula. Noites de intensos estudos, questionamentos e aprofundados debates foram enriquecendo o saber do grupo, que amadurecia dia a dia.

Seis subtemas específicos foram escolhidos entre vários outros para lastrearem a elaboração de artigos acadêmicos. Escritos em duplas, forjados a partir de múltiplas e recíprocas contribuições dos integrantes, resultaram em primorosos trabalhos que consubstanciam o presente livro.

O artigo inaugural foi escrito pelos integrantes **Carlos César Carqueija** Júnior e **Maiara Cruz de Oliveira**. O tema escolhido foi: "A HIPERCONECTIVIDADE COMO INCREMENTO AOS CRIMES COMETIDOS NA INTERNET". Não por acaso, foi eleito para iniciar o presente livro, pelo fato de que dois são os caminhos mais nítidos que conduzem o futuro da evolução do crime cibernético: as novas modalidades de crime que nascem com o surgimento de novas tecnologias e o incremento quantitativo dos crimes a partir de um crescimento exponencial de novos usuários e/ou dispositivos a serem agregados à rede, inclusive os autônomos, fenômeno este denominado "hiperconectividade".

Demonstrou o artigo – com maestria - o que é a hiperconectividade, como ela tem contribuído para o incremento de delitos através de dispositivos in-

formáticos, quem são as pessoas mais afetadas, a evolução da prática desses ilícitos e como essa temática é tratada pelo sistema jurídico brasileiro, a fim de levantar questionamentos quanto ao desempenho do Poder Público no combate desses crimes, futuramente. O tema, realmente, dá o tom do que ainda está por vir em matéria de cibercriminalidade.

Acompanhando a ideia de hiperconectividade demonstrada no artigo anterior, bem como aprofundando a análise da cultura da superexposição e da evasão da privacidade e intimidade por parte dos usuários do ciberespaço, as integrantes **Marcella Almeida Brandão Rebouças e Renata Lorena Almeida Brandão Rebouças** se debruçaram sob o tema "A SUPEREXPOSIÇÃO NAS REDES E O ROUBO DE DADOS PESSOAIS VISANDO A PRÁTICA DE CRIMES". O Artigo teve por objetivo apontar os riscos e a evolução dos crimes cibernéticos com base no uso dos dados pessoais fornecidos pelo usuário, ante a cultura da excessiva exposição da vida pessoal em redes sociais.

O cibercrime está evoluindo para se tornar personalizado, como forma de eliminar - através de engenharia social refinada - desconfianças da vítima, que acaba enxergando veracidade no ardil empregado pelo delinquente cibernético. Usando-se dos dados pessoais coletados em fontes abertas, principalmente os evadidos pelos próprios usuários em redes sociais, ataques cibernéticos estão cada vez individualizados (com destaque para os phishings), tornando extremamente eficiente o golpe. Conclui o artigo pelo direcionamento de possíveis soluções visando minimizar esta problemática, conseguindo com sucesso transportar o leitor até muito próximo de sua realidade, de seus riscos e suas vulnerabilidades diárias quando do uso das redes sociais.

Avançando com base nas temáticas anteriores, o artigo escrito pelos integrantes **Filipe Hamilton Zani e Leandro dos Anjos Figueiredo** versaram sobre o tema "A MIGRAÇÃO DOS CRIMES PATRIMONIAIS PARA A INTERNET ANTE A CONSOLIDAÇÃO DO MERCADO PARALELO NA VENDA DE MALWARES E VULNERABILIDADES ZERO-DAY NA DEEP WEB". Os escritores buscaram abordar os mecanismos de invasão computacionais, tais quais malwares e vulnerabilidades zero-day, frente ao avanço da criminalidade em um ambiente deveras propício ao seu desenvolvimento, conhecido por *Deep Web*.

Temas como o expressivo crescimento do mercado paralelo da *Deep Web* no que diz respeito à vendas dos mecanismos de invasão computacionais, especialização dos criminosos que agem através da realização de crimes patrimoniais, bem como das organizações criminosas, favorecendo por conseguinte a migração e crescimento da criminalidade nos meios digitais, foram enfrentados com profundidade, abordando-se, ao final, os meios de combate a esse fenômeno e as dificuldades atuais e os problemas futuros que surgirão dessa relação.

Em simbiose com a temática do artigo anterior, as integrantes **Daniela Santos Dias e Livanilda Vieira Pereira Meneses** mergulharam no tema "O AVANÇO DAS FACÇÕES CRIMINOSAS TRADICIONAIS PARA A INTERNET OBJETIVANDO A VENDA DE PRODUTOS ILÍCITOS". Assunto deveras atual, as políticas nacionais e estaduais de segurança pública elegeram o enfretamento às facções criminosas como uma de suas prioridades, ante o enorme poderio na macrocriminalidade organizada. Conforme demonstrou o artigo, as facções criminosas também vêm ganhando força no território baiano, marcadas todavia – ao menos por enquanto - pela desorganização e falta de estrutura escalonada entre seus membros, mas que vem dominando bairros e comunidades baianas, em verdadeira guerra por domínio de territórios, que no futuro, podem ser o próprio ciberespaço.

Com brilhantismo, as escritoras analisaram o avanço das facções criminosas tradicionais para a internet, oportunizado em razão da massiva utilização de meios de dispositivos e plataformas eletrônicas, assim como na vulnerabilidade dos usuários e a facilidade de se obter dados pessoais por meio da engenharia social. Demonstrou-se o viés da migração da macrocriminalidade para o espaço cibernético. Ao fim, concluiu o artigo que essa prática adquirida no decorrer das atividades delitivas fez com que as facções viessem a se fortalecer, antevendo a possibilidade de vender produtos ilegais através do ciberespaço, não só na *surface web*, como também no lado obscuro da internet, a chamada *dark web*. Lugares até então pouco conhecidos de muitos, mas caracterizado por uma intensa interface comercial.

A preocuação com a criminalidade cibernética de alto nível de sofisticação e, por isso mesmo, de grande risco exponencial, mormente tendo como alvo as plataformas industriais e as infraestruturas críticas para o funcionamento social, fez como que as integrantes **Bárbara Emily Ribeiro de Oliveira e Eloah Lucena Bicalho** superassem as dificuldades e a raridade de material escrito sobre o tema e se lançassem no tema "VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS: CYBER ATAQUES E A NECESSIDADE DA OBRIGATORIEDADE DE "REPORT" NO BRASIL"**.** Embora pareça uma realidade distante do leitor à primeira vista, basta relembrar que no Estado da Bahia se encontra o maior complexo petroquímico da América Latina, sendo lá uma grande concentração de plataformas industriais de alto risco, todas informatizadas.

O artigo abordou de forma ampla todas as infraestruturas críticas, conceituando como aquelas compreendidas como de extrema importância para o país, pois o impacto do seu não funcionamento implica em consequências sociais, econômicas, podendo ainda, causar danos ambientais e para a segurança nacional. Efetuou profunda análise dos novos cenários cibercriminosos, identificando as possibilidades dessas ocorrências já estarem convergindo para atingir

as infraestruturas críticas nacionais, tendo em vista as comprovações e ataques que geraram grandes repercussões. As escritoras analisaram os mecanismos e vulnerabilidades do sistema informáticos que dirigem as infraestruturas críticas, identificando, de fato, os riscos de serem os próximos e/ou possíveis alvos desses ataques, os quais - se ocorrerem - ensejarão em prejuízos de grande escala para toda sociedade. Ao final defenderam o mecanismo de "report" como uma ferramenta obrigatória no Brasil, com a criação de um centro estadual de reportagem de ataques cibernéticos.

Fechando com chave de ouro, os integrantes **Aline Maria Proence Pereira Lopes e Guilherme Celestino Conceição Tadeu** desafiaram as complexidades técnico-jurídicas e se lançaram na escrita do tema "DA UBIQUIDADE COMPUTACIONAL PARA A REALIZAÇÃO DE CRIMES CIBERNÉTICOS". A complexidade restou demonstrada por ser o escrito que mais demandou texto para sua conclusão, mesmo com todo esforço de síntese dos autores. Laborou o artigo na análise da computação ubíqua, perpassando pelo conceito, evolução histórica e os ramos da computação que foram fundamentais para a origem da onipresença computacional, apresentando na sequência as áreas de aplicações da ubiquidade computacional contemporânea que impactam o cotidiano das pessoas.

O artigo demonstrou como a eficiência tecnológica tornou a internet um novo meio para a prática de novos delitos que não eram previstos na legislação, apresentando um estudo sobre o tratamento dado pelo Direito Penal brasileiro aos crimes cometidos com o auxílio dos sistemas computadorizados. Nas considerações finais, demonstrou como a utilização da computação ubíqua - tão presente em nosso mundo digital em que estamos todos imersos - expõe o indivíduo, o vulnerabilizando e potencializando os crimes futuros que poderão afligir nossa sociedade

Concluída esta apresentação, ressalto, outrossim, que a qualidade dos trabalhos e as palpitantes temáticas abordadas levarão os leitores, sem dúvidas, à inarredáveis reflexões sobre o futuro da criminalidade nessa nova sociedade digital na qual fazem parte. E justamente por isso, o Primeiro Grupo de Estudos em Direito Digital da Faculdade Baiana de Direito tem a honra e o prazer de entregar à sociedade esta contribuição, terminando ao final com uma indagação: Estaremos preparados para este futuro quando se fizer presente?

1

A HIPERCONECTIVIDADE COMO INCREMENTO AOS CRIMES COMETIDOS NA INTERNET

Carlos César Carqueija Júnior
e Maiara Cruz de Oliveira[1]

RESUMO: Este artigo visa mostrar, ainda que de maneira sucinta, o que é a hiperconectividade como ela tem servido de caminho para o cometimento de delitos através de dispositivos informáticos, como por exemplo, a pornografia de revanche e a fake news; mostrar quem são as pessoas mais afetadas, a evolução da prática desses ilícitos e como essa temática é tratada pelo sistema jurídico brasileiro, a fim de levantar questionamentos em relação a se o desempenho do Poder Público para combater esses crimes tem sido eficaz a ponto de haver, ou não, diminuição e até mesmo extinção na prática desses crimes futuramente, bem como abordar possíveis soluções a respeito de como enfrentar essas situações.

PALAVRAS-CHAVE: AVANÇO TECNOLÓGICO; HIPERCONECTIVIDADE; CRIMES CIBERNÉTICOS; EDUCAÇÃO DIGITAL.

1. INTRODUÇÃO

Com o advento da tecnologia, foram criados os primeiros computadores e, após alguns anos, os cientistas pensaram em criar uma rede que não tivesse um

1 Graduandos em Direito na Faculdade Baiana de Direito – 2018.2

comando central, mas que possibilitasse a unificação dos computadores a partir de diferentes locais. Foi assim que surgiu a internet (Arpanet).

O tempo foi passando e a tecnologia evoluía cada dia mais; juntamente a este avanço, foram surgindo dispositivos informáticos mais aprimorados, os aplicativos foram conquistando espaços, novas redes sociais foram surgindo, as informações passaram a chegar de maneira mais rápida e, com isso, a necessidade de inclusão ao mundo digital foi se tornando indispensável. Assim, as pessoas foram se inserindo nesse mundo digital e suas relações sociais e culturais foram se moldando a este novo espaço, permitindo, então, o surgimento de uma sociedade digital.

O avanço tecnológico trouxe contribuições positivas para a sociedade, sobretudo no que tange à facilidade na comunicação, mas devemos atentar para o uso consciente e responsável dos meios tecnológicos, como forma de evitar e, principalmente, de nos proteger de situações indesejadas.

A atração gerada por esses avanços tem fomentado o uso excessivo da internet, ou seja, pessoas que dedicam a maior parte do seu tempo para ficarem conectadas ao mundo virtual. Isto é o que chamamos de hiperconectividade.

Assim, analisaremos alguns problemas decorrentes desse uso em excesso da internet, como o cometimento de crimes contra a pessoa que eram praticados sem a utilização da internet e que passaram a ser praticados através do uso de dispositivos informáticos, a fim de demonstrar quais são as consequências disso no mundo jurídico e como tem se dado o enfrentamento dessas problemáticas.

Neste sentido, trataremos sobre a hiperconectividade como incremento à prática dos delitos cometidos na internet, abordando como exemplo alguns crimes contra a pessoa, para demonstrar as consequências dessa prática não apenas na sociedade e no mundo jurídico, mas também nas relações interpessoais, para que seja possível uma melhor compreensão da importância da educação digital e da qualificação de profissionais que atuam no combate à repressão desses crimes.

2. HIPERCONECTIVIDADE

Quando o primeiro e-mail foi enviado pelo protótipo da primeira rede de internet, a Arpanet, não se imaginava, ainda, as proporções que tal ação ocasionaria nos dias atuais. Entretanto, com a evolução da internet, o que se constata hoje é a total vinculação da nossa sociedade aos meios digitais, os quais são essenciais, atualmente, a todo o pensar e desenvolver de qualquer país. Por isso, cabe a nós, aqui, discutir, inicialmente, os termos dessa conexão atual, sem, no entanto, nos esquecer de, prospectivamente, analisar como essa situação pode

acarretar em eventuais crimes futuros e, portanto, comprometer nosso próprio desenvolvimento enquanto sociedade.

Segundo pesquisa do Facebook (2015), o acesso à internet no mundo vem crescendo a cada ano. Não obstante, vários autores e estudiosos do tema, a exemplo de Tom Chatfield, Marcelo Crespo e Patrícia Peck, vêm trazendo pesquisas para informar e alertar sobre o cuidado que devemos ter quanto ao uso desses meios, já que o acesso aos meios digitais sem a devida instrução desses sujeitos para que aprendam como lidar com a internet ocasiona vulnerabilidades com relação a diversos crimes, os quais serão tratados mais adiante.

Além disso, é inegável a alta conectividade das pessoas aos computadores, celulares e outros aparelhos digitais. Nesse sentido, é que a pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE) revela que o Brasil fechou 2016 com 116 milhões de pessoas conectadas à internet, o equivalente a 64,7% da população com idade acima de 10 anos. Em 2015, o mundo tinha 3,2 bilhões de pessoas conectadas à internet, segundo a União Internacional das Telecomunicações (UIT).

Frederico Vieira (2015, p. 127-128), doutor em comunicação social, analisa a questão dessa hiperconectividade e as relações atuais, trazendo, assim, a seguinte ideia:

> "Sujeitos-mensagens" não é um conceito delimitado, mas antes uma ideia provocativa, um questionamento acadêmico a priori sobre nossa condição existencial nesse mundo. O eu expandido do mundo contemporâneo se faz presente nas plataformas online, nas redes sociais da web; hoje o indivíduo, por meio de sua página virtual, para além de seu próprio suporte, é também o de seus interagentes; mas não como uma espécie de automídia, pois incorreríamos no risco de reduzi-lo a um canal, à modulação por onde a mensagem apenas "flui". Ao contrário, em rede, os sujeitos se compõem dos textos e das imagens que postam, que dão a ver, que tiram do interior de suas casas e levam a público. Mas que também se permitem ser apropriadas pelo outro, que o cutuca em rede, o curte, o comenta, o compartilha, o promove, o toma de empréstimo. Essas atitudes on-line são tácteis, e têm, não raro, efeitos inevitáveis sobre o mundo presencial, por mais díspares que as realidades on-line e offline possam parecer em alguns contextos. Nesse sentido, não podemos ignorar que, antes de possibilitar o acesso, viabilizar o encontro, disponibilizar um link ou conteúdo, nas plataformas online o sujeito é mensagem.

Portanto, é notório essa condição existencial, onde os sujeitos se tornam vinculados ao ambiente virtual. Porém, é preciso ressaltar que a hiperconectividade não atingiu seu ápice, visto que, segundo a UIT, ainda que o acesso tenha aumentado nesses 15 anos, ainda há um pouco mais de 3 bilhões de pessoas desconectadas em todo o mundo, sendo que o abismo é maior nos países menos

desenvolvidos, onde apenas 89 milhões de pessoas possuem conexão, de um total de 940 milhões.

No Brasil, não é diferente. Um relatório sobre economia digital divulgado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento apontou o Brasil como quarto lugar no ranking mundial de usuários da internet, com 120 milhões de pessoas conectadas. O Brasil fica atrás apenas dos Estados Unidos (242 milhões), Índia (333 milhões) e China (705 milhões). No entanto, esses dados não demonstram a relação do número de usuários com o número total da população do país. Se formos considerar o total de usuários em relação à população, o desempenho do Brasil é inferior. Segundo dados da União Internacional de Telecomunicações (UIT), o país tem 59% de usuários conectados, percentual inferior ao do Reino Unido (94%), Japão (92%), Alemanha (90%), Estados Unidos (76%) e Rússia (76%).

Assim, é preciso ter em mente que as consequências sentidas hoje por conta dessa hiperconectividade deverá aumentar, e muito, a sua intensidade pois, como demonstram as pesquisas, não temos, ainda, nem 50% de pessoas conectadas em todo o mundo. Sendo assim, verifica-se que a tendência mundial é o aumento da conectividade.

Sabemos e também sentimos todos os benefícios diários de uma sociedade conectada, quais sejam velocidade de informação e facilidade em busca de conteúdo, possibilidade de aproximação social, facilitação na comunicação em relação ao trabalho, dentre diversos outros benefícios. No entanto, esses benefícios não serão objeto de discussão, mas sim os males causados por um ambiente que pode ser extremamente nocivo, principalmente em uma sociedade que não tenha preparo, isto é, educação digital para lidar com tal ambiente.

Um dos grandes problemas que estamos enfrentando atualmente e que tende a piorar é o fato de a hiperconectividade intensificar os conflitos entre as pessoas, uma vez que há algum tempo estamos passando pelo processo de migração da vida social para o ambiente virtual. Assim, conflitos que são intrínsecos ao convívio humano também estão migrando para este espaço e, por isso, a internet tem sido utilizada como mecanismo para cometer, dentre outros, crimes contra a pessoa.

Foi nesse sentido que, segundo a jornalista Mayara Carvalho do Jornal Opção (2014), o Tribunal de Justiça de Goiás, através de um levantamento, constatou que entre 2014 e 2018 quase 4,2 mil processos tratam de conflitos ocorridos através da internet, mais especificamente utilizando redes sociais, tendo em vista que esta ferramenta permite maior rapidez na divulgação e consequentemente maior visibilidade a conduta delituosa.

Dessa forma, trataremos a seguir de algumas dessas práticas que estão ganhando, progressivamente, destaque com a hiperconectividade, delineando o que leva as pessoas estarem mais propensas a cometer tais delitos e a serem vítimas, bem como o tratamento jurídico que é dado a estas condutas, a fim de mostrar a necessidade de buscar soluções para inibir e combater tais práticas.

3. EXEMPLOS DE CRIMES COMETIDOS NA INTERNET

A tecnologia surgiu como uma ferramenta capaz de facilitar a comunicação entre as pessoas em qualquer lugar do mundo e, aos poucos, foi nos conquistando devido a suas serventias, proporcionando aprendizado, acesso a diversos conteúdos, compartilhamento, liberdade, etc. Entretanto, com todo o avanço tecnológico, veio também a facilidade em cometer crimes sem que, muitas vezes, sejam descobertos, pois na internet não há fronteiras – um dos grandes atrativos dos criminosos.

Com isso, abordaremos algumas práticas que foram incrementadas com a hiperconectividade, mostrando qual o reflexo delas na sociedade.

3.1. PEDOFILIA

Este é um tema bastante delicado e que, por isso, merece muita atenção, tendo em vista que muitas vezes é tratado de maneira equivocada – a Pedofilia. Desta forma, cumpre-nos responder, antes de tudo, "o que é Pedofilia?".

Em nosso cotidiano estamos acostumados a ouvir e transmitir de maneira errônea que Pedofilia é um crime, porém, em nosso ordenamento jurídico, não existe o tipo penal "Pedofilia", isto porque, segundo a Organização Mundial de Saúde (OMS), a pedofilia é uma doença, ela consiste em um transtorno psicológico no qual adultos do sexo masculino e feminino – os chamados pedófilos – têm preferência sexual por crianças que ainda não atingiram a puberdade.

O que é considerado crime, é a exteriorização da doença, ou seja, condutas que normalmente são praticadas por pedófilos e que estão tipificadas no Código Penal Brasileiro e no Estatuto da criança e Adolescente (ECA), como por exemplo, o estupro de vulnerável (art. 217-A, do CP) e a comercialização ou exposição de pornografia envolvendo criança ou adolescente (art. 241, do ECA). Assim, para que um pedófilo seja punido e considerado um criminoso, ele tem que praticar uma conduta prevista como crime.

Devido a toda facilidade que a internet proporciona, é que os pedófilos costumam agir nesse campo para encontrar suas vítimas. É através das redes sociais ou sites que eles, se aproveitando da vulnerabilidade das crianças, cometem seus crimes. Os pedófilos costumam criar perfil falso, adotam um com-

portamento para atrair os jovens, ganham confiança e se passam por amigos para alcançar seus objetivos. É o que relata o delegado da Gerência de Combate aos Crimes de Alta Tecnologia (Gecat), Eduardo Botelho, em uma entrevista (OLIVEIRA, 2017):

> Geralmente eles se apresentam como amigos, iniciam uma conversa, fazem elogios, brincadeiras, e passam a ganhar confiança da vítima antes de iniciar a conversa com a real intenção. A partir do momento que se cria uma intimidade e confiança com o "alvo", o pedófilo começa a realizar os pedidos de fotos, conversas mais aprofundadas até o momento em que intima a vítima para um encontro real, quando geralmente é abusada.

Como já dito, pedófilos sentem atração por crianças pré-púberes, e a maioria dos seus alvos na internet são menores de 14 anos, devido ao risco de denúncia ser menor já que são mais vulneráveis e não têm capacidade para resistir. Também porque esses menores compartilham suas informações sem nenhum cuidado, tornando as coisas mais fáceis para o pedófilo.

Assim, os pedófilos se sentem muito à vontade para praticarem os crimes. Os jornalistas Alan Rodrigues e Mário Simas Filho, em uma matéria da Revista ISTOÉ (2004), escreveram o seguinte:

> A violência cibernética se concretiza, basicamente, em dois níveis: um deles consiste em conquistar a garotada para a prática sexual ou buscar nessa criança o objeto para a exposição de fotografias em situações eróticas. O outro é jogar para as crianças imagens pornográficas sem a menor cerimônia e, a partir delas, estabelecer um vínculo promíscuo.

De acordo com uma pesquisa realizada em 2008 pela Safer Net Brasil, entidade referência nacional no enfrentamento aos crimes e violações aos Direitos Humanos na Internet, no quesito "amigos virtuais" 54% dos jovens dizem que possuem algum colega que já encontrou com um amigo virtual; 27% dos jovens afirmam já ter encontrado (presencialmente), ao menos uma vez, amigos que conheceram pela Internet; e 18% dos pais já se aventuraram a vivenciar um encontro com alguém que conheceram on-line. Já no que se refere à "segurança na internet", 53% tiveram contato com conteúdos agressivos e que consideravam impróprios para sua idade; 53% dos pais nunca sentem que seus filhos estão seguros on-line, enquanto 40% dos jovens consideram que estão sempre seguros e podem se defender de qualquer ameaça; 38% dos jovens internautas relataram já terem sido vítimas de ciberbullying; 10% afirmaram já ter sofrido algum tipo de chantagem on-line; entre os pais, o maior receio é de que os filhos sejam vítimas de um adulto mal intencionado (84%), seguido pelo medo de os filhos terem contato com conteúdo impróprios (74%); cerca de 40% dos pais

informaram que seus filhos já explicitaram incômodo ou constrangimento em relação ao que vivenciaram pela Internet. Apesar disso, 63% dos pais afirmam não impor regras para o uso que os filhos fazem da Internet.

O que se extra dos resultados obtidos através dessa pesquisa é que os jovens acabam se colocando como vítimas, por falta de acompanhamento dos pais e, principalmente, por falta de educação digital. São crianças que tem contato precoce com o mundo virtual e, devido a isso, acabam sendo alvos fáceis de criminosos – dentre eles os pedófilos.

A atuação de pedófilos na internet não se dá de maneira isolada, ela tem se dado através de redes de pedofilia que movimentam milhões de dólares em todo o mundo, com a comercialização de material pornográfico infantil; isso significa que a pedofilia está intimamente relacionada com o crime organizado.

Eles criam essas redes de pedofilia a fim de formar uma espécie de banco de dados de crianças que têm potencial para se tornarem suas vítimas de abuso sexual e, assim, transformar tais abusos em material pornográfico infantil para ser compartilhado. Nesse sentido, é imprescindível destacar três casos de grande repercussão, quais sejam: "Cathedral", "Wonderworld" (mundo maravilhoso) e "TinyAmerican Girls" (pequenas meninas americanas).

Tudo começou através de uma investigação que ocorreu na Califórnia (EUA), de um abuso sexual isolado, em que foi descoberto que um sujeito abusou de uma menina menor de 10 anos e compartilhou o abuso em tempo real, através de um site criado para práticas como essa. O sujeito foi preso e condenado, sendo que com ele foi apreendido uma quantidade significantiva de material pornográfico infantil (Caso Cathedral). O referido caso deu azo para que a investigação estendesse e fossem identificadas diversas redes de pedofilia, dentre elas, uma chamada "Wonderland Club", na qual foi identificado um arsenal de imagens de abusos sexuais com mais de 1267 crianças diferentes, num total de 758 imagens e 1860 horas de filmagens (Caso Wonderland – Mundo Maravilhoso). O último caso, "Tiny American Girls", trata-se de um fotógrafo que solicitava a autorização dos pais das vítimas, dizendo que faria fotografias artísticas das meninas. Como os pais não acompanhavam as sessões, ele registrava fotografias das crianças nuas e em poses pornográficas. O sujeito foi detido e ficou conhecido como "El Artista", entretanto, a rede de pedofilia continuou comercializando material pornográfico infantil por mais alguns anos (TRINDADE e BREIER, 2013).

Hoje, há uma conscientização e preocupação muito grande com este problema, e órgãos como o Ministério Público Federal e Estadual, a Polícia Civil, Polícia Federal, ABMP, RECRIA, CECRIA, CEDECA, ABRAPIA, UNESCO e

muitas outras instituições e entidades estão firmando acordos para combater esses absurdos praticados por esses delinquentes na Web (NOGUEIRA, 2001).

Portanto, é necessário que se entenda o que é a pedofilia enquanto doença e a diferencie das condutas penalmente proibidas. Para além, é fato que precisamos investir em diversos aparatos tecnológicos que ajudem na investigação e punição desses crimes, sem, no entanto, deixar de entender que carecemos de educação digital e social para que se atinja o cerne do problema, e não só as suas consequências.

3.2. FAKE NEWS

No mundo sempre existiu propagação de conteúdos inverídicos, no entanto, essas informações não conseguiam alcançar uma quantidade significativa de pessoas de maneira muito rápida; isto somente seria possível se fossem divulgados através dos grandes meios de comunicação, por exemplo, dos telejornais. Entretanto, com o avanço tecnológico e o surgimento das redes sociais tornaram-se mais fáceis a divulgação e o alcance desses conteúdos devido ao grande número de pessoas hiperconectadas à internet; assim surgiu o que chamamos de "Fake News".

De acordo com o que se extraí do Dicionário de Cambridge[2], Fake News são histórias falsas com características de notícia jornalística, compartilhadas na internet ou através de outras mídias. Elas geralmente são criadas com o intuito de influenciar na política ou na economia, bem como o de atingir a imagem de determinado grupo ou pessoa.

Esse é um dado muito preocupante, tendo em vistas as conseqüências devastadoras que a propagação de conteúdos falsos pode gerar. Como exemplo disso é possível citar o caso da Escola Base, em que foi divulgada na imprensa e nas redes sociais a falsa informação sobre estupro de crianças envolvendo os donos de uma escola particular. Devido ao enorme alcance da Fake News, os donos da escola tiveram suas vidas arruinadas. Outro grande exemplo são as eleições norte-americanas disputadas entre Donald Trump e Hillary Clinton em 2016, em que houve disseminação de Fake News com o intuito de influenciar os eleitores.

Um estudo realizado pela Kantar revelou que a prática de compartilhamento de Fake News se intensificou entre 2016 e 2017 (BUENO, 2017). Como a hiperconectividade contribui para a intensificação? Como já dito, grande parte da sociedade está conectada à rede da internet. Existem diversas redes sociais e diversos sites onde são espalhadas informações, por segundo. A facilidade

2 https://dictionary.cambridge.org/us/dictionary/english/fake-news

e a velocidade com que os conteúdos chegam até as pessoas fazem com que muitas vezes elas não confiram a veracidade desses conteúdos, e é assim que a Fake News se tornou algo viral, de modo que existem sites e até mesmo empresas instituídas para criar e divulgar Fake News voltadas a um determinado segmento.

Nesse sentido, um estudo realizado pelo Instituto de Tecnologia de Masachussetts (MIT) revelou que as informações falsas têm 70% mais de chances de viralizar que as notícias verdadeiras. O estudo mostra que cada postagem verdadeira atinge, em média, mil pessoas, enquanto as postagens falsas mais populares atingem de mil a 100 mil pessoas (CASTRO, 2018).

Pode-se citar outros fatores que contribuem para esse fenômeno, como por exemplo, o fato de que as pessoas tendem a acreditar mais facilmente em informações que confirmem seu modo de pensar; o prestígio de sua fonte direta para atribuir confiabilidade ao conteúdo, ou seja, pessoas próximas em quem confiamos que nos enviam pedindo para repassar e automaticamente compartilhamos e a falta de verificação a respeito da veracidade da informação (GIOVANELLI, 2018).

Assim, com a falta de educação digital da sociedade, a cultura de não verificar a veracidade das informações, o mercado de propagação de conteúdos sensacionalistas, a criação em massa de sites de notícias e a dificuldade que o Poder Público tem para combater essas práticas, a tendência é que essa prática de compartilhamento de Fake News cresça ainda mais.

3.3. PORNOGRAFIA DE REVANCHE

A hiperconectividade pode trazer consequências negativas para as nossas vidas, e uma dessas questões que deve ser tratada com mais veemência é a chamada Pornografia de Revanche ou, em inglês, "*revengeporn*".

A promotora Maria Gabriela Manssur (2015) define a pornografia de revanche deste modo:

> A divulgação/publicação/transmissão de imagens (fotografias, vídeos) e conversas íntimas em rede social/aplicativos, sem o conhecimento e consentimento da vítima, como forma de retaliação pelo fim do relacionamento. Como se a vontade da mulher, mais uma vez, não fosse respeitada. Como se ela fosse obrigada a manter um relacionamento contra a sua vontade.

Segundo Ana Paula Gonçalves (2017), a origem desse comportamento remete à década de 80, nos EUA, e condiz com o ato de divulgar, através dos meios digitais, fotos ou vídeos contendo cena de nudez ou sexo, sem autorização da vítima com o propósito de causar dano a ela. Tal denominação surgiu quando

uma revista masculina passou a ter uma seção para a divulgação de fotos de mulheres comuns nuas, muitas vezes tiradas em locais públicos.

Ana Paula Gonçalves (2017) relata que, até então, ainda se tratava de um comportamento obscuro na sociedade, sendo que, conclui:

> Em 2010, a pornografia de vingança entrou oficialmente na pauta da sociedade norte-americana diante da criação do site IsAnyOneUp.com, cujo serviço resumia-se à publicação de conteúdo pornográfico disponibilizado anonimamente pelos próprios usuários.

Observa-se, então, como há a mudança de comportamentos na sociedade, exatamente por termos, nesse tempo, a passagem de uma sociedade pouco conectada para uma sociedade hiperconectada, o que acaba gerando novos tipos de crimes, os quais devem ser alcançados pelo direito penal. Um crime que na década de 80 era executado por meio de revistas, para onde os usuários enviavam fotos de mulheres a fim de serem publicadas, em 2010, o mesmo crime assume uma nova roupagem, ainda mais severa, visto que, como bem diz Maria Gabriela Manssur (2015), "a vítima terá a sua intimidade, inclusive sexual, devastada. E em rede nacional. Não. Pior. Em rede mundial!".

Destarte, as consequências são devastadoras. As consequências morais e psicológicas, para as vítimas, vão desde a vergonha de sair de casa, de frequentar escola, faculdade, trabalho, de sentimento de culpa, até o desenvolvimento de depressão, doenças psicossomáticas, síndrome do pânico, autolesão e suicídio (MANSSUR, 2015). Nesse sentido, a Revista Fórum (2013) publicou uma matéria relatando o suicídio de duas meninas vítimas da Pornografia de Revanche.

É preciso, ainda, diferenciar o conceito de Pornografia de Revanche da conduta que é tipificada pela Lei n° 12.737/2012, intitulada de "Lei Carolina Dieckmann". Para tanto, devemos esclarecer que esta lei abrange os casos de violação de eletrônicos com algum tipo de sistema de segurança, ou seja, não trata de casos em que o indivíduo tem a confiança da vítima e, a partir disso, comumente após o término do relacionamento, divulga fotos íntimas com o intuito de constrangê-la. Portanto, há uma clara diferença entre as condutas previstas pela Lei nº 12.737/2012 e a pornografia de revanche, a qual, hoje, é abarcada pela Lei 13.718/2018.

No Brasil, essa conduta tomou proporções maiores e alcançou visibilidade ímpar nos últimos anos, especialmente em virtude da popularização da internet e de redes sociais, e trouxe à tona uma contemporânea forma de violência contra as mulheres, já que elas figuram as vítimas, via de regra, desse tipo de crime (MANSSUR, 2015).

A Pornografia de Revanche, portanto, está intimamente ligada à cultura machista. Nesse sentido, uma pesquisa produzida pela ONG End Revenge Porn (2014) aponta que 90% das vítimas são mulheres, e constata que 50% das pessoas que sofrem com esse crime usaram o celular para receber ou enviar conteúdo íntimo.

Diante disso, verifica-se que as mulheres figuram como vítimas assíduas desse tipo de comportamento, muito por conta da conduta que a sociedade, machista como é, encara um homem e uma mulher exposta na rede mundial, visto que enquanto o homem é, muitas vezes, glorificado quando, por exemplo, tem uma vida sexualmente contínua, a mulher, quase sempre, é ridicularizada e vista com adjetivos não tão gentis quando exposta à mesma situação.

Para além, verifica-se também que há uma desinformação crassa de uma sociedade que não foi ensinada a manusear a internet com o cuidado adequado, já que pelo menos metade das vítimas enviam ou recebem fotos íntimas, ou seja, mantêm um comportamento que parece ser inofensivo, contudo, nitidamente, percebe-se a ofensividade desse comportamento, quando se aprende a manusear a internet com a devida cautela. Mais uma vez, portanto, se observa a importância da educação digital.

3.4. CRIMES DE ÓDIO

O crime de ódio é uma das variadas formas de violência existente na nossa sociedade e se direciona a um grupo social em específico, por questões de preconceitos desse agressor. Além disso, tal crime ocorre, em regra, contra as chamadas minorias sociais, que são aquelas pessoas que historicamente sofrem preconceitos em nossa sociedade, como mulheres, gays, negros e deficientes (ORTEGA, 2015).

É importante entender, então, que é um delito não permitido pelo nosso ordenamento jurídico, por questões notórias, já que atenta contra a própria dignidade humana, a qual é positivada na constituição no seu artigo 1º, não por outro motivo que não seja a sua importância histórica. A dignidade da pessoa humana faz com que vivamos com respeito mútuo e tenhamos condições mínimas de vida em sociedade. O artigo 3º da CF/88 diz que é um dos objetivos da República Federativa do Brasil promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. Portanto, a proibição dos crimes de ódio consta na peça principal do nosso ordenamento.

Sendo assim, este tipo de conduta atenta contra o direito fundamental, talvez, basilar do nosso ordenamento, qual seja, a dignidade da pessoa humana, e, consequentemente, atenta, inclusive, contra o Estado democrático de direito,

visto que não há como conceber este tipo de Estado sem respeitar os direitos fundamentais, ainda mais se tratando da dignidade da pessoa humana. Diante disso, se torna imprescindível a discussão e consequente combate aos crimes por motivo de crença, etnia, orientação sexual ou motivado por qualquer outro preconceito.

Os crimes de ódio ganham relevância inegável com a hiperconectividade, prova disso é a preocupação dos órgãos competentes com esse tipo de crime. O Ministério Público Federal (2018), por meio da sua Procuradora da República, Priscila Costa Schreiner, numa audiência pública na comissão de direitos humanos e minorias da Câmara dos Deputados, demonstra a sua preocupação, principalmente, com a prevenção e a educação. O Ministério da Justiça (2014) determinou o reforço ao combate deste tipo de crime com ações da polícia federal, com o objetivo de monitorar e mapear crimes contra os direitos humanos nas mídias sociais.

Com isso, demonstra-se a relevância dos crimes de ódio com o advento da hiperconectividade. As pessoas estão mais conectadas, e a tendência é que esse número aumente, sendo que, com isso, proporcionalmente, o cometimento desse crime na internet também deve aumentar. Isso porque a internet traz uma falsa sensação de que os indivíduos que a utilizam estão altamente protegidos, ou seja, anônimos, o que, já vimos, não é verdade. Nesse sentido, a procuradora Priscila Schreiner (2018) contesta esta proteção demasiada que os indivíduos acham ter na internet, dizendo exatamente que os crimes cometidos no ambiente digital deixam rastros e, portanto, não há esse anonimato, em regra. Principalmente quando estamos falando de sujeitos que, a priori, não tem conhecimento profundo em internet, ou seja, quando falamos de sujeitos comuns que utilizam a internet para propagar ódio aos seus inimigos ou, simplesmente, por motivos de preconceitos mesmo, sem qualquer fundamento que explique tal ato.

Com o mundo digital, os números deste crime no Brasil são surpreendentes. Nos últimos 11 anos, quase 4 milhões de denúncias relacionadas a crimes de ódio na internet foram recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos. Isso porque as redes sociais facilitaram a replicação de informações de modo escalável. Com isso, proporcionaram uma infraestrutura para que as pessoas repliquem discursos, muitas vezes sem uma posição crítica (PUGLIERO, 2018).

Vale salientar que muita gente ainda não tem acesso digital e, por isso, se tornam tão preocupantes esses números de cometimento deste crime. Em São Paulo, por exemplo, a polícia civil registra um crime de ódio a cada 12 horas, que ocorre com mais frequência contra negros, gays, imigrantes ou por motivações religiosas, sendo cometidos, principalmente, por homens brancos e jovens (CARDOSO, 2017).

Por isso, esse é um dos crimes que muito provavelmente terá tratamento especial pelos órgãos brasileiros responsáveis pelo combate à violência, a qual, neste caso, ocorre de maneira digital, trazendo diversos transtornos à vítima, pois não deixa de ser tão ou mais gravoso que um crime cometido fisicamente.

3.5. CYBERBULLYING

A palavra "bullying", que vem do inglês, significa oprimir, assustar ou, ainda, ameaçar. Sendo assim, verifica-se que há, nesses casos, um assédio moral, que é um outro significado da palavra, relatado por uma breve pesquisa no Google Tradutor. No entanto, essas atitudes tão comumente cometidas em ambiente escolar ganhou um incremento importante, o qual permite ampla divulgação e efeitos, às vezes, mais danosos do que o seu antecedente. Portanto, o *bullying* tradicional ganha o seu sucessor, não menos importante ou incomum, o *Cyberbullying*.

Como bem remonta Lucas Oliveira (2018), sociólogo, bullying seria composto por atitudes sucessivas, portanto, repetitivas, que visam maltratar, humilhar ou violentar o outro. Já o *Cyberbullying* acontece quando a agressão se passa em ambiente digital, envolvendo e-mails, redes sociais e até telefones.

Desta forma, percebe-se que a diferença básica entre o bullying e o Cyberbullying são os ambientes nos quais eles se passam. No entanto, essas práticas hostis podem gerar, inclusive, o suicídio da vítima. Nesse sentido, uma reportagem publicada pela revista "Isto é" (2017) mostra o relato dos pais. Vejamos: "Os pais contaram que a jovem, que sonhava com ser advogada, era agredida em redes sociais, além da escola: nesse dia, antes de tentar se matar, já havia sido alvo de piadas por causa do aparelho nos dentes".

Nos dedicaremos a entender por que essa prática cometida insistentemente em ambiente escolar passou a ser executada em redes sociais. Beatriz Santomauro (2010) destaca três motivos pelos quais o *Cyberbullying* passou a crescer intensamente e se tornou ainda mais cruel do que o bullying tradicional. Notemos:

> (1) No espaço virtual, os xingamentos e as provocações estão permanentemente atormentando as vítimas. Antes, o constrangimento ficava restrito aos momentos de convívio dentro da escola. Agora é o tempo todo. (2) Os jovens utilizam cada vez mais ferramentas de internet e de troca de mensagens via celular - e muitas vezes se expõem mais do que devem. (3) A tecnologia permite que, em alguns casos, seja muito difícil identificar o(s) agressor(es), o que aumenta a sensação de impotência.

Assim, a hiperconectividade, nesse caso dos jovens, é um dos fatores para que tenhamos o aumento de números do *Cyberbullying*, visto que esse ambiente digital se torna, cada vez mais, imprescindível às relações sociais atuais. No

entanto, no mundo online, as agressões têm uma quantidade de espectadores muito maior, além de, também, atingir a vítima onde quer que ela esteja, visto que o bullying eletrônico não finda quando a criança deixa a escola, por exemplo, mas, sim, enquanto ela permanecer conectado às redes sociais, a vida dela poderá ser exposta.

Um estudo realizado pelo Ministério da Educação, Organização dos Estados Ibero-americanos para Educação Ciência e Cultura (OEI) e Faculdade Latino-Americana de Ciências Sociais (Flacso) demonstra que o ambiente escolar é reprodutor desse tipo de violência (ABRAMOVAY, 2015). Também um estudo feito pelo instituto iStart (2018) mostra que ao menos 77,7% dos incidentes nas instituições de ensino envolvem conflitos nos grupos de WhatsApp e, em 2015, o *Cyberbullying* era o problema com maior incidência nos colégios, correspondendo a 75% das ocorrências.

Desta forma, temos que o problema central na discussão sobre o bullying digital é a sua incidência majoritária no ambiente escolar, o qual envolve, muitas vezes, a presença de menores e, por isso, a discussão criminal atinge um conceito muito mais restritivo como, de fato, deve ser.

Dito isto, nota-se como a hiperconectividade contribui para a intensificação da prática desses delitos na internet e, principalmente, para o aumento dos conflitos interpessoais. Mas é possível vislumbrar outros fatores que, junto com a hiperconectividade, são incrementos a essas práticas criminosas, como a falta de educação digital e também de preparo técnico dos profissionais que atuam no combate aos crimes.

4. OUTROS FATORES QUE INCREMENTAM O COMETIMENTO DESSES DELITOS

Sabe-se que a tecnologia avança a passos largos, como foi demonstrado anteriormente neste artigo. No entanto, precisamos atentar para o fato de esse avanço estar acontecendo agora. Um grande exemplo é a criação da internet mais rápida do mundo, a qual tem velocidade de 1,4 tbps (Tech Mundo, 2014). Observa-se, portanto, que é preciso que toda a sociedade se prepare para este avanço tecnológico que estamos vivendo, tanto nós, cidadãos comuns, como os próprios agentes responsáveis por combater esse tipo de crime.

Segundo estudo realizado pela empresa de segurança Palo Alto Networksa, o Brasil é o segundo país da América Latina que mais sofre com os crimes cibernéticos, ficando atrás apenas do México (tecnologia). Esses dados tornam ainda mais visível a necessidade de mudança de rumo no Brasil no que se refere ao combate aos crimes cibernéticos. É importante, portanto, analisar que há uma dupla via nessa análise: a primeira, é esse combate efetivo para a dimi-

nuição desse tipo de crime; e, a segunda, é a consequente prospecção de crimes que poderão ocorrer, caso não tenhamos essa reestruturação no combate dos crimes cibernéticos.

Com isso, aduz-se necessário, de logo, que todos os membros da sociedade tenham oportunidade de aprender a utilizar o ambiente virtual de forma adequada, visto que a desinformação relativa ao ambiente digital deixa o indivíduo ainda mais vulnerável. Uma pesquisa feita pela SaferNet Brasil constata que apenas 15% dos entrevistados sabiam onde denunciar um crime digital, sendo que essa pesquisa foi feita tendo como entrevistados professores, os quais são responsáveis pela formação de indivíduos.

É urgente, então, trazer esse tema para a sala de aula, fazer com que ele faça parte da grade curricular obrigatória, desde o ensino fundamental, visto que a falta de informação com algo que se utiliza desde muito cedo faz com que fiquemos reféns e sejamos alvos mais fáceis.

Ademais, é preciso também capacitar os agentes responsáveis por combater e verificar os crimes, sejam eles delegados, promotores e juízes. Isso porque existem cidades nas quais há delegacias com departamentos específicos para os crimes cibernéticos, a exemplo de Rio de Janeiro e São Paulo, e outras que não têm esse departamento (LANDIM, 2011). A ANATEL diz o seguinte: "Para tratar de crimes cibernéticos no Brasil, atualmente, existem onze delegacias especializadas em crimes virtuais. Elas encontram-se nas capitais dos estados do Espírito Santo, Goiás, Mato Grosso, Minas Gerais, Pará, Paraná, Rio de Janeiro, Rio Grande do Sul, São Paulo, Sergipe e no Distrito Federal."

Nas cidades em que não há departamentos especializados para tal, a comunicação do crime pode ocorrer em qualquer delegacia. No entanto, muitas vezes, os próprios profissionais do direito não sabem lidar com esse avanço tecnológico que estamos vivendo. Nesse sentido, o Ministro do STJ, Rogério Schietti, segundo Marcelo Galli, numa palestra sobre o direito contemporâneo na era digital, disse que:

> [...] outros aspectos dificultam o combate aos crimes desse tipo no Brasil. Ele cita a profunda deficiência de conhecimentos mínimos de linguagem da informática de grande parte da sociedade brasileira, e também no meio jurídico. E a velocidade diferente existente entre o desenvolvimento das Ciências da Computação e do Direito.

Portanto, é inegável a necessidade de capacitar profissionais para lidar com os novos desafios. Importante dizer, também, que não só com relação aos agentes do Estado, mas também com relação à sociedade em geral, especialmente os nossos legisladores, visto que muitas de nossas legislações são ultrapassadas

e não conseguem, sequer, tipificar condutas reprováveis ou oferecer uma pena mínima condizente com a gravidade do crime exercido.

Sendo assim, temos uma tarefa árdua e que deve ser exercida conjuntamente por todos os membros da sociedade. Quando alguém é vítima de um crime digital, ela deve ir à delegacia mais próxima, seja ela especializada ou não, para poder efetuar o boletim de ocorrência, levando consigo todas as provas possíveis. Então, nessa atuação, precisamos de, pelo menos, três agentes capazes, e o primeiro é o próprio indivíduo, o qual deve ter conhecimento mínimo de informática para poder levar conteúdos probatórios, que corroborarão com a sua alegação. O segundo é o próprio agente policial, que deve ter conhecimentos relativos à matéria de direito digital para que possa efetuar uma investigação adequada desse tipo de crime. Os terceiros são o MP e os advogados para que tenhamos uma discussão judicial para definir se, de fato, esse crime aconteceu ou não.

Todos esses sujeitos deverão se utilizar de meios adequados para a persecução do resultado, condenação ou absolvição, com base em análise do caso concreto. No entanto, é importante salientar que todos eles, em algum momento, estão adstritos à lei e, portanto, esta é quem deve ser o seu norte. Se temos leis digitais fracas e lacunosas, a atuação desses três sujeitos será necessariamente deficitária.

Contudo, salienta-se que não estamos pregando a política do punitivismo; não acreditamos que o aumento de pena ou de tipos penais, pura e simplesmente, seja a solução para a diminuição dos crimes cometidos no espaço virtual, mas sim que para um combate efetivo as autoridades responsáveis pelo enfrentamento dessas questões dependem do amparo da lei para que ajam dentro da legalidade, além de preparo técnico de informática para saber lidar com os criminosos no ambiente virtual.

Desta forma, acredita-se que, assim como todos os fatores, ora mencionados contribuem para a prática dos delitos que ocorrem através da internet, estes também podem ser utilizados no combate, desde que utilizados corretamente tanto pela sociedade civil, para evitar se colocar como vítimas, quanto pelo Poder Público, ao combater os crimes.

5. ANÁLISE PROSPECTIVA DOS CRIMES NA INTERNET

O que abordamos acima é apenas uma delimitação dos crimes que são cometidos na internet e como a situação se encontra hodiernamente. Com isso, já podemos perceber como o caso é delicado, no entanto, devemos nos atentar para o seguinte questionamento: será que esse quadro pode ficar ainda pior?

Na atualidade, nem toda a sociedade global está conectada à rede de internet. De acordo com o relatório "Digital in 2018", disponibilizado em janeiro deste ano pelos sites We Are Social e Hootsuite, no planeta existem cerca de 7.593 bilhões de pessoas, sendo que deste total 4.021 bilhões já estão conectadas, ou seja, no início de 2018 apenas 3.572 bilhões de pessoas ainda não estavam conectadas.

Diante desta informação, temos que analisar o fato de que se atualmente, sem que toda a população global esteja conectada, o número de crimes cibernéticos cresce de forma exponencial; imagina quando a internet chegar para toda a sociedade.

Com isso, é correto afirmar que a tendência é que a situação se agrave, ou seja, que aumente ainda mais o número de crimes cometidos na internet, e para evitar que isto ocorra, sem a devida repressão, é que analisaremos o que, além do avanço tecnológico e hiperconectividade, contribui para o crescimento dos delitos na internet.

Como já visto, os crimes cibernéticos crescem na medida em que a internet se torna mais acessível, e isto se dá porque o universo virtual ganhou um espaço importante no que tange à vida social e profissional dos indivíduos. Com a informatização, quase tudo que é essencial para a sociedade migrou para a rede, a exemplo de documentos de identificação que antes eram físicos e passaram a ser digitais; as compras, que antes eram realizadas em lojas físicas agora é possível serem feitas através de lojas virtuais; movimentações bancárias, através de dispositivos informáticos, etc.

Coisas que, num primeiro momento, foram pensadas para facilitar a vida das pessoas, hoje podem acabar trazendo muita dor de cabeça, tendo em vista que toda essa circulação de dados pessoais na internet, sem o devido cuidado e segurança tem servido de grande atrativo para criminosos, tornando o ambiente virtual um lugar propício para o cometimento de delitos. Assim, crimes que eram praticados antes do advento da internet, migram para o mundo virtual – a exemplo dos crimes mencionados anteriormente – e outros tipos criminais acabam surgindo, os chamados crimes próprios, a exemplo dos crimes de *phishing* e *ransomware*[3].

Esse processo de inclusão tecnológica da sociedade e, consequentemente, a transferência e circulação de seus dados sensíveis tornam ilimitada a variedade

3 O *Ransomware* é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário. Já o *phishing* é um termo em inglês que significa pesca. Traduz-se em um golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Disponível em <https://cartilha.cert.br/glossario/>. Acesso em 09 out 2018.

de crimes que podem ser cometidos na internet, sendo um dos fatores chave para que os criminosos se sintam atraídos por este ambiente e para a quantidade dos delitos cometidos aumentem a cada dia.

A "Central Nacional de Denúncia de Crimes Cibernéticos" da SaferNet revela os seguintes dados, coletados entre 2006 e 2018:

> Em 12 anos, a Central de Denúncias recebeu e processou 3.925.405 denúncias anônimas envolvendo 701.224 páginas (URLs) distintas (das quais 246.699 foram removidas) escritas em 9 idiomas e hospedadas em 94.155 hosts diferentes, conectados à Internet através de 56.416 números IPs distintos, atribuídos para 101 países em 5 continentes; a Polícia Federal recebeu e processou 561.854 denúncias anônimas envolvendo 122.554 páginas (URLs) distintas (das quais 54.857 foram removidas) escritas em 9 idiomas e hospedadas em 25.266 hosts diferentes, conectados à Internet através de 16.878 números IPs distintos, atribuídos para 82 países em 5 continentes; a Secretaria de Direitos Humanos recebeu e processou 30.695 denúncias anônimas envolvendo 11.364 páginas (URLs) distintas (das quais 3.723 foram removidas) escritas em 9 idiomas e hospedadas em 1.914 hosts diferentes, conectados à Internet através de 1.999 números IPs distintos, atribuídos para 48 países em 5 continentes; e a SaferNet Brasil recebeu e processou 3.119.921 denúncias anônimas envolvendo 551.770 páginas (URLs) distintas (das quais 194.891 foram removidas) escritas em 9 idiomas e hospedadas em 56.828 hosts diferentes, conectados à Internet através de 31.576 números IPs distintos, atribuídos para 99 países em 5 continentes.

Esses dados são preocupantes, pois, conforme acima demonstrado, das denúncias contabilizadas que chega a aproximadamente 4 milhões, apenas 600 mil são recebidas e processadas pelo Poder Público. A diferença é alarmante, revela a ineficácia da atuação estatal e a necessidade de aprimoramento de técnicas visando coibir a prática de crimes na internet. É nesse sentido que disse o presidente da High Technology Crime InvestigationAssociation – HTCIA, Paulo Quintiliano (2017):

> Os criminosos usam a tecnologia para ter anonimato e buscar impunidade, por isso o Estado deve se preparar melhor para enfrentar e ter agilidade na atuação, pois a criminalidade age com velocidade incrível. Judiciário, Polícia e MPF têm que se preparar para enfrentar esses crimes com mais eficácia.

A nossa sociedade ainda não consegue acompanhar os avanços tecnológicos, no sentido de estar preparado para utilizar o ambiente virtual e saber quais cuidados devem ter neste espaço. Por isso, acabam se tornando alvos fáceis para os criminosos. O próprio Estado tem grande dificuldade para criar mecanismos que desestimulem a prática dos crimes na internet e poucas ferramentas que possibilitem o combate efetivo desses delitos.

Cabe salientar o quão dificultoso é fazer prova de crimes cometidos na internet, em virtude de demandar conhecimento técnico dos usuários – o que muitos não têm – e isso acaba impactando negativamente, na investigação, porque, segundo o advogado criminalista Luiz Augusto D'urso (2017):

> É necessário localizar a origem da conexão, apreender os dispositivos suspeitos, periciar o material apreendido, e, só após tudo isto, identificar de qual dispositivo foi praticado o crime, e, assim, concluir quem é o responsável pelo ato ilícito.

Infelizmente, são poucos os profissionais capacitados para investigar e combater os crimes cibernéticos; apenas de uns anos para cá a polícia brasileira passou a investir na capacitação técnica em tecnologia dos policiais, bem como na utilização de equipamentos informáticos para combater os crimes, conforme dito pelo assessor-chefe da Temática de Tecnologia da Informação e Comunicação da Seap, Marcelo Caiado (2017):

> Está claro que a perícia digital e as investigações de crimes cibernéticos apresentam grandes desafios, sendo essencial que as forças da lei possuam profissionais capacitados e equipamentos adequados para poderem atuar adequadamente, além da necessidade de uma legislação apropriada e de uma satisfatória cooperação internacional

Há que se falar ainda que, apesar de existirem tipificações de alguns crimes cometidos na internet, conforme já mencionado neste artigo, estes se mostram insuficientes perto da multiplicidade de delitos que podem ser cometidos no ambiente virtual; o que nos permite afirmar que a legislação brasileira não consegue acompanhar os avanços tecnológicos da mesma forma que os delinquentes, na medida em que buscam a cada dia aprimorar suas técnicas e descobrir outras ferramentas que a tecnologia oferece, com fulcro em obter êxito nos crimes, não adotando um comportamento padrão a ponto de as vítimas conseguirem se esquivar de novas "armadilhas", bem como para dificultar ainda mais o combate desses delitos.

Isso contribui significativamente para que o cibercriminoso tenha uma sensação – ainda que falsa – de que a lei não o alcançará e, assim, não será responsabilizado pelos crimes que cometeu e que virá a cometer.

Percebe-se, portanto, que o maior problema das autoridades no que se refere ao alto índice de delitos cometidos na internet e da população que acaba se tornando refém dessas práticas é o próprio avanço tecnológico e as facilidades que este nos permite. O ambiente virtual não tem fronteiras, é um espaço fértil e ideal para que criminosos se sintam à vontade. Faz-se necessário um avanço também no que se refere à legislação brasileira e nos mecanismos e ferramentas utilizadas pelo Poder Público no combate ao cibercrime.

6. CONSIDERAÇÕES FINAIS

O presente estudo possibilitou a análise da hiperconectividade e o seu avanço, além de verificar como os crimes cibernéticos se adequariam a essa nova realidade. A proposta deste artigo foi mostrar os impactos dos crimes cometidos na internet, delimitando aqueles contra a pessoa que, de certa maneira, acabam contribuindo para a intensificação dos conflitos interpessoais e como esse problema tem sido tratado pelo ordenamento jurídico mas, principalmente, alertar que a situação tende a piorar e que, por isso, tanto o poder público quanto a sociedade precisam estar preparados.

Vimos que esses crimes já são cometidos atualmente, no entanto, tenderão a se intensificar com o passar do tempo, visto que o crescimento dos chamados sujeitos-mensagens sintetiza a sociedade que teremos daqui para frente, a qual será muito mais conectada do que antes. O aumento de pessoas conectadas no mundo, em passos largos, faz com que surja a preocupação de como lidar com isso, uma vez que, como foi demonstrado, os delitos passaram a sofrer intensificação e aprimoramento em ritmo muito mais acelerado do que o ritmo com que a legislação consegue tipificar as condutas previstas.

A importância deste tema se torna nítida, ao passo que temos uma ebulição da Internet das Coisas (OIT) e, portanto, uma população altamente conectada. Em contrapartida, se não tivermos uma adequada educação digital, nos moldes que foi explicado, haverá um perigo enorme para a sociedade, que deverá se tornar refém dos sujeitos que quiserem cometer crimes.

A educação digital se torna uma das armas mais fortes para podermos utilizar nesse momento, visto que é com ela que iremos aprender como nos comportar no ambiente virtual. Observe que a ideia não é imputar à vítima a culpa de um eventual delito cibernético, dizendo que ela será responsável por ele e deve se precaver disso; pelo contrário, a posição deve ser no sentido de aprender a como se proteger do ambiente virtual, perceber quais tipos de situações podem ou não ser produzidas na internet e, além disso, saber quais os riscos de determinadas condutas.

Portanto, é entender, na verdade, que um simples nude enviado por redes sociais pode ser, no futuro, objeto de uma ameaça de determinado indivíduo contra a vítima, mesmo que o receptor da foto seja o seu atual parceiro. Ou, ainda, entender que mesmo com a iniciação precoce do contato das crianças com o ambiente digital, é importante que tenhamos um controle dos pais sobre qual o conteúdo acessado por elas, com quem elas se relacionam e, inclusive, determinar o que pode ou não ser feito por elas nesse ambiente.

Além disso, a educação digital vai possibilitar que os indivíduos entendam que muitos sujeitos autores do cyberbullying, por exemplo, têm a falsa percep-

ção de que estão totalmente protegidos, pelo simples fato de criar um perfil falso, o qual será utilizado para coagir as vítimas. Isso porque deve-se perceber que a questão pode ser levada a autoridades devidamente capacitadas, que terão a incumbência de solucionar o caso com os aparatos disponíveis e necessários para identificar aquele autor e responsabilizá-lo.

Com isso, nasce o dever do Estado brasileiro de promover políticas públicas e diretrizes necessárias ao desenvolvimento e capacitação digital de toda a sociedade, para que possamos entender, inclusive, que novas possibilidades de se cometer crimes podem chegar e teremos que lidar com elas.

O momento atual, portanto, pede seriedade nas ações governamentais com relação à internet e, mais do que isso, conhecimento. Notou-se que grande parte do aparato policial do Brasil está despreparado para lidar com essa nova situação. Com isso, é preciso, urgentemente, agir para que tenhamos poder Judiciário, Ministério Público e força policial fortemente atuantes e capacitados para lidar com esse novo panorama jurídico-social, visto que de nada adianta levarmos os casos a autoridades competentes se elas próprias não sabem como resolvê-los.

Visto isso, há uma importância de tal tema na perspectiva individual, para que o indivíduo possa se preparar para a onda tecnológica que está por vir, e na perspectiva coletiva, de sociedade, pois esta deve estar atenta a todos os empecilhos que podem vir a causar algum tipo de transtorno coletivo.

O uso responsável da internet é um outro lado que também deve ser frisado neste momento. É importante entender sobre o meio que se utiliza para que se possa agir com responsabilidade, havendo, portanto, correlação entre o uso responsável e a educação digital. Aqui, mais uma vez, se analisa a conduta dos pais na proteção de seus filhos pois, via de regra, são eles quem vão determinar quais condutas podem ou não ser feitas, quanto tempo os filhos passam na internet ou a forma como eles utilizam.

Questão interessante para pensarmos, prospectivamente, é como mudar esse panorama atual de falta de conhecimento. Acredita-se que o papel do Estado é fundamental; isso porque os sujeitos mais novos já nascem inseridos nesse ambiente, enquanto os mais velhos, no caso os pais, aprendem com o passar do tempo. Observamos que os jovens estão mais conectados do que os mais velhos e, portanto, estes sabem mais sobre o ambiente digital. Como, então, conceber que a educação digital vai partir, via de regra, dos pais para os filhos, e não o inverso? Então a ideia, aqui, é que o Estado seja o responsável por trazer o debate à tona, assim como a sociedade civil como um todo.

O parágrafo anterior traz uma preocupação, principalmente, com as famílias mais pobres e, consequentemente, as que, em regra, tem menos contato com

o tema educação digital. Sendo assim, o ambiente escolar é um vanguardista desta situação, ou seja, um dos grandes responsáveis por mudar esse panorama, sendo que por termos escolas públicas precárias, enquanto que as escolas particulares despontam em qualidade de ensino, temos a necessidade de intervenção estatal, para que pessoas de baixa renda tenham contato com esse tema.

Dito isso, ressalta-se que o tema abordado é de suma importância atual e futuramente, tendo em vista que ele está intimamente ligado com o nosso cotidiano e tem causado reflexos indesejados no mundo jurídico e na sociedade, sobretudo no que se refere às relações interpessoais. Assim, cumpre-nos atentar para o fato de que o combate à prática de crimes cometidos na internet perpassa pela questão da educação digital da sociedade, controle familiar no que se refere ao contato precoce com o mundo virtual e qualificação técnica dos profissionais que atuam no enfrentamento desses delitos.

REFERÊNCIAS:

ABRAMOVAY, Miriam. Coord. Juventudes na escola, sentidos e buscas: Por que frequentam? / Miriam Abramovay, Mary Garcia Castro, Júlio Jacobo Waiselfisz. Brasília-DF: Flacso - Brasil, OEI, MEC, 2015.

BRASIL. Constituição Federal de 1988. Promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>. Acesso em: 03 dez. 2018.

BUENO, Sonia. Trust in News: 'Fake news' reforçam confiança na imprensa. Disponível em: https://br.kantar.com/tecnologia/comportamento/2017/trust-in-news-confianca-nas-noticias-estudo-kantar/>. Acesso em: 01 dez 2018.

CARDOSO, Wiliiam. Um crime de ódio é registrado a cada 12 horas na cidade de São Paulo. Folha de São Paulo, 12 nov. 2017. Disponível em: < https://www1.folha.uol.com.br/cotidiano/2017/11/1934809-um-crime-de-odio-e-registrado-a-cada-12-horas-na-cidade-de-sao-paulo.shtml > Acesso em: 03 dez. 2018.

CARVALHO, Mayara. Brigas em redes sociais aumentam número de processos na Justiça. Jornal opção, 15 abril 2018. Disponível em < https://www.jornalopcao.com.br/ultimas-noticias/brigas-em-redes-sociais-aumentam-numero-de-processos-na-justica-122637/>. Acesso em 26 jul 2018.

CASTRO, Fábio de. 'Fake news' têm 70% mais chance de viralizar que as notícias verdadeiras, segundo novo estudo. Disponível em: < https://ciencia.estadao.com.br/noticias/geral,fake-news-se-espalham-70-mais-rapido-que-as-noticias-verdadeiras-diz-novo-estudo,70002219357>. Acesso em: 01 dez 2018.

D'URSO, Luiz Augusto. Cibercrime: perigo na internet!. Disponível em <https://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet/>. Acesso em 09 out 2018.

FILHO, Mário Simas; **RODRIGUES**, Alan. Perigo Digital. Disponível em <https://istoe.com.br/9581_PERIGO+DIGITAL/>. Acesso em: 22 jul 2018.

G1. Mundo tem 3,2 bilhões de pessoas conectadas à internet, diz UIT. 26 maio 2015. Disponível em:<http://g1.globo.com/tecnologia/noticia/2015/05/mundo-tem-32-bilhoes-de-pessoas-conectadas-internet-diz-uit.html>. Acesso em 27 jul 2018.

GIOVANELLI, Carolina. Quatro motivos para a disseminação das fake news. Disponível em: < https://vejasp.abril.com.br/blog/terapia/fake-news-motivos-compartilhar/>. Acesso em: 01 dez 2018.

GONÇALVES, Ana Paula Schwelm. A vingança pornô e a Lei Maria da Penha. Jus, fev. 2017. Disponível em: <https://jus.com.br/artigos/56026/a-vinganca-porno-e-a-lei-maria-da-penha > Acesso em: 27 jul. 2018.

Hootsuite. Disponível em: <https://hootsuite.com/pt/pages/digital-in-2018>. Acesso em 09 out 2018.

INTERNET.ORG; FACEBOOK. State of Connectivity 2015. A Report on Global Internet Access. Disponível em: < https://fbnewsroomus.files.wordpress.com/2016/02/state-of-connectivity-2015-2016-02-21-final.pdf>. Acesso em: 26 jul 2018.

ISTART. Conflitos em WhatsApp lideram ocorrências digitais nas escolas. Disponível em: <Conflitos em WhatsApp lideram ocorrências digitais nas escolas> Acesso em: 16 ago. 2018.

MANSSUR, Maria Gabriela Prado. Pornografia de Revanche. Justiça de saia, 21 jun. 2018. Disponível em: <http://www.justicadesaia.com.br/pornografia-de-revanche/>. Acesso em: 27 jul. 2018.

MINISTÉRIO DA JUSTIÇA. Governo federal irá mapear crimes de ódio na internet. Brasília, 20 nov. 2014. Disponível em: < http://www.justica.gov.br/news/governo-federal-ira-mapear-crimes-de-odio-na-internet> Acesso em: 03 dez. 2018.

MINISTÉRIO PÚBLICO FEDERAL. A melhor forma de combater os crimes de ódio na internet é a prevenção e a educação. Disponível em: < http://www.mpf.mp.br/pgr/noticias-pgr/a-melhor-forma-de-combater-os-crimes-de-odios-na-internet-e-a-prevencao-e-a-educacao-defende-mpf > Acesso em: 03 dez. 2018.

MINISTÉRIO PÚBLICO FEDERAL. Órgãos do sistema de Justiça precisam se preparar para combater crimes cibernéticos. Disponível em <http://www.mpf.mp.br/pgr/noticias-pgr/orgaos-do-sistema-de-justica-precisam-se-preparar-para-combater-crimes-ciberneticos>. Acesso em 09 out 2018.

NOGUEIRA, Sandro D'amato. Pedofilia e tráfico de menores pela Internet: O lado negro da web. In: **Âmbito Jurídico**, Rio Grande, II, n. 6, ago 2001. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5556>. Acesso em: 23 jul 2018.

OLIVEIRA, Jeferson. Pedófilos atacam crianças vulneráveis pelas redes sociais**.** Disponível em: <http://circuitomt.com.br/editorias/cidades/113219-criancas-sao-vitimas-de-pedofilia-digital.html>. Acesso em: 22 jul 2018.

OLIVEIRA, Lucas. Brasil Escola. Cyberbullying. Disponível em: <https://brasilescola.uol.com.br/sociologia/cyberbullying.htm> Acesso em: 15 ago. 2018.

ONG END REVENG PORN. Revengeporn em números, 20 fev. 2014. Disponível em: <http://www.administradores.com.br/infograficos/tecnologia/revenge-porn-em-numeros/26/> Acesso em: 28 jul. 2018.

ORTEGA, Flávia Teixeira. O que são os crimes de ódio. Jus Brasil, 2015. Disponível em: < https://draflaviaortega.jusbrasil.com.br/noticias/309394678/o-que-sao-os-crimes-de-odio > Acesso em: 03 dez. 2018.

PUGLIERO, Fernanda. Como o ódio viralizou no Brasil. Carta Capital, 20 ago. 2018. Disponível em: < https://www.cartacapital.com.br/sociedade/como-o-odio-viralizou-no-brasil > Acesso em: 03 dez. 2018.

REVISTA FÓRUM. Pornografia de revanche: em dez dias, duas jovens se suicidam, 21 nov. 2018. Disponível em: <https://www.revistaforum.com.br/revenge-porn-divulgacao-de-fotos-intimas-culmina-com-suicidio-de-duas-jovens/> Acesso em: 27 jul. 2018.

REVISTA ISTO É. 'Feia e perdedora': adolescente vítima de bullying nos EUA se suicida. 05 dez. 2017. Disponível em: <https://istoe.com.br/feia-e-perdedora-adolescente-vitima-de-bullying-nos-eua-se-suicida/> Acesso em: 15 ago. 2018.

SANTOMAURO, Beatriz. Cyberbullying: a violência virtual. Nova escola, 01 jun. 2018. Disponível em: <https://novaescola.org.br/conteudo/1530/cyberbullying-a-violencia-virtual> Acesso em: 16 ago. 2018.

SAFER NET BRASIL. Disponível em: <http://www.safernet.org.br/site/jornalistas/pauta/crescem-den%C3%BAncias-de-pornografia-infantil>. Acesso em: 22 jul 2018.

SAFER NET BRASIL. Dísponível em <http://indicadores.safernet.org.br/>. Acesso em 09 out 2018.

TRINDADE, Jorge; **BREIER**, Ricardo. Pedofilia - Aspectos Psicológicos e Penais - Col. Direito e Psicologia - 3ª Ed. 2013.

UNICEF. 2º Congresso Mundial contra a Exploração Sexual e Comercial de Crianças. Disponível em: <https://www.unicef.org/events/yokohama/>. Acesso em 22 jul2018.

VIEIRA, Frederico. Viver nas redes: A presença dos sujeitos entre as tecnologias online e o mundo offline. MARTINO, Luís Mauro Sá, MARQUES, Angela Cristina Salgueiro (Organizadores)Teorias da comunicação: processos, desafios e limites.São Paulo: Plêiade, 2015, p. 127-128.

WE ARE SOCIAL. Digital in 2018: world's internet users pass the 4 billion mark**.** Disponível em <https://wearesocial.com/blog/2018/01/global-digital-report-2018>. Acesso em 09 out 2018.

2

A SUPEREXPOSIÇÃO NAS REDES E O ROUBO DE DADOS PESSOAIS VISANDO À PRÁTICA DE CRIMES

Marcella Almeida Brandão Rebouças[1]
e Renata Lorena Almeida Brandão Rebouças[2]

RESUMO

Esse artigo busca apontar crimes cibernéticos atuais ocasionados pela superexposição na rede, parte da própria cultura brasileira, e que vem ocasionando graves danos à população, além de direcionar para uma possível solução do problema.

Palavras-chave: Superexposição. Roubo de dados pessoais. crimes cibernéticos.

1. INTRODUÇÃO; 2. história da internet; 3. Redes Socais 3.1. Exposição de dados pessoais em redes sociais 3.2. Meio de Ingresso nas Redes Sociais 3.3. Consequências Práticas das Redes Sociais 3.3.1. Aplicação de Golpes 3.3.1.1. Uso de OSINTS na prática de golpes 3.3.1.2. Roubo de Dados Através de Cookies 3.3.2. O OUTRO LADO; 4. Aplicação da inteligência DIGITAL PARA CONTENÇÃO DE CRIMES; 5. LEGISLAÇÃO 5.1. Legislação brasileira 5.1.1. Lei Geral de Proteção de Dados 5.2. Legislação comparada 5.2.1 Nova Lei de Proteção de dados da União Europeia; 6. CONCLUSÃO.

1. INTRODUÇÃO

No Século XXI, as redes sociais tornaram-se um dos maiores meios de comunicação e interação social. Aquilo que nos diferenciava nos primórdios

1 Graduanda em Direito pela Faculdade Baiana de Direito

2 Graduada em Direito pela Faculdade Baiana de Direito

da civilização, em que os acidentes geográficos determinavam o isolamento de povos e cidades e provocavam, inclusive, o surgimento de variáveis do idioma, agora cede lugar a uma acessibilidade total, sem fronteiras espaciais, em que se fala uma única linguagem, a das Wikis.[3] Acontece que, no brasil, uma cultura de superexposição cresceu junto com a expansão das redes sociais.

O Direito Digital se incumbiu de uma difícil missão, a de equilibrar uma relação coexistente entre a privacidade, o anonimato, a responsabilidade e o interesse comercial ocasionada pelos veículos de comunicação modernos. Para que isso, de fato, ocorra é necessária uma vigilância e procedimentos de punibilidade que precisam ser determinados pelo próprio direito digital.

São comuns, nos dias atuais, as postagens diárias e frequentes dos usuários das plataformas da internet, contando cada passo do dia, sem se preocupar com aqueles que podem estar acompanhando aquilo.

O excesso de exposição na rede é o que ocasiona uma serie de crimes bastante graves, e é justamente isso que será detalhado ao longo do presente trabalho: como as leis podem prevenir e coibir a prática desses crimes diante das postagens desenfreadas.

2. HISTÓRIA DA INTERNET

O primeiro relato da Web é datado da década de 90, na Suíça, com Tim Berners-Leda e boa parte dos estudiosos do assunto acreditam que, até o momento, a mesma passou por três fases importantes. Para muitos, a primeira fase é conhecida como a "internet das empresas"; nesta, os consumidores (usuários) tinham a função de apenas consumir o conteúdo colocado pelas grandes empresas. Neste momento da web, não havia comunicação de duas vias entre cliente e marca, período em que a internet ainda estava se popularizando, aproximadamente entre os anos de 1998 a 2003, quando o número de usuários ainda era inexpressivo.

Esta primeira fase também ficou conhecida como Web 1.0; sua grande virtude foi a democratização do acesso à informação. Entretanto, havia uma baixa interação do usuário, um mero espectador dos conteúdos publicados por empresas, sem poder contar com canais adequados de interação, basicamente ofertadas somente através de chats online ou e-mails, um processo onde poucos produzem e muitos consomem, algo muito parecido com o modelo de broadcasting da indústria midiática de hoje.

3 DIMANTAS, Hermani. As Zonas de Colaboração. Tese (Doutorado) Escola de Comunicação e Artes, Universidade de São Paulo. 2010. Disponível em:<http://www.teses.usp.br/teses/disponiveis/27/27154/tde-17022011-1224000/…/679860.pdf>.

A segunda fase é conhecida como Web 2.0, marcada pela participação direta do internauta como um produtor de conteúdos; é uma fase onde muitos produzem e todos podem consumir, há uma grande popularização de serviços como blogs, redes sociais e sites de publicação de vídeos. A função do usuário muda, ele deixa de ser apenas consumidor e se torna um produtor.

A internet deixou de ser apenas uma rede de computadores e se consolidou como uma rede de pessoas; pessoas que participam cada vez mais, que querem se expor, seja por meio de divulgação de textos, comentários em blogs, compartilhamento de links ou apenas pela publicação das fotos do seu último aniversário. A interatividade que movimenta este momento da Web apresenta um panorama completamente diferente do anterior, pois os produtores são, ao mesmo tempo, o público, o qual também é composto das pessoas que estão apresentando ideias, divulgando materiais que outras pessoas fizeram ou colaborando com o aprimoramento de conteúdo já publicado.[4] Um grande avanço que esta fase trouxe foi a democratização da produção de conteúdo, que não ocorria na fase anterior.

A terceira fase da Web é conhecida também como Web Semântica, reúne as duas anteriores e soma a essas a inteligência das máquinas. Na Web 3.0 a produção de conteúdo, assim como as ações, são derivadas da união dos usuários às máquinas; com isso, a infraestrutura da internet passa a ser protagonista quando se trata de gerar conteúdo. Nessa fase é possível que sejam levados aos usuários serviços e produtos com alto valor agregado, graças a sua alta personalização, tornando possível a democratização da capacidade de ação e conhecimento, que antes só estava acessível às empresas e aos governos.

Alguns entendedores defendem que já estamos na fase da Web 3.0, outros acreditam que ainda estamos caminhando para isso. Essa divergência se da devido ao que cada um considera inteligência das máquinas. Os que defendem que já se vive a terceira fase da Web entendem que a personalização do conteúdo que chega para o usuário já é derivado da inteligência das máquinas, divergindo dos que acreditam que ainda não se alcançou esse momento, por não considerar tal fato suficiente para caraterização da Web 3.0.

3. REDES SOCIAIS

O avançar tecnológico na comunicação se dirige ao objetivo de criar uma Aldeia Global, que permita que todas as pessoas do mundo possam ter acesso a um fato de modo simultâneo, sendo esse o princípio que determinou a criação das redes mundiais.

4 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg.449.

Esse cenário se expandiu tanto que provocu a necessidade de expandir tais benefícios aos lares. Por essa razão, teve início a um movimento para instalar um computador em cada casa, saindo da esteira econômico-corporativa e passando a levar a tecnologia para dentro dos lares, interligando uma rede de consumidores ávidos por informação, serviços e produtos[5].

Com o avanço da tecnologia e o aumento da globalização se torna cada vez mais comum que as pessoas tenham uma ou mais redes sociais, chegando a serem considerados um ponto fora da curva aqueles que não possuem. Hoje em dia, até mesmo no momento em que você preenche uma ficha de emprego já solicitam a sua rede social.

Nesse cenário, como afirma Patricia Peck Pinheiro[6], cabe ao Direito Digital o papel de equilibrar a relação existente entre o interesse comercial, a responsabilidade, o anonimato e a privacidade, gerada pelos inovadores veículos de comunicação. São inúmeras as redes sociais existentes atualmente e utilizadas no âmbito do Brasil; as mais populares entre os brasileiros são o Facebook, Instagram e Twitter, embora existam ainda inúmeras outras também muito utilizadas.

De acordo com Nogueira[7], as redes sociais são o meio pelo qual os indivíduos se reúnem por afinidades e com objetivos em comum, sem haver barreiras geográficas e sendo possível a realização de conexões com dezenas, centenas e milhares de pessoas, sejam elas conhecidas ou não.

Já Marteleto, citado por Castro[8], define as redes sociais como sendo algo que representa um conjunto de participantes autônomos, que unem ideias e recursos em torno de valores e interesses compartilhados. A questão central das redes, segundo ele, é justamente a valorização dos elos informais e das relações, em detrimento das estruturas hierárquicas. As redes sociais são as relações entre os indivíduos na comunicação mediada por computador. Esses sistemas funcionam através de uma interação social, buscando conectar pessoas e proporcionar sua comunicação.

A rede social possui uma capacidade tão grande que alcança a rápida mobilização de pessoas fortemente concentradas a um determinado objetivo. As grandes manifestações que houve no Brasil em 2013 são um exemplo claro des-

5 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 67.

6 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 94.

7 NOGUEIRA, Josicleido. O que são Redes Sociais? Administradores. Jun/2010. Disponível em: <http://www.administradores.com.br/artigos/tecnologia/o-que-sao-redes-sociais/45628>. . Acesso em: 19 de Abril de 2018.

8 CASTRO, Raisa. Redes Sociais e a sua contínua evolução. Petcomofam. Jun/2013. Disponível em: <http://petcomufam.com.br/2013/06/redes-redes-sociais-e-sua-continua-evolucao.html> Acesso em: 19 de Abril de 2018.

se potencial. A mobilização se iniciou nas redes sociais e alcançou as ruas com uma eficácia e intensidade que conseguiu assustar a cúpula governamental, isso porque os acontecimentos chegavam rápido às redes sociais e se espalhavam.

Através das redes sociais torna-se possível a criação de discussões para um determinado tema, surgem opiniões, formam-se artigos, pretensões e até mesmo conclusões, ou seja, é um meio que oferece o crescimento e amadurecimento em um debate.

É também considerado meio de ajuda na carreira profissional, na medida em que existem sites de relacionamento com perfil profissional, em que se podem apresentar suas ideias, ate mesmo grandes projetos, e é um local em que empreendedores e empresas buscam novos profissionais, constituindo, assim, uma rede interativa.

São inúmeros os benefícios das redes sociais na vida das pessoas; através delas é possível reencontrar velhos amigos de infância, estar perto e acompanhar a vida das pessoas que você gosta mesmo quando se muda pra longe; é um novo canal de denúncias contra agressões de todos os tipos, torna possível ter noticias dos amigos mesmo não podendo vê-los com tanta frequência, por conta da agenda, é um meio de voz pois, através dos compartilhamentos, pode-se atingir um número de leitores jamais imaginado, além de ser também uma distração para momentos de estresse.

Só que, como tudo na vida, também tem seus pontos negativos, uma vez que as redes sociais oferecem um relacionamento superficial com as pessoas, os usuários, sem perceber, acabam perdendo muito tempo da vida nas redes sociais, deixando de viver; por conta disso, passa-se muito tempo verificando o que o outro está fazendo em vez de cuidar da própria vida, e há um estimulo a uma exposição constante de felicidade; busca-se cada vez mais compartilhar e expor uma vida perfeita que, na maioria das vezes, não existe, o que pode trazer muitas consequências ruins.

Conclui-se, portanto, que o surgimento das redes sociais possibilitou diversos avanços, facilitando o encontro de pessoas seja para se reencontrar ou para se conhecer, possibilitando discussões de todos os ramos. Com a sua criação também surgiu um novo espaço para as mentes criminosas aprimorarem os seus crimes e conseguir atingir mais pessoas.

3.1. Exposição de dados pessoais em redes sociais

Atualmente há uma superexposição das pessoas nas redes sociais, e isso tem sido uma grande problemática. Por um lado, algumas pessoas enxergam na exposição via internet uma maneira de promoção da sua imagem pessoal. Já por outro viés, há aqueles que defendem a privacidade e o bom senso.

As redes sociais são usadas por muitas pessoas como forma de promoção da sua imagem, chegando a ser reconhecida, no cenário atual, a profissão de "digital influencer", que são aquelas pessoas que postam sua vida nas redes sociais e influenciam pessoas com isso, e ganham das empresas para divulgarem os seus produtos.

Ocorre que as pessoas estão cada vez mais querendo se espelhar nessas influenciadoras, não só adquirindo o que elas divulgam, mas, também, querendo postar assim como elas, acreditando que irão conseguir os mesmos benefícios que aquelas possuem. A atualidade passou a medir as pessoas pelo número de seguidores.

Todavia, essa busca desenfreada por popularidade nas redes sociais acaba expondo as pessoas de um modo que muitas vezes elas nem percebem, passando a correr riscos desnecessários. O número de golpes realizados por conta do conteúdo das redes sociais tem crescido assustadoramente, a superexposição tem sido uma ferramenta de trabalho daqueles que se utilizam da internet para prática de crimes.

O que é postado em uma rede social hoje pode ganhar uma grande proporção; quem posta não tem como saber onde vai ter um fim; não é possível voltar atrás e retirar aquilo que já foi exposto. As pessoas estão se acostumando a postar coisas sensíveis sem atentar para quem pode vir a usar aquilo. Principalmente os jovens, se acostumaram a postar a sua rotina nas redes sociais, nas famosas "histórias". Postam a saída de casa, fotos na academia, escola, faculdade, a festa que vão, restaurantes onde comem e ainda cometem o grande erro de marcar onde estão, facilitando ainda mais a vida daqueles que querem usar aquilo para a prática de crimes.

Além das "histórias", existe o "feed", que é a sua página, de fato, e as pessoas nela postam fotos da vida, da família. Cita-se nome dos familiares, dos cachorros que se tem, dos amigos que possui, das viagens que faz, entre as demais coisas da rotina dos usuários. Acontece que as pessoas, ao postarem, não percebem que fazem da vida um livro aberto, e que qualquer estranho pode vir a saber da sua vida.

É justamente na fragilidade dos usuários que as mentes criminosas encontram espaço para a prática dos seus crimes. Qualquer pessoa passa a conhecer a vida daqueles que postam frequentemente e fica habilitada a se passar por alguém conhecido e obter a confiança das suas vítimas.

3.2. Meio de Ingresso nas Redes Sociais

O meio pelo qual se torna possível ingressar nas redes sociais é um ponto complexo. Para entrada em uma rede social o usuário tem que se inscrever em algum site, sendo esse tipo de serviço fornecido gratuitamente, na maioria dos casos.

Ocorre que para realizar essa inscrição é necessário informar os dados pessoais no ato, podendo ser acessados pelos demais usuários conforme o consentimento dono do perfil. Os dados como: nome, idade, email, telefone, entre outros, a depender da rede social. Esses dados são uma espécie de apresentação online, que permite aos interessados uma visualização de algumas informações por parte daquele que busca.

Além dos dados do cadastro, ao ingressar na rede, normalmente, informa-se também local em que se estudou ou trabalhou, com a justificativa de encontro dos amigos que estiveram no mesmo local que você.

Ademais, existem também os termos de uso, que os usuários são obrigados a concordarem se quiserem ingressar na rede social. O Facebook, por exemplo, tem uma política de dados que fica disponível na plataforma, mas poucos são aqueles que leem. O facebook informa os seguintes termos:

> Para fornecer os Produtos do Facebook, precisamos processar informações sobre você. Os tipos de informações que coletamos dependem de como você usa nossos Produtos. Para saber mais sobre como acessar e excluir as informações que coletamos, acesse as Configurações do Facebook e do Instagram.
>
> Coisas que você e outras pessoas fazem e fornecem.
>
> Informações e conteúdos que você fornece. Coletamos o conteúdo, comunicações e outras informações que você fornece quando usa nossos Produtos, inclusive quando você se cadastra para criar uma conta, cria ou compartilha conteúdo, envia mensagens ou se comunica com outras pessoas. Isso pode incluir informações presentes ou sobre o conteúdo que você fornece (como metadados), como a localização de uma foto ou a data em que um arquivo foi criado. Isso pode incluir também o que você vê por meio dos recursos que fornecemos, como nossa câmera, de modo que possamos realizar ações como sugerir máscaras e filtros de que você pode gostar, ou dar dicas sobre o uso de formatos da câmera. Nossos sistemas processam automaticamente o conteúdo e as comunicações que você e outras pessoas fornecem a fim de analisar o contexto e o conteúdo incluído nesses itens para as finalidades descritas abaixo. Saiba mais sobre como controlar quem pode ver o conteúdo que você compartilha.
>
> Dados com proteções especiais: é possível optar por fornecer informações nos campos de perfil ou nos Acontecimentos do Facebook sobre sua opção religiosa, preferência política, saúde ou por quem você "tem interesse". Essas e outras informações (como origem racial ou étnica, crenças filosóficas ou filiações sindicais) podem estar sujeitas a proteções especiais de acordo com as leis do seu país.

O Facebook informa aqueles que buscam informação a sua política de dados e, desse modo, confirma que compartilha as informações dos usuários com

a justificativa de facilitar a vida desses, propiciando a eles o que eles buscam de forma mais rápida, por já conhecerem a sua procura. São inúmeras as laudas que explicam as políticas e dados e os termos de uso de cada rede social, por isso a grande maioria das pessoas não leem, o que as torna mais vulneráveis.

Atualmente a maior parte dos termos de uso destes serviços deixa cristalino que, mesmo deixando de ser usuário daquela rede, o que ali foi compartilhado permanecerá lá e na galáxia da Internet para sempre. Cabe, portanto, apenas ao indivíduo, a responsabilidade de reflexão sobre qual conteúdo quer deixar a seu respeito, já que o direito ao esquecimento não é algo fácil de ser conquistado[9].

Conclui-se, portanto, que para o ingresso nas redes sociais é necessário a entrega de inúmeros dados pessoais; para o simples acesso, já é imprescindível a abertura da sua vida para informar um pouco sobre si. Ademais, há necessidade da leitura dos termos de uso das redes sociais, para que as pessoas tenham consciência sobre os dados que estão disponibilizando ao público.

3.3. Consequências Práticas das Redes Sociais

A superexposição nas redes sociais pode ocasionar inúmeras consequências práticas. Aqueles que veem na internet uma ferramenta para a prática de crimes se utilizará daquilo que as pessoas postam contra elas mesmas.

Segundo Sandra Gouveia[10], hoje em dia, com a massificação dos computadores e das redes, qualquer pessoa pode praticar delitos através da informática. Em relação às vítimas dos crimes praticados, as pesquisas são unânimes em dizer que nenhuma estatística é confiável, porque a maioria dos usuários da rede sequer sabem que estão sendo atingidos e, quando descobrem, na maioria dos casos, preferem se calar e arcar com os prejuízos.

Existem vários tipos de crimes que podem ser realizados através das redes sociais ou com o auxílio destas. Além disso, o simples fato de se cadastrar em algumas redes sociais já deixa a pessoa exposta a ter os seus dados vendidos pelas empresas que se utilizam do que você posta e pesquisa para lucrar. Quanto mais dados são fornecidos online, mais fácil para quem quiser utilizá-los para cometer os mais diversos tipos de crimes.

Com a exposição dos dados pessoais como nome de familiares, lugares que frequentam e amigos com que convivem, são inúmeros os tipos de golpes que podem ser aplicados pelas mentes maliciosas que utilizam a fragilidade das pessoas para as atacarem.

---

9 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 101.

10 GOUVÊA, Sandra. O Direito na Era Digital. Rio de Janeiro: Mauad. 1997. Pg. 60.

Muitos utilizam a visualização da rotina através das redes sociais para encontrar as vítimas; com os dados por elas fornecidos, se passam por conhecidos se aproximando e atraindo a usuária para uma armadilha, após conquistar a sua confiança. Com isso podem serem levadas para um sequestro, estupro, roubo com violência ou inúmeros outros crimes semelhantes.

Além desses crimes contra a integridade física, existem crimes como o roubo de dados que, normalmente, é cometido a partir da criação de sorteios ou de prêmios em páginas de redes sociais. Na busca por premiações os usuários da rede precisam se cadastrar e baixar alguns aplicativos, tendo que inserir dados pessoais, CPF, endereço, datas de aniversário etc. Esse crime é tipificado no art.171 do Código Penal Brasileiro[11]:

> "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento."

É possível, ainda, a falsificação de cartões de crédito e a realização de transações bancárias e muito mais, uma vez que existem também alguns softwares que, quando instalados em uma máquina, permitem o acesso a todos os dados pessoais registrados no computador; com os dados em mãos, é possível a prática dos crimes.

Esse crime é muito mais comum e, por isso, está tipificado no art. 154-A do Código Penal Brasileiro[12], nos seguintes termos:

> "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: (...)"

Tendo em vista que a criação de contas em redes sociais é bem fácil, simples e rápido, é normal que pessoas mal-intencionadas utilizem isso para prejudicar pessoas físicas ou empresas. É possível a criação de contas utilizando nomes falsos, o que possibilita a divulgação de conteúdos mentirosos e difamatórios, gerando, desse modo, problemas para as pessoas expostas. Um aspecto cruel dessa realidade interativa é a possibilidade de construção de uma imagem digital de um indivíduo criada pelos demais, apenas com a análise do que por ele é compartilhado, sem que a própria pessoa consiga interferir ou evitar.

---

11 BRASIL. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm> Acesso em: 29 de Out. de 2018.

12 BRASIL. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm> Acesso em: 29 de Out. de 2018.

A era atual não é da liberdade de expressão individual, mas sim da de todos; há um fenômeno coletivo-social ilimitado. Nesse quesito entram as leis, com a finalidade de restringir até onde se pode ir, sem ferir o outro[13].

São inúmeros os tipos de golpes que podem ser aplicados através da internet e eles estão cada vez mais individualizados para cada tipo de vítima e de ataque. A maioria dos golpes que temos hoje são em massa, enviados por email, mensagem... Mas a tendência é que os golpes se tornem mais personalizados, os criminosos já estão usando as informações pessoais divulgadas pelos próprios usuários para fornecer uma falsa impressão de segurança; golpes individualizados são muito mais prováveis de obter sucesso. Alguém que, por exemplo, recebe um email com seu nome, nome de sua mãe, cidade onde mora, lugar que frequentou recentemente, e outras informações facilmente adquiridas em uma rede social, dificilmente vai imaginar que não é um email verídico.

O maior problema jurídico dos crimes virtuais é a raridade das denúncias, e, pior, o despreparo da polícia investigativa e de perícia para apurá-las. Embora seja possível fazer boletins de ocorrência pela Internet[14], são poucos as equipes e profissionais preparados para a investigação de um crime virtual.

É importante lembrar que os criminosos da Internet não são criminosos incomuns - a imagem de um sujeito extremamente inteligente e com vasto conhecimento técnico já não corresponde à realidade pois, atualmente, é muito fácil encontrar na Internet o código-fonte aberto de um vírus ou trojan.[15] As pessoas precisam ficar atentas para as informações que fornecem e as coisas que divulgam, pois é muito difícil saber a intenção de quem está do outro lado e, com a hiperconexão, a quantidade de ataques só tende a aumentar.

3.3.1. Aplicação de Golpes Atuais e Futuros

É muito comum o uso de plataformas como o Instagram ou Facebook para a venda de produtos online. Existem vários perfis que são verdadeiras lojas, com diversas opções de produtos, e afirmando que entregam em todo o Brasil, e até no exterior. Essa opção facilitou muito a vida de alguns comerciantes, reduzindo seus gastos, visto que deixam de pagar aluguel ou realizar compra de "ponto" para a sua loja. Entretanto, existem pessoas que se aproveitam do fato de a relação ser toda online para aplicar golpes.

---

13 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 101.

14 Portaria DGP n. 1, de 4 de fevereiro de 2000: Disciplina a recepção e o registro de ocorrências

15 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 383

O crime eletrônico é, em princípio, um crime de meio[16], isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*[17] que, de algum modo, podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não.[18] A maioria dos crimes cometidos na rede ocorre também no mundo real. A internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona.[19]

Existem vários relatos pelo país de pessoas que pagaram por produtos que foram vendidos em redes sociais e nunca os receberam. Normalmente são produtos com preço abaixo do mercado, afirmando ser uma grande promoção, algumas lojas mandam produtos grátis para influenciadores digitais para que estes divulguem o seu perfil, passando credibilidade para os possíveis compradores. Muitas vezes botam um prazo de entrega muito longo, para que nesse período consigam realizar o maior número de "vendas" possível e, quando o consumidor percebe que foi enganado, o perfil da loja não existe mais, deixando-o sem saber o que fazer para ter o seu dinheiro de volta.

Alguns criminosos praticam até mesmo a clonagem de sites, que, nesse caso, exige expertise tecnológica acima da média, utilizando-os para roubar informações dos usuários, tais como RG, CPF, residência, telefone, e-mail, dados

16 Segundo proposto por Robson Ferreira em sua tese de crimes eletrônicos, podemos estudar uma classificação dos crimes por computador levando em conta o papel do computador no ilícito: 1) quando o computador é o alvo - p ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação do conteúdo do banco de dados furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo de fora da empresa; 2) quando o computador é o instrumento do crime - p.ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraudes de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime - ex.: crimes contra a honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registo de atividades do crime organizado; 4) quando o crime esta associado com o computador - p. ex.: pirataria de software, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas, comércio ilegal de equipamentos e programas.

17 No Brasil a tendência de que sejam tipificadas algumas condutas criminosas próprias da Internet se confirmou com a aprovação de suas leis de crimes digitais.

18 Fortalecendo esta corrente de pensamento, temos o julgamento pelo Ministro Sepúlveda Pertence, do STF, de um habeas corpus (76689/PB 22-9-1998) sobre o crime de computador: "Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminosa, o meio técnico empregado para realizá-la pode até se de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendida morte dada a outra mediante arma de fogo."

19 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 380

bancários - informações utilizadas posteriormente para que o criminoso assuma outras identidades em operações comerciais com uso de cartão de crédito clonado. O combate a esses crimes torna-se extremamente difícil por dois motivos: a) a falta de conhecimento do usuário, que, dessa forma, não passa às autoridades as informações relevantes e precisas; e b) a falta de recursos, em geral, das autoridades policiais.[20]

Trata-se de prática usual também a criação de perfis falsos (*fakes*) para a difamação de pessoas ou estabelecimentos. Muitas pessoas que não têm coragem de fazer coisas em nome próprio, ou querem fazer coisas que se em nome próprio trariam consequências que elas não desejam, utilizam os perfis fakes. É comum entre jovens, muitas vezes utilizado como ferramenta para a realização do *bullying*, que pode terminar com consequências drásticas.

As redes sociais também são utilizadas para obter informações sobre a vítima para a realização de crimes como extorsão ou sequestro. Nesses casos, são utilizadas as informações que a própria vítima expõe sobre si mesma, seus hábitos, seus familiares; o criminoso se aproxima da vítima e passa um sentimento de confiança.

Existem crimes comuns, como a criação de perfis falsos usando a foto de outras pessoas para aplicar golpes. Um exemplo seria entrar em aplicativos de paquera, conversar com alguém se passando por outra pessoa, adquirir a confiança da vítima e pedir dinheiro com alguma desculpa; os usuários, por acharem que conhecem quem está do outro lado, acabam dando, para ajudar aquela pessoa que se quer existe de verdade. Parece algo estranho dar dinheiro a alguém que nunca viu, mas esse tipo de crime é mais usual do que aparenta ser.

Há também a possibilidade de ter o seu perfil hackeado e utilizado por outra pessoa. Páginas de hotel e até mesmo telefones, por exemplo, podem ser hackeados e confirmarem reservas com desconto, caso o depósito do pagamento seja imediato, e feito em uma conta oferecida pelo criminoso.

Além dos crimes envolvendo o patrimônio, existem aqueles ainda mais perigosos que são os sequestros. Existem inúmeros meios de se chegar a esse fim de forma fácil através da internet, tanto conquistando a confiança da vítima através de conversas e a seduzindo até o alvo, ou analisando a sua rotina através das suas postagens para capturá-la no momento mais oportuno.

Pode-se concluir, portanto, que os ataques cibernéticos estão cada vez mais personalizados e individualizados; as vítimas são estudadas e atacadas no momento mais oportuno, e esse ataque não fica só no campo virtual, se exterioriza, podendo ocasionar lesões à integridade física dos usuários.

---

20 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 383

3.3.1.1. A Evolução Futura: uso habitual de OSINTS na prática de golpes

OSINT (Open Source Intelligence) é o termo usado, principalmente, na língua inglesa, para descrever o serviço de inteligência que coleta informações através de dados disponíveis para o público em geral, através de jornais, revistas e, especialmente, redes sociais e sites virtuais.

Trata-se de uma ferramenta de inteligência que objetiva encontrar, adquirir e selecionar informações de fontes abertas para que possam ser analisadas e, juntas, produzirem conhecimento.

O Foreign Broadcast Information Service (FBIS) é um serviço norte-americano que primeiro utilizou o sistema de OSINT. O inicio das atividades ocorreu no final da década de 1930, na Universidade de Princenton. Esse sistema surgiu na Segunda Guerra Mundial, com o objetivo de analisar os noticiários internacionais captados por rádio e, durante a Guerra Fria, monitorar publicações oficiais provenientes da União das Repúblicas Socialistas Soviéticas, como o Pravda e o Izvestia.

A finalização da Guerra Fria propiciou ao FBIS um período de ostracismo, até o momento dos atentados, em 2001, contra o Pentágono e o World Trade Center. Esses atos de terrorismo trouxeram à tona a importância da utilização das fontes abertas. Para o governo, a utilização de OSINT é interessante devido ao baixo custo que se tem na coleta através de fontes abertas, principalmente em comparação com as operações de campo, que são bastante onerosas.

Ocorre que não só as autoridades governamentais se utilizam dessa ferramenta. Hoje, criminosos já dominam o uso das OSINTS e, com isso, são capazes de coletar os dados abertos das suas vítimas para obter informações concretas sobre elas. Através desse método de inteligência, é possível a clonagem de cartões e descobertas de senhas de bancos, por exemplo.

Percebe-se que as OSINTS podem ser muito proveitosas para as investigações públicas, pelo seu baixo custo, mas a sua existência possibilita também o seu uso por criminosos, que encontraram nessa inteligência mais uma fonte para prática de crimes cibernéticos, que precisem de um número maior de dados para serem concretizados.

É necessário que as pessoas tenham ciência da existência dessa ferramenta, capaz de juntar dados disponíveis para obtenção de um conhecimento especifico sobre a vítima, sua conta bancária e outras informações capazes de propiciar estelionatos e outros crimes.

3.3.1.2. Roubo de Dados Através de Cookies

Existem arquivos de internet que são capazes de armazenar temporariamente aquilo que o internauta visita na rede, são conhecidos como *cookies*. São bays que usualmente possuem formato de texto e que não ocupam espaço

no disco rígido dos computadores; ainda assim, não possuem limites para as informações que podem ser armazenadas.

Os *cookies* são capazes de registrar as preferências de pesquisa no Google, um endereço de e-mail, a cidade de onde o usuário está conectado, entre outras muitas informações. É justamente a capacidade de registro que pode o tornar um grande vilão da internet, se for usado com objetivos ruins.

Os *cookies* são os responsáveis pela guarda da senha e logins em sites que precisam dos mesmos, o que parece prático e eficaz, mas pode ser um perigo na medida em que se acesse esses tipos de site em computadores públicos e que podem acabar registrando informações confidenciais.

Além das informações armazenadas, os *cookies* têm a capacidade de registrar sites que os internautas acessam enquanto navegam, expondo a privacidade dos usuários das redes para outras pessoas.

Essas informações guardadas, muitas vezes são vendidas para as empresas conseguirem anunciar especificamente o que o usuário busca na rede, apresentando promoções e lojas que ofereçam aquele produto.

Os *cookies,* além de te induzirem à compra de produtos com a propaganda excessiva daquilo que você buscou, podem atrapalhar o desempenho do computador, tendo em vista que, apesar de não ocuparem muitos dados, eles acabam se tornando uma sujeira virtual, junto com outros arquivos virtuais.

Nos dias atuais existe um novo tipo de profissional responsável por estudar a ciência da análise de dados, para que se possa até mesmo prever ou determinar certos comportamentos.

De acordo com o que afirma Stephen Baker, citado por Patricia Peck Pinheiro[21], os Numerati determinam-se por ser uma elite global de cientistas da computação e matemáticos que analisam todos os nossos movimentos através de uma grande quantidade de dados. Desse modo, se torna possível montar padrões de comportamento prevendo, dentre outros, em quem iremos votar, o que iremos comprar e aptidões profissionais.

A força dos Numerati está diretamente ligada com a imensa gama de informações que cada indivíduo compartilha, seja de forma privada, através de cadastros, ou de forma aberta, através das Mídias Sociais[22].

Hoje já há proteção legal para a privacidade que foi positivada na Lei do Marco Civil da Internet e ganhou uma proteção ainda maior na nova Lei Geral de Proteção de Dados, aprovada em 2018.

---

21 BAKER, Stephen apud PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 95.

22 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 96.

Passou a haver um limite na medida em que o usuário tem o direito de não querer que usem e repassem seus dados, assim como a empresa tem o direito de não querer tê-lo como cliente. Por isso as autorizações e termos de uso; se o usuário não aceita expressamente, sequer pode seguir no site.

Antes do Marco Civil da Internet, se um usuário deixasse a rede os seus dados continuavam com ela, podendo ser usados e repassados, de forma ilimitada e para qualquer tipo de propósito, mas hoje isso passou a ser regulamentado.

Logo, pode-se perceber que as leis estão vindo para tentar controlar e regular o uso da internet, mas as pessoas precisam ficar atentas para entenderem que aquilo que buscam poderá ser visto por outras pessoas e utilizado para propaganda dentro da rede de cada usuário, assim como ler de fato os termos de uso dos sites que acessam para analisarem a real viabilidade de os acessarem ou não.

4. APLICAÇÃO DA INTELIGÊNCIA DIGITAL PARA CONTENÇÃO DE CRIMES

Por outro lado, a superexposição também já está sendo útil para auxilio da polícia brasileira. A Polícia Civil de São Paulo tem utilizado uma técnica chamada "cerca elétrica", para prevenir delitos e mapear suspeitos. O método, também chamado de coleta em fonte aberta, permite acompanhar em tempo real informações em redes sociais como Facebook, Instagram e Twitter.

Para isso, os agentes usam filtros de geolocalização, delimitando uma área específica, ou por palavras-chave, as *tags*. Nesse caso, se alguma postagem contiver um dos termos selecionados ("assalto", "tiro", "arma de fogo", por exemplo), o policial recebe um alerta. "Não é um método intrusivo, a coleta é feita com informações que os próprios usuários disponibilizam", explica Caselli. "A grande técnica é conseguir 'minerar' as informações." Na capital, a Secretaria da Segurança Pública (SSP) tem um núcleo de inteligência que, entre as suas atribuições, monitora publicações na internet.[23]

Se, por um lado, temos as mentes criminosas se utilizando das novas técnicas digitais para especificar seus golpes, por outro temos alguns locais do Brasil com uma equipe de polícia especializada em conter golpes, se utilizando das mesmas ferramentas que os bandidos usam para práticá-los.

Todavia, apesar de existir, em alguns lugares, equipe especializada para o uso das novas técnicas digitais, a realidade comum do Brasil é de uma polícia investigativa despreparada que, na maioria dos casos de crimes digitais, não tem conhecimento técnico suficiente para solucionar o caso.

---

23 Felipe Resk, O ESTADÃO DE SP. Disponível em: https://sao-paulo.estadao.com.br/noticias/geral,cerca-eletronica-da-policia-na-internet-ajuda-a-resolver-crimes,70002599616. 25 de novembro de 2018.

5. LEGISLAÇÃO

Com o passar do tempo, a internet foi se desenvolvendo e se tornando cada vez mais complexa; com isso, leis foram surgindo para tentar acompanhar o seu crescimento, mas não na mesma velocidade, o que fez com que os usuários acabassem desprotegidos, em várias situações.

Qualquer lei sobre privacidade, bem como proteção de dados, terá um impacto direto na economia digital, podendo romper por completo com a forma com a qual a internet se desenvolveu. A proteção da privacidade tem um custo e ocasiona um ônus para o usuário final, que em tese, muitas vezes, esta satisfeito com a possibilidade de "pagar" por serviços com a entrega de seus dados[24].

A privacidade dos indivíduos, no que diz respeito à utilização da internet, é de extrema relevância para ser discutido apenas em nível nacional, cada país com a sua própria regulamentação, uma vez que a internet possui natureza global.

Apesar da enorme relevância das leis existentes no Brasil atualmente, é necessário também um tratamento adequado a respeito da privacidade, o que se torna difícil utilizando apenas a lei nacional, sem estabelecer um compromisso internacional sobre a matéria. Por isso analisar-se-a tanto a legislação nacional quanto a comparada sobre o assunto.

5.1. Legislação brasileira

A Lei Federal no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), ficou conhecida por ser uma legislação inovadora, desde seu processo de elaboração, de viés colaborativo, até o seu conteúdo, que tem servido de inspiração para a declaração dos direitos na internet em outros países.[25]

De acordo com Francisco Carvalho de Brito[26], a gênese do Marco Civil da Internet está umbilicalmente ligada à mobilização contrária a outro projeto de lei que visava à regulação da Internet no Brasil. Esse projeto foi o PL 84/1999, de autoria do deputado pernambucano Luiz Piauhylino (PSDB). Com forte apelo penal, este PL foi, durante vários anos, chamado de "AI-5 digital" por seus opositores no debate público.

---

24 PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017. Pg. 98.

25 GONÇALVES, Pedro Vilela Resende. Marco Civil da Internet. Disponível em: <http://irisbh.com.br/marco- civil-da-internet/>. Acesso em: 20 de maio de 2016.

26 ALMEIDA, Guilherme Alberto Almeida de. Democracia 3.0 – Desafios na utilização de tecnologias da informação para uma gestão pública eficiente e participativa. Pg. 262- 293. Disponível em: <http://www.abre.ai/guitecpp> Acesso em: 12 de Out de 2018.

Para Laysmara Edoardo, "a legislação brasileira para internet é uma das mais progressistas do mundo, uma vez que garante direitos invioláveis para acesso, neutralidade e comunicação".[27]

Surge, então, o Projeto de Lei Complementar nº 53, que busca alterar alguns artigos da Lei nº12.965, e também criar normas gerais de proteção de dados pessoais. Essa regulamentação altera o Marco Civil da Internet e aparece em uma época propícia, marcada por enormes vazamentos de informações e polêmicas que envolvem justamente o uso indevido de informações pessoais.

5.1.1. Lei Geral de Proteção de Dados

Senado aprovou no dia 10 de julho de 2018 a Lei Complementar 53/18, da Câmara dos Deputados, que regulamenta o uso, a proteção e a transferência de dados pessoais, ficando conhecida como "marco legal de proteção, uso e tratamento" de informações. O texto legal foi aprovado pela Câmara e não foi modificado pelos senadores; a proposta altera o Marco Civil da Internet, visando garantir aos cidadãos maior controle sobre suas informações pessoais e foi inspirada na regulação europeia.

Sem uma legislação específica, o Brasil se isolaria, podendo ter problemas ao precisar compartilhar dados de segurança ou realizar transações comerciais que envolvam dados pessoais com países que possuam legislação mais avançada.

A LGPD conceitua dado pessoal como informação relacionada à pessoa natural identificada ou identificável; dado sensível como aquele que pode ser usado para causar dano ao titular, como dados sobre raça/etnia, religião, sexualidade, opinião política, dados genéticos e biométricos; e dado anonimizado como dados pessoais relativos a um titular que não possa ser identificado.

Com a nova regulamentação será necessário o consentimento explícito dos usuários para a coleta e uso dos dados, tanto pela iniciativa privada como pelo poder público, sendo necessária também a existência de opções para o usuário visualizar, corrigir e excluir esses dados.

A nova legislação possui uma proteção especial para crianças e adolescentes, garantindo, em seu artigo 14, que o tratamento de dados pessoais desses deva ser realizado em seu melhor interesse, sendo necessário conhecimento específico por pelo menos um dos pais ou responsáveis legais para a coleta e tratamento de dados de crianças de até 12 anos e repassá-los a terceiros requer uma nova autorização.

Dispõe também sobre os contratos de adesão, nos quais o titular deverá ser claramente informado quando o tratamento de dados pessoais for condição para

27 EDOARDO, Laysmara Carneiro. Legislação para Internet e Combate aos Ciber Crimes: Um Diálogo Criptografado. In Revista Estudos Legislativos. Porto Alegre, ano 10, n. 10, 2016, p. 207.

o fornecimento de produto ou serviço. Com excessão dos dados tornados manifestamente públicos pelo titular, para ter acesso e usar um dado pessoal, uma empresa ou órgão público precisa ter o consentimento do titular. Uma alteração que chama a atenção é o fato de que depois de atingida a finalidade da coleta do dado pessoal, ele deve ser excluído pelo responsável que não tenha obrigação legal de mantê-lo ou para fins de estudo. No quesito territorialidade, fica definido que a lei será aplicável mesmo a empresas com sede no exterior, desde que a operação de tratamento de dados seja realizada no território brasileiro.

Um novo direito concedido aos cidadãos é o de pedir revisão humana dos seus dados mantidos por empresas ou órgãos públicos em casos de decisões automatizadas, como recusa de crédito por um banco, por exemplo. A nova legislação cobra que órgãos públicos organizem dados de forma "estruturada", para que sejam mais acessíveis. É necessário também que seja feita uma indicação de quem é a pessoa responsável pelo tratamento dos dados pessoais de terceiros para que as reclamações e pedidos sejam enviadas a este representante e, havendo uma falha na segurança que comprometa os dados pessoais que estava sob responsabilidade da empresa ou órgão público, o órgão competente deverá ser notificado. Violações a lei podem acarretar multa de ate 2% do faturamento ou suspensão das atividades com dados pessoais alheios por seis meses.

5.2. Legislação comparada

A nova Lei de Geral de Proteção de Dados brasileira é totalmente inspirada na Regulamento Geral sobre a Proteção de Dados da União Europeia, que entrou em vigor em 25 de maio de 2018, passando a existir um conjunto único de regras de proteção de dados para todas as empresas ativas na UE, independentemente da sua localização, incentivando com isso a aprovação do projeto lei nº53 brasileiro, que a ela tanto se assemelha.

5.2.1. Nova Lei de Proteção de dados da União Europeia

A Regulamentação Geral de Proteção de Dados, que ficou conhecida pela sigla GDPR, oferecerá mais poder aos usuários sobre quais das suas informações pessoais serão coletadas ou compartilhadas pelas empresas. As novas regras devem ser seguidas em todos os países membros da União Europeia e também no Reino Unido. Previsto desde 1995, o GDPR foi proposto em 2012, e aprovado apenas em 2016 pela comunidade europeia, que deu dois anos de prazo para os setores público e privado se ajustarem às novas exigências.

Com as novas regras, os cidadãos passam a ter muito mais poder sobre seus próprios dados, e a empresa precisará especificar de forma clara sobre o uso que pretende dar a qualquer tipo de dado, antes de os coletar e armazenar. Se a

finalidade do serviço prestado não "bater" com todos os tipos de dados pedidos pela empresa, ela terá que reduzir a lista de exigências e só solicitar aquilo que for essencial para sua atividade. O GDPR permite ao usuário pedir acesso a todo o banco de informações que uma empresa detém sobre si, podendo solicitar alterações e até a exclusão de tudo.

Com a nova lei, empresas que sofrerem qualquer tipo de vulnerabilidade na segurança, resultando na exposição de dados pessoais armazenados por ela, devem notificar os usuários e a autoridade nacional em menos de 72h, sendo dispensável em casos de vazamentos que não coloquem em risco os direitos e a liberdade das pessoas envolvidas. O desrespeito de qualquer regra imposta pela lei poderá gerar multas milionárias.

6. CONCLUSÃO

Percebe-se, portanto, que o surgimento das redes sociais foi responsável por diversos avanços, facilitando o encontro de pessoas e possibilitando discussões de todos os ramos. Todavia, com a sua criação também surgiu um novo espaço para as mentes criminosas aprimorarem os seus crimes, ampliando o seu alcance de vítimas.

Na fragilidade dos usuários, criminosos encontram espaço para a prática dos seus delitos. Qualquer pessoa esta apta a conhecer a vida daqueles que postam frequentemente nas redes sociais as suas rotinas, devido à hiperconectividade; com isso, ficam habilitados a se passar por conhecidos e obter a confiança das suas vítimas.

Por essa razão há uma necessidade de imediata educação na internet. Torna-se cada vez mais necessário um alerta à população que usa frequentemente as redes sociais, possibilitando a aprendizagem sobre proteção na internet, para que se possa fazer postagens mais seguras, não se expondo abertamente. Essa educação deve se iniciar na escola; os jovens estão entre os que mais se expõem online, mas não deve parar por aí; há necessidade de reforço na sociedade, por meio de campanhas de conscientização.

Vale ressaltar, ainda, a exposição que ocorre com o ingresso nas redes sociais, que exige de imediato a entrega de inúmeros dados pessoais para o simples acesso. Ademais, destaca-se a necessidade da leitura dos termos de uso das redes sociais para que as pessoas tenham consciência dos dados que estão disponibilizando para o público.

Pode-se concluir, portanto, que os ataques cibernéticos estão cada vez mais personalizados e individualizados; as vítimas são estudadas e atacadas no momento mais oportuno, e esses ataques não ficam só no campo virtual, se exte-

riorizam, podendo ocasionar até mesmo lesões à integridade física dos usuários. O maior problema jurídico dos crimes virtuais é a raridade das denúncias, e, pior, o despreparo da polícia investigativa e de perícia para apurá-las.

Os crimes atuais já estão personalizados e em constante expansão com a hiperconectividade e as redes sociais, o que, somado à falta de educação digital e de capacitação dos agentes públicos de persecução, está criando um ambiente propício ao combate ainda mais dificultado, diante de novas técnicas presentes e futuras de golpes.

A nova Lei de Proteção de Dados tem a intenção de promover a segurança dos usuários e chamar atenção para programas e redes sociais que se aproveitam deles, mas não basta a lei se não houver a sua efetiva fiscalização e o seu cumprimento. O ponto chave do presente artigo é provocar um alerta para as todas as gerações de usuários dos riscos aos quais estão sendo expostos diariamente na rede, e sobre os cuidados que devem possuir para que não se tornem vítimas tão frágeis.

Com o cenário atual de uma sociedade cada vez mais digital não há como fugir da necessidade de orientar e educar os jovens quanto às condutas no ambiente virtual. Deve-se ensinar a busca pelo zelo para tentar alcançar a segurança digital , sem deixar de agir de forma ética, a fim de criar bons cidadãos digitais. A educação digital precisa ser promovida simultaneamente à inclusão digital dos usuários, seja da nova geração que já nasceu nessa nova era ou ou daqueles que só tiveram o primeiro contato com as máquinas no ambiente de trabalho.

Pais e escolas precisam orientar seus filhos e alunos sobre a educação digital, já não basta mais apenas ensinar a não aceitar doces de estranhos, hoje não se deve também abrir e-mail de estranhos. Esse comportamento seguro e ético na rede necessita ser ensinado desde cedo, para ser reproduzido no futuro quando essa nova geração crescer.

Uma formação precoce do cidadão digital é de suma importância para o bom uso e a segurança dos meios eletrônicos existentes. A educação desde cedo é um investimento seguro e muito rentável, pensando no futuro e nos novos profissionais que terão no mercado.

Conclui-se, portanto, que apesar da nova lei, para que ela cumpra a sua finalidade é necessário uma educação da população sobre os cuidados que devem ser adotados na rede, principalmente para as novas gerações, que já nasceram dentro desse ambiente cibernético e, por conta disso, têm uma falsa sensação de proteção e segurança na rede. Há que se ressaltar, também, a personalização e expansão dos crimes atuais e como, no futuro, não muito longe, eles estarão ainda mais individualizados e perigosos ante a falta de conhecimento.

REFERÊNCIAS

ALMEIDA, Guilherme Alberto Almeida de. Democracia 3.0 – Desafios na utilização de tecnologias da informação para uma gestão pública eficiente e participativa. Pg. 262- 293. Disponível em: <http://www.abre.ai/guitecpp> Acesso em: 12 de Out de 2018.

BAKER, Stephen apud PINHEIRO, Patricia Peck. Direito Digital. Ed. Saraiva Jur, 6ª ed. revista ampliada e atualizada, 2017.

BRASIL. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm> Acesso em: 29 de Out. de 2018.

BRASIL. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm> Acesso em: 29 de Out. de 2018.

CASTRO, Raisa. Redes Sociais e a sua contínua evolução. Petcomofam. Jun/2013. Disponível em: <http://petcomufam.com.br/2013/06/redes-redes-sociais-e-sua-continua-evolucao.html> Acesso em: 19 de Abril de 2018.

DIMANTAS, Hernani. Tese **As Zonas de Colaboração.** Tese de Doutorado. Universidade de São Paulo, Escola de Comunicação e Artes, 2010. Disponível em:<http://www.teses.usp.br/teses/disponiveis/27/27154/tde-17022011-1224000/…/679860.pdf>.

EDOARDO, Laysmara Carneiro. Legislação para Internet e Combate aos Ciber Crimes: Um Diálogo Criptografado. In Revista Estudos Legislativos. Porto Alegre, ano 10, n. 10, 2016.

FERREIRA, Robson. **Privacidade de Dados no Âmbito da Rede Mundial de Comunicações e seus Reflexos no Direito Brasieiro**. 2004. Dissertação (Mestrado em Direitos Fundamentais) – Faculdade de Direito, Centro Universitário FIEO, Osasco/SP.

GONÇALVES, Pedro Vilela Resende. Marco Civil da Internet. Disponível em: <http://irisbh.com.br/marco- civil-da-internet/>. Acesso em: 20 de maio de 2016.

GOUVÊA, Sandra. O Direito na Era Digital. Rio de Janeiro: Mauad. 1997.

NOGUEIRA, Josicleido. O que são Redes Sociais? Administradores. Jun/2010. Disponível em:<http://www.administradores.com.br/artigos/tecnologia/o-que-sao-redes-sociais/45628>. . Acesso em: 19 de Abril de 2018.

PINHEIRO, Patricia Peck. Direito Digital. São Paulo. Saraiva. Jur, 6ª ed. revista ampliada e atualizada, 2017.

RESK, Felipe. Cerca eletrônica da polícia na internet ajuda a resolver crimes. O Estado de São Paulo. São Paulo, 25 nov. 2018. Disponível em: https://sao-paulo.estadao.com.br/noticias/geral,cerca-eletronica-da-policia-na-internet-ajuda-a-resolver-crimes,70002599616..

SÃO PAULO (Estado). Portaria DGP n. 1, de 4 de fevereiro de 2000: Disciplina a recepção e o registro de ocorrências.

3

A MIGRAÇÃO DOS CRIMES PATRIMONIAIS PARA A INTERNET, ANTE A CONSOLIDAÇÃO DO MERCADO PARALELO NA VENDA DE *MALWARES* E VULNERABILIDADES *ZERO-DAY* NA *DEEP WEB*

Filipe Hamilton Zani[1]
e Leandro dos Anjos Figueiredo de Lima[2]

Resumo: O presente trabalho diz respeito à busca pela conceituação legal e técnico-informática dos mecanismos de invasão computacionais, tal qual *malwares* e vulnerabilidades *zero-day*, frente ao avanço da criminalidade em um ambiente deveras propício ao seu desenvolvimento, conhecido por *Deep Web*. Diante desse cenário, foi constatado o expressivo crescimento do denominado mercado paralelo da *Deep Web*, no que diz respeito a vendas dos mecanismos de invasão computacionais, promovendo uma especialização dos criminosos que agem em especial através da realização de crimes patrimoniais, bem como das organizações criminosas, favorecendo, por conseguinte, a migração e crescimento da criminalidade nos meios digitais. Para tanto buscou-se abordar meios de combate a esse fenômeno, bem como pontuar as dificuldades atuais e os problemas futuros que surgirão dessa relação. De modo que se chegou à conclusão de que medidas devem ser adotadas para buscar refrear o avanço da criminalidade nos meios digitais, e que essa adoção de medidas passa, em primeiro lugar, pela capacitação, tanto dos operadores do direito e agentes da lei, quanto da população em geral.

---

1 Bacharel em Direito pela Faculdade Baiana de Direito e Gestão.

2 Advogado, pós-graduado em Direito Digital e Compliance, membro da Comissão de Informação, Tecnologia e Direito Digital da OAB/BA, vice-presidente e diretor jurídico do Instituto Baiano de Direito Digital (IBADDC).

Palavras-Chave: Crimes Patrimoniais; Internet; *Malwares*; Zero-Day; *Deep Web*.

SUMÁRIO: 1. INTRODUÇÃO; 2. CRIMES DIGITAIS; 2.1 CONCEITO; 2.2 HISTÓRIA; 2.4 CRIMES DIGITAIS PATRIMONIAIS; 2.4.1 ESTELIONATO; 2.4.2 FURTO MEDIANTE FRAUDE ; 2.4.3 ESTELIONATO X FURTO; 3. *MALWARES;* 3.1 CONCEITO; 3.2 TIPOS; 3.2.1 *PHISHING;* 3.2.2 *RANSOMWARE;* 3.2.3 *BOTNET;* 3.2.4 VÍRUS; 4. *DEEP WEB* ; 4.1 CONCEITO; 4.2 HISTÓRIA; 4.2.1 *SILK ROAD;* 5. MERCADO PARALELO; 5.1 ORGANIZAÇÕES CIBERCRIMINOSAS; 5.2 VENDA DE *MALWARES* E VULNERABILIDADES; 6. DIFICULDADES INVESTIGATIVAS ; 6.1 NECESSIDADE DE ORDEM JUDICIAL; 6.2 GUARDA DE *LOGS;* 6.3 INVESTIGAÇÃO DE MATERIAIS COM CONTEÚDOS CRIPTOGRAFADOS OU ESTEGANOGRAFADOS; 6.5 CLOUD COMPUTING; 7. FORMAS DE COMBATE À CIBERCRIMINALIDADE PATRIMONIAL; 7.1. CAPACITAÇÃO E APARELHAMENTO DOS ENTES ESTATAIS; 7.2 DESAPARELHAMENTO DE ORGANIZAÇÕES CRIMINOSAS ATUANTES NA REDE; 7.3 INTEGRAÇÃO DOS ENTES INVESTIGATIVOS; 7.4 COOPERAÇÃO INTERNACIONAL; 7.5 EDUCAÇÃO DIGITAL; 8. PREJUÍZOS CAUSADOS PELOS CRIMES CIBERNÉTICOS PATRIMONIAIS; 9. FUTURO; CONCLUSÃO; REFERÊNCIAS;

1. INTRODUÇÃO

O mundo experimenta enormes mudanças implementadas pelo avanço das tecnologias informáticas e a sua cada vez maior influência em nossas vidas e na vida de nossas sociedades.

Vivemos atualmente o que muitos estudiosos consideram como um "boom tecnológico" em meio à evolução humana. De modo que as pessoas acabaram por ficar mais dependentes das novas tecnologias em todos os setores de suas vidas, seja pelo avanço contínuo dos computadores pessoais ou pela própria migração desses computadores para uma modalidade ainda mais portátil, que são os *smartphones*.

Nesse contexto, e acompanhando a maioria das evoluções tecnológicas, a vida consumerista e econômica das empresas e indivíduos acabou por não ficar de fora. Sendo assim, inúmeros são os artifícios que as empresas de compra e venda de produtos, instituições financeiras e prestadoras de serviços disponibilizam aos seus usuários a fim de se manterem conectados e bem servidos de opções no mundo online.

Dessa maneira, as operações financeiras e operações comerciais, em sua grande maioria, passaram a ser realizadas quase que inteiramente, e em alguns casos inteiramente, pelos meios digitais, que hoje se configuram como o meio de maior alcance e de maior facilidade de acesso para pessoas e empresas.

Ocorre que tudo isso só foi possível a partir da evolução da internet, através de seus navegadores e estruturas ocultas, que veremos mais à frente, de modo que tornou-se possível a utilização da Internet como a principal ferramenta de comunicação e prestação de serviços da humanidade.

Desta forma, com o avanço da Internet, em especial de sua zona mais escondida, a *Deep Web*, foi possível também aos criminosos e demais pessoas à margem da sociedade, aprimorarem e migrarem as suas atuações criminosas, em prol de atingirem esse novo rol de atividades financeiras e vítimas, que hoje executam as suas operações financeiras pelo meio online.

É nesse contexto que esse artigo vem a desvendar a migração das atuações criminosas para esse novo ambiente que é a internet, em especial por meio da chamada *Deep Web*, que possibilita o exercício das atividades criminosas de maneira mais escondida e protegida para criminosos.

Sendo assim, buscar-se-á, através desta obra, entender de que forma esse fenômeno vem ocorrendo e quais as efetivas formas de combate e enfrentamento a essa questão, que devem ser adotadas pela nossa sociedade.

2. CRIMES DIGITAIS

2.1. CONCEITO

Crimes digitais são crimes bastante presentes na vida das pessoas na atualidade, seja no âmbito pessoal quanto no âmbito profissional.

Segundo Cassanti (2014), o crime digital ou cibercrime, como se refere o autor, é toda atividade necessariamente onde um computador ou uma rede de computadores acaba sendo utilizada como ferramenta ou como base de ataque ou como meio de crime.

Ainda conforme o mesmo, são utilizados outros termos para se referir a essa atividade, como: crime informático, crime eletrônico, crime virtual ou crime digital, e aqui acrescentamos mais uma denominação, qual seja, a de crime cibernético.

Já, em conformidade com Barreto; Brasil (2016), temos, ainda, uma nova denominação, a de crime tecnológico que, segundo a visão dos autores, seria gênero do qual os demais são subespécie, e se conceituam como aqueles crimes que envolvem o uso de tecnologias, tais quais computadores, internet e caixas eletrônicos, e se configuram, em regra, como meio, ou seja, de acordo com os autores, nessa modalidade, apenas a forma como são praticados é inovadora.

Segundo, ainda, os autores, essas espécies de crime, apesar de se concretizarem em ambientes virtuais, acabam por trazer efeitos no mundo real.

De acordo com Cassanti (2014), os crimes virtuais não são praticados apenas por pessoas com conhecimento profundo de informática, vez que crimes como ameaça, agressão e ataques preconceituosos, são praticados por usuários na internet todos os dias e têm se tornado uma prática cada vez mais comum.

Ele cita o exemplo da calúnia, que ao poder ser praticada tanto em um jornal quanto na internet é o mesmo crime, mudando apenas o meio de sua realização, pontuando apenas o fator da potencialização dos efeitos pelo meio escolhido, qual seja, a internet.

Neste sentido, segundo Peck (2016, p. 380), "A maioria dos crimes cometidos na rede ocorre também no mundo real", e questões relacionadas à conceituação de crime, delito ato e efeito são as mesmas que são aplicadas ao Direito Penal.

Consoante Cassanti (2014, p. 40), "o maior incentivo aos crimes virtuais é dado pela falsa sensação de que o meio digital é um ambiente sem leis (...)", de modo que, segundo o autor, se faz imprecindível saber que, quando o computador é uma ferramenta para a prática dos delitos, existe a possibilidade de moldar os ilícitos cometidos nos tipos penais já existentes.

Nesse sentido, a internet é um prato cheio para os criminosos, abrindo margem para a prática de crimes em diversas modalidades, bem como sendo fonte de conteúdo para uma infinidade de outros.

Conforme, ainda, Cassanti (2014), crimes virtuais não são praticados apenas por pessoas com sofisticado conhecimento de informática, mas também por pessoas que veem na internet um ambiente propício para extravasar seus sentimentos mais sórdidos, em prol de um falso sentimento de liberdade.

Nesse contexto, os principais crimes cometidos por esses usuários vão desde ameaças até crimes mais sofisticados, como o uso de avançados *malwares* e vulnerabilidades zero-day, como veremos a seguir.

Sendo assim, apontam Barreto, Caselli, Wendt (2017) que os criminosos estão se utilizando de diversas informações dispostas na internet, tais como fóruns, sites pessoais e redes sociais para praticar delitos, acumulando informações através de fotografias da vítima e de parentes, telefones, locais frequentados e hábitos como fontes de informação para obter auxílio no cometimento da prática delitiva.

De forma que a internet se transformou em meio de pesquisa bastante utilizado pelos criminosos para o cometimento de crimes, como através de análise de *check ins* (logins por geolocalização), bem como para a compra e venda de artefatos como *malwares* para o cometimento de crimes dentro da própria internet, ou compra e venda de entorpecentes, armas, bem como serviços ilegais.

2.2. HISTÓRIA

A história dos Crimes Digitais é tão antiga quanto a própria internet; desde os seus primórdios inúmeras foram as tentativas, fazendo-se uso das ferramentas tecnológicas possibilitadas pela rede mundial de computadores, de lucrar, obter vantagens de todos os tipos e de lesar outros usuários.

Nesse contexto temos que, por diversas vezes, a história da cibercriminalidade se confunde com a própria história dos *malwares*, também conhecidos popularmente por vírus de computador que, no entanto, não se confunde por aquele ser gênero do qual este faz parte.

Sendo assim, afirmam Jorge; Wendt (2013, p. 24-25): "No mesmo passo que a revolução dos recursos tecnológicos, as ameaças praticadas via computador se aprimoraram com o passar dos anos."

Conforme os autores, a ideia de vírus de computador (programas de computador autorreplicantes) remonta ao final da década de 50, mais especificamente ao ano de 1949, quando o cientista John von Neumann escreveu seu postulado "Theory and Organization of Complicated Automata" que traz a ideia de como um programa de computador poderia se reproduzir.

Diz-se que, na década de 50, funcionários da empresa americana Bell Labs deram vida a ideia de von Neumann, criando o jogo "Core Wars". Tal jogo consistia no envio de *softwares* "organismos" que competiam pelo controle do computador.

Na década seguinte (década de 60), surgiram os legítimos antecessores dos códigos maliciosos, tendo tudo começado quando um grupo de programadores desenvolveu um jogo chamado *Core Wars*, capaz de se reproduzir cada vez que era executado, sobrecarregando a memória da máquina do outro jogador.

Por fim: "Os inventores desse jogo também criaram o primeiro antivírus, batizado de *Reeper*, com capacidade de destruir as cópias geradas pelo *Core Wars*." (JORGE; WENDT, 2013, p. 24-25)

No entanto, conforme Rankin (2018), é na década de 70 que começam a surgir os primeiros vírus catalogados.

Conforme o autor, ano de 1971 foi em um laboratório de uma empresa que trabalhava com a construção do ARPANET, que um funcionário conhecido como Bob Thomas criou o *software* "*Creeper Virus*" ou "*Creeper Worm*", que se configurou na época como o modelo a ser seguido pelo demais *malwares* do segmento.

De acordo com o mesmo, quando a ARPANET ainda existia, Thomas utilizou esse *software* para copiar sua imagem nos sistemas remotos onde aparecia a mensagem "*Im the creeper, catch me if you can*!"

O *Creeper Virus* consistia em um *software* automultiplicador, e até hoje é considerado o primeiro vírus de computador a ser desenvolvido. Consoante Jorge; Wendt (2013, p. 24-25): "Esse artefato malicioso era um vírus autorreplicante cujo objetivo era infectar computadores DEC PDP-10 que rodavam o sistema operacional TENEX."

Segundo os autores supracitados, no entanto, o vírus teria acidentalmente ganhado acesso à ARPANET e, ao infectar seus usuários, apresentava a mensagem: "im the creeper, catch me if you can!", algo como "eu sou a erva daninha, pegue-me se você puder".

Na década posterior (década de 80), o programador Richard Skrenta, no ano de 1982, um estudante à época, com apenas quinze anos de idade, criou o Elk Cloneria, considerado por muitos até hoje como o primeiro vírus desenvolvido para infectar computadores, apesar de na época ainda não receber esse nome, e de, temporalmente falando, ter supostamente surgido após o *Creeper Virus*.

Esse artefato contaminava o computador Apple DOS 3.3 e se difundia por cópias do disquete contaminado. Consoante Jorge; Wendt (2013), é importante pontuar que esse código malicioso não causava grandes problemas, mas teve grande importância como precursor do conceito.

Ele era um *software* muito pouco nocivo à máquina que, além de apresentar um pequeno "poema", na tela do equipamento infectado, era capaz de gerar cópias de si mesmo quando um disquete era inserido no computador. Possuía, ainda, a capacidade de se dispersar em outro equipamento, quando a mídia era utilizada em outro sistema.

De acordo com os autores, a existência do jogo, seus efeitos e a forma certa de desativá-lo, só vieram a público em 1983, por um artigo escrito por um de seus criadores, publicado em uma conceituada revista científica da época: "Dois anos depois, em 1984, Fred Cohen apresentou um paper, chamado Experiments With Computer Viruses, em que criou o termo "vírus de computador", que denomina programas maliciosos, nocivos ao sistema como um todo." (JORGE; WENDT, 2013, p. 25-27)

Tal qual os autores, ainda na década de oitenta, dois irmãos paquistaneses, no ano de 1986, criaram um vírus de computador chamado *Brain*. Segundo eles, o programa atingia o setor de inicialização do disco da máquina e tinha como finalidade detectar uso não autorizado de um *software* médico de monitoramento cardíaco que haviam desenvolvido. Porém, o código sofreu inúmeras modificações mal intencionadas, as quais o transformaram em um vírus que se espalhava através de disquetes infectados. Desse modo, o vírus denominado Brain causava lentidão nas operações do sistema e ocupava valiosos *kilobytes* de memória dos computadores.

Em 1986 também surgiram os primeiros Cavalos de Tróia de que se tem notícia. Exemplo disso foi o caso do PC Write, que se apresentava como uma versão de demonstração de um processador de textos mas, quando era execu-

tado, apagava e corrompia os arquivos do disco rígido do computador vítima, segundo os autores.

Esse tipo de código evoluiu muito rapidamente, de modo que o primeiro antivírus que se tem notícia foi criado no ano de 1988, por Denny Yanuar Ramdhani, em Bandung, na Indonésia, e tinha como função principal imunizar o sistema do computador contra o vírus denominado Brain.

Conforme os autores:

> Segundo estudo elaborado pela Kaspersky, até 1995 os vírus de boot representavam aproximadamente 70% das ameaças, mas tambem existiam outros, como por exemplo, programas maliciosos que infectavam arquivos executáveis D0821. (JORGE; WENDT, 2013, p. 25 - 27)

Nesse contexto, conforme os autores, com a popularização de outros dispositivos afins utilizados para o acesso à rede mundial de computadores, também surgiram novos meios para a difusão de ameaças. Sendo assim, no ano de 2004, oriundo das Filipinas, surgiu o primeiro vírus de celular. O vírus denominava-se Cabir, e foi criado para infectar aparelhos que utilizavam o sistema operacional Symbian "(hoje, presente em mais de 70% dos celulares)" (JORGE; WENDT, 2013).

Consoante os pesquisadores, o objetivo do Cabir, que se dissemina através da tecnologia *Bluetooth,* é descarregar toda a bateria dos celulares infectados. Em sistemas contaminados pelo referido vírus, uma mensagem característica, com a palavra «Caribe», aparece no visor do aparelho e se repete sempre que o equipamento é ligado.

Segundo BAIO, Ferreira apud JORGE; WENDT (2013), no mesmo ano houve o aprimoramento do vírus por um brasileiro chamado Marcos Velasco, que criou um vírus com código aberto chamado Lasco (também conhecido como Lasco A. ou Symbos_Vlasco.A), vírus de autoinstalação para Symbian, com código aberto e transmitido por *Bluetooth*. Esse vírus também podia ser transmitido pelo computador e descarregava a bateria do celular.

Por fim, conforme Jorge; Wendt (2013), cabe esclarecer que muitos são os marcos de criação dos primeiros vírus de computador, porém, em relação ao assunto, não existe na comunidade científica uma posição pacífica sobre quando surgiu o primeiro vírus de computador, tendo em vista que, para alguns, o primeiro vírus foi o Elk Cloner e, para outros, o Brain.

Igualmente, há muito mistério envolto na criação e utilização desses dispositivos por *hackers* mundo afora, de modo que muitos dos aspectos que englobam a história do surgimento e criação dos vírus não são conhecidos.

2.4. CRIMES DIGITAIS PATRIMONIAIS

Conforme Coêlho (2014, p. 584),

> Patrimônio é um conjunto de bens ou interesses de valor econômico vinculados a um titular, pessoa física ou jurídica." Ainda de acordo com o mesmo: o patrimônio é representado por bens materialmente considerados ou interesses, todos representativos de valor pecuniários.

Nesse sentido, são considerados patrimônios de uma pessoa física ou organização (pessoa jurídica), os seus bens, o seu poderio econômico e as generalidades de seus direitos de importância, no sentido da expressão econômica para seu proprietário. Deste modo, temos que crimes patrimoniais se configuram como ilícitos penais onde, sobremaneira, se configuram como sendo aqueles que vão de encontro ao patrimônio de determinada(s) pessoa(s) ou organização(ões).

Já os crimes digitais patrimoniais vão no mesmo sentido. Com a diferença que este, diferentemente daquele, é realizado, sobremaneira, por intermédio de meios digitais, como a internet, ou contra eles.

Desta forma, os crimes digitais patrimoniais são ilícitos cometidos contra o patrimônio de pessoas ou empresas que atuam na internet, bem como outros meios digitais, ou em prol dela, de maneira a se obter vantagens econômicas indevidas.

Exemplos desses crimes são os crimes de estelionato e furto mediante fraude, tipificados nas condutas de *DNS Spoofing*, quando, por exemplo, o endereço *url* da página de um banco redireciona o usuário para uma outra página, esta falsa, administrada pelos criminosos, que coletam login, senha e outros dispositivos de identificação de segurança do usuário, como forma de, posteriormente à aquisição dos dados, aplicar um golpe no usuário.

Temos, ainda, a conduta criminosa denominada como *phishing*, que se origina do termo "'pescaria", em inglês, e tem por objetivo exatamente "pescar" os dados financeiros da vítima, através da inserção de *malwares* no seu dispositivo informático, de modo a poder, posteriormente, aplicar o golpe junto às instituições financeiras e agências bancárias.

2.4.1. ESTELIONATO

A definição do crime de estelionato se encontra no artigo 171 do Código Penal Brasileiro. De acordo com o caput do artigo: "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento".

Nas palavras de Rogério Sanches Cunha (2014, p. 350), é punido aquele que, através da "astúcia", da "esperteza", do "engodo", da "mentira", busca

separar a vítima do seu patrimônio, fazendo com que esta entregue a coisa almejada espontaneamente, não se utilizando de meios violentos.

Os criminosos sempre estão buscando aprimorar suas habilidades e, como já se viu, a tecnologia serve como um facilitador para o cometimento de crimes, sendo possível o cometimento do crime de estelionato na modalidade eletrônica.

Um exemplo seria o envio de e-mail ou mensagens para a vítima onde, através de engenharia social, é possível obter informações sobre a vida pessoal ou trabalho, para fazer a vítima acreditar no conteúdo da mensagem e, eventualmente, enviar o que foi pedido pelo criminoso.

2.4.2. FURTO MEDIANTE FRAUDE

O crime de furto está previsto no artigo 155 do Código Penal Brasileiro, com a seguinte redação: "subtrair, para si ou para outrem, coisa alheia móvel". Conforme Cunha (2014, p. 263) a conduta, que recebe a punição estatal, é o apoderamento do agente, para si ou para outrem, de coisa alheia móvel, retirando, assim, o bem da vítima. Por coisa alheia móvel deve-se entender aquele bem economicamente apreciável.

O furto mediante fraude (furto fraudulento) está previsto no parágrafo quarto, inciso II, do artigo 155, que traz a qualificadora: "com abuso de confiança, ou mediante fraude escalada ou destreza".

Segundo Damásio de Jesus, a fraude é um meio enganoso hábil a ludibriar a vigilância do ofendido e viabilizar, com maior facilidade, a subtração do objeto material. Para melhor compreensão, o autor traz o exemplo de uma situação em que o praticante do delito se traja de funcionário de uma empresa legítima de companhia telefônica, para poder entrar na casa da vítima e subtrair bens. (JESUS, 2004, p. 327)

Diante do exposto, o furto fraudulento eletrônico vai apresentar características semelhantes a sua modalidade no plano fático; a diferença é a utilização do meio eletrônico. Um exemplo para compreender essa modalidade criminosa é a utilização da técnica do *phishing* (que será melhor analisada adiante), onde a vítima, acreditando estar acessando um site legítimo, como um site de um banco, coloca seus dados pessoais e financeiros nos campos da página fraudulenta. A consequência disso é o envio dessas informações para o criminoso, que poderá usá-las de diversas formas.

2.4.3. ESTELIONATO X FURTO MEDIANTE FRAUDE

Ainda que muito semelhantes, os dois tipos não podem ser confundidos, pois existem diferenças essenciais. No estelionato, a fraude tem o objetivo de

fazer com que a vítima incida em erro, entregando o objeto espontaneamente ao criminoso. No furto mediante fraude, o agente visa reduzir a vigilância da vítima para poder realizar a subtração, de modo que o bem é retirado sem que a vítima perceba o dano a seu patrimônio. Nesse sentido, existe no furto mediante fraude uma vontade apenas unilateral (apenas o criminoso deseja), enquanto no estelionato, essa vontade é bilateral (vítima e agente desejam). (CUNHA, 2014, p. 275)

3. *MALWARE*

Diante das facilidades oferecidas pela internet, está ocorrendo cada vez mais a migração dos crimes patrimoniais para o ambiente em rede, bem como a utilização cada vez maior de *malware*s por pessoas comuns para atingir finalidades ilícitas.

Nos Estados Unidos, o FBI criou, no ano de 2000, o IC3 (Internet Crime Complaint Center), visando receber denúncias de crimes virtuais. Segundo o relatório deste centro de denúncias, desde sua criação, já foram recebidas mais de 4.000.000 de notícias sobre crimes cibernéticos das mais variadas formas. Somente entre 2013 e 2017 foram, aproximadamente, 1.400.000 notícias de crimes ocorridas em ambiente virtual, o que demonstra uma crescente evolução, tanto na frequência destes crimes, quanto no percentual de encaminhamento de notícias. (IC3, 2017, p. 4)

No Brasil já é comum a ocorrência de crimes virtuais e esses estão ficando cada vez mais usuais no dia a dia do brasileiro. Não é errado afirmar que na sociedade tupiniquim houve uma inclusão digital dos indivíduos desassociada de uma educação digital, o que possivelmente acarreta o índice crescente de crimes cibernéticos percebidos dentro do país, já que os usuários não possuem o conhecimento necessário e, justamente por esse desconhecimento, se tornam vítimas.

Segundo o Internet Crime Report de 2017 (2017, p.18), produzido pelo IC3, o Brasil consta no 7º lugar do *ranking* de países por envio de notícias de crime, totalizando o número de 558 *reports*. Pela tendência concreta de crescimento desse tipo de crime, são necessários instrumentos eficientes e adequados para que a realidade brasileira esteja adaptada a esse novo contexto que está surgindo.

Nesse sentido, é necessário que o leitor tenha conhecimento das consequências de um uso irresponsável da rede mundial de computadores, onde a desatenção e o despreparo podem ocasionar danos irreversíveis, e que podem ser prevenidos primariamente com bons hábitos de uso da Internet, juntamente com a utilização de antivírus e *firewalls* seguros e atualizados.

3.1. CONCEITO

A palavra *malware* está etimologicamente relacionada à expressão *malicious software*. Nesse sentido, um *malware* é um *software* malicioso, que tem como objetivo ocasionar danos no sistema informático ou roubar informações de um alvo.

Segundo Lima (2016), eles se configuram como *softwares* criados com a função de causar danos. Ainda que se utilizem de diferentes classificações, os *malwares* têm atuações múltiplas conforme sua especialidade. A depender de sua espécie, irá ter uma diferente operacionalização. As diferentes especialidades serão vistas no tópico abaixo.

3.2. TIPOS

Existem diferentes tipos de *malware*, cada uma com uma diferente forma de atuação. *Malware* é um gênero do qual deriva diversas outras espécies. Os *malwares* vistos a seguir são os principais e mais comuns, exemplificativos e não taxativos, tendo em vista que todos os dias novos *malwares* são desenvolvidos com diferentes variações, já que os cibercriminosos estão constantemente aprimorando as suas habilidades em buscas de *malwares* mais eficientes.

3.2.1. PHISHING

Conforme menciona Rankin (2018), CMO da empresa de cibersegurança *Lastline*, tecnicamente, o *phishing* não é um tipo específico de *malware*. Segundo o autor, está mais associado a uma conduta criminosa que distribui *softwares* maliciosos.

De forma resumida, o ataque *phishing* faz com que o usuário clique em um *URL* "infectado", criado especificamente para obter informações pessoais do indivíduo. Nesse sentido, o indivíduo que acessa o link malicioso está acreditando que está visitando o site original, entregando, assim, suas informações bancárias e pessoais para o criminoso.

O principal exemplo de *phishing* são e-mails enviados se passando por bancos, solicitando informações sobre pagamentos, dados financeiros ou cadastrais. Por isso é importante que o usuário fique sempre atento a este tipo de e-mail, já que instituições financeiras dificilmente (para não dizer nunca) buscam fazer contato através deste método.

Conforme menciona Lima (2016, p. 86), com a diminuição do uso dos e-mails (até então principal método de envio de *phishing*) e com o aperfeiçoamento da filtragem anti-*phishing* utilizada pelos melhores provedores de cor-

reio eletrônico, os criminosos têm direcionado suas condutas para o lançamento de informações falsas em anúncios de redes sociais como Facebook e Twitter.

3.2.2. RANSOMWARE

O *ransomware* é uma espécie de *malware* que impede que os usuários acessem os seus sistemas informáticos ou documentos pessoais, exigindo um pagamento para que o usuário volte a ter acesso às suas informações.

Conforme menciona Robert Richardson (2017), as informações do computador da vítima são "trancadas" por criptografia, e o pagamento geralmente é feito por criptomoedas, a exemplo do *bitcoin*, para proteger a identidade do cibercriminoso.

Há diversos vetores de *ransomware* que podem permitir o acesso ao computador. Segundo Josh Fruhlinger (2017), o mais comum é o *phishing spam* (anexos dentro de um email enviado à vítima que, quando baixados e abertos, podem infectar o seu computador).

O *malware* pode atuar no computador do usuário vitimado de várias formas, porém a conduta mais comum é a encriptação dos dados, bloqueando o acesso a esses. Deste modo, os arquivos somente podem ser descriptografados com uma chave matemática que somente o cibercriminoso tem conhecimento. Geralmente, o *layout* exposto pelo *malware* contém as instruções para que seja feito o pagamento e liberado o acesso aos dados. (FRUHLINGER, 2017)

De acordo com Richardson (2017), existem diferentes maneiras de o cibercriminoso realizar sua aproximação e extorquir as vítimas de modo a obter criptomoedas. A mais comum é a mensagem do *ransomware* mencionando, informando que se o pagamento não for feito dentro do prazo estabelecido, todas as informações criptografadas serão destruídas. Outro modo é quando o *ransom* se passa por órgão investigativo oficial. Nesse sentido, quando é detectado que o alvo utiliza alguma licença ilegal de *software*, ou possui conteúdo impróprio no seu computador, aparece o aviso do *ransom* como se fosse uma autoridade policial solicitando o pagamento de uma "multa eletrônica".

Existe uma variação do *ransomware* chamada *leakware* ou *doxware*, onde o cibercriminoso ameaça publicar informações sensíveis armazenadas no computador da vítima, exigindo o pagamento do *ransom* para a não divulgação. (FRUHLINGER, 2017)

Em um mundo cada vez mais conectado, escolas, hospitais, empresas e qualquer residência com computador e acesso a internet são potenciais alvos de *ransomware*. Os ataques deste tipo de *malware* estão ficando cada vez mais sofisticados, tendo em vista o aprimoramento de seus métodos pelos cibercri-

minosos com o passar dos anos, sendo necessário que a sociedade esteja atenta a essas mudanças para que haja a prevenção em relação a esse tipo de ameaça.

3.2.3. BOTNET ou BOTS

De acordo com Rankin (2017), *Botnet* ou *Bots* são *softwares* maliciosos criados para infiltrar computadores, sendo previamente instruídos de suas ações e respondem automaticamente aos direcionamentos dados pelo cibercriminoso. Os *bots* podem se autorreplicar (como os *worms*) ou se replicar pela ação do usuário (como vírus e trojans).

Segundo Chris Hoffman (2016), "*bot*" vem da palavra "r*obot*". Ao infectar determinada máquina, o *bot* faz contato com o servidor remoto responsável pelo seu controle, onde irá aguardar instruções ou praticar comandos que foram previamente determinados. Um cibercriminoso isoladamente pode comandar um alto número de *bots*.

O que faz o computador fazer parte de uma *botnet*, é o fato de ser controlado remotamente por um outro computador. Assim, é possível que um computador infectado por *bots,* seja alvo de outros ataques comandados. Por exemplo, o cibercriminoso pode ordenar que os *bots* façam downloads de outros *malwares*, a exemplo do *ransomware* ou do trojan, aumentando o nível de ameaça.

Os *bots* podem ter diferentes propósitos, já que permitem que centenas de milhares de computadores atuem conjuntamente para atingir um objetivo comum. Assim, o uso de *bots* torna possível um ataque DDoS (*Distributed Denial of Service*), que consiste em um bombardeio de acessos de um determinado *Website*, congestionando o tráfego de dados e deixando o site inacessível. (HOFFMAN, 2016)

Outro exemplo é a possibilidade de distribuição de *malware*. Assim, o cibercriminoso pode dar um comando para o *bot* fazer o download de um *keylogger*, de modo a obter as senhas da vítima, bem como fazer o download de um *ransomware* e criptografar as informações do usuário.

3.2.4. VÍRUS

De forma breve, o vírus pode ser resumido como um programa malicioso, dentro do computador do usuário, que age sem o seu conhecimento, praticando atos danosos, a exemplo da destruição de informações e de arquivos sensíveis do computador.

Depois que o vírus entra no computador ele se anexa a algum outro programa, de modo que, quando for iniciada a execução deste programa hospedeiro, também ativará a ação do vírus de forma simultânea.

Segundo Danilo Amoroso (2008), a característica peculiar do vírus é a possibilidade de infectar um determinado sistema, se autorreplicar e tentar espalhar-se por outros computadores. Vale ressaltar que nem todo vírus é destrutivo, porém a grande maioria foi criado com esse propósito de causar danos.

Ainda segundo o autor, um dos vírus mais perigosos que já existiu foi o denominado "ILOVEYOU", uma carta de amor que foi espalhada por e-mail. Atribui-se a este *malware* a responsabilidade pela perda de mais de 5 bilhões de dólares em diversas empresas. (AMOROSO, 2008)

Conforme menciona Guilherme Tagiaroli (2010), este vírus vinha por e-mail com um anexo nomeado "*Love-letter-for-you*" que, após a sua execução, enviava o mesmo anexo para todos os contatos cadastrados da pessoa. Citando entrevista com Craig Schumugar, pesquisador de ameaças da McAfee Labs, o mesmo vírus sobrescrevia alguns arquivos e contaminava outros, além de ser ativado toda vez que o usuário tentasse abrir um arquivo MP3.

Instituições como o Pentágono e a CIA tiveram seus sistemas de e-mail paralisados devido ao alto fluxo de mensagens que congestionou o tráfego da rede. Este *malware* infectou apenas sistemas operacionais Windows. (TAGIAROLI, 2010)

3.2.5. TROJAN

Conforme entendimento de Bert Renkin (2018), o Trojan é um programa malicioso camuflado de um *software* confiável. Os cibercriminosos estão diariamente aprimorando os seus métodos de modo a fazer com que o indivíduo instale o *malware* em seu computador.

O termo faz referência à história da Grécia antiga, onde foi utilizado um cavalo de madeira como um presente aos Troianos. Porém, o cavalo estava repleto de soldados e foi uma maneira de fazer uma infiltração silenciosa. (RANKIN, 2018)

De acordo com Hopping e McCallion (2018), quando o programa é baixado e instalado no computador, o vírus se estabelece no sistema hospedeiro e inicia o seu trabalho malicioso. Nesse sentido, ele vai registrar toda a atividade do usuário, inclusive todas as teclas que foram digitadas, viabilizando a invasão do computador e permitindo o acesso de *hackers* que podem roubar informações pessoais, acessar o computador remotamente, destruir ou encriptar dados.

Ainda em consonância com os autores, existem algumas categorias de trojan. Os "*backdoors trojans*" são aqueles que, uma vez baixados e executados, vão permitir aos *hackers* o acesso remoto do computador, possibilitando a visualização de todas as informações do sistema. (HOPPING; MCCALLION, 2018)

Os "*downloaders trojans*" funcionam como uma ponte para a entrada de outros *malwares*. Quando baixados e instalados, começam a fazer o download de outros programas maliciosos, a exemplo de *keyloggers*, *cryptojackers* e *ransomwares*. (HOPPING; MCCALLION, 2018)

"*Banking trojans*" têm como alvo especificamente as informações e transações financeiras. Quando baixados, fazem buscas nos cookies para obter informações relacionadas a serviços financeiros, que ficam armazenados no computador quando o usuário acessa sua conta no site do banco por exemplo. Com esses dados, o trojan vai redirecionar o usuário do site do banco legítimo para um site scam, visando roubar suas informações financeiras. Os mais famosos entre os hackers são o Zeus, o Dridex e o Kronos, que estão menos efetivos devido às melhorias de segurança realizadas pelas instituições financeiras. (HOPPING; MCCALLION, 2018)

3.2.6. CRYPTOJACKING

Conforme definição dada por Ray Li (2017), engenheiro de *software* e editor do site *Hackerbits*, o *cryptojackin*g é o uso clandestino de um dispositivo informático para a mineração de criptomoeda. Pode ocorrer de duas formas: a primeira é quando algum arquivo malicioso é instalado no sistema e começa a mineração secretamente, enquanto a segunda decorre simplesmente de acessar um determinado site pelo *browser*.

A primeira maneira é a mais tradicional, quando um *malware* tem um comando específico de minerar criptomoedas através do sistema infectado. A segunda, se utiliza do *JavaScript* do site o qual está sendo realizado o acesso, para minerar criptomoeda.

Essa segunda maneira, conhecida como "i*n-browser cryptojacking*" apresentou alto crescimento no primeiro semestre de 2018, superando, inclusive, o percentual de ocorrência dos *ransomwares*, conforme relatório da Malwarebytes Labs (2018).

O *cryptojacking* realizado no navegador ou nos dispositivos móveis ocorrem secretamente e sem o consentimento do indivíduo. Com o passar do tempo, o valor de criptomoeda que foi minerado é enviado para a carteira do criminoso, sendo extremamente difícil de rastrear.

Por essas características, é fácil compreender o motivo da ascensão desta forma de ataque. O *in-browser cryptojacking* é menos invasivo e apresenta uma maior lucratividade quando comparado ao *ransomware*, que exige uma abordagem mais refinada, havendo, ainda, o risco de a vítima, simplesmente, se recusar a pagar o resgate das informações criptografadas.

4. *DEEP WEB*

A *Deep Web* é a parcela da internet que não foi indexada pelos buscadores convencionais (a exemplo do Google, Yahoo e Bing). Essa outra face da internet possui uma grande quantidade de informações que, geralmente, só são acessíveis com o uso de recursos específicos, a exemplo do navegador «TOR», que possui o símbolo de uma cebola, fazendo referência a sua constituição em camadas. (PINHEIRO, 2016, p. 406)

A internet convencional, ou *surface*, é a parte da rede mundial de computadores usada diariamente pela maioria das pessoas em situações cotidianas, a exemplo da visualização das caixas de entradas de e-mail, acesso a redes sociais, pesquisas em buscadores, dentre outros. Conforme menciona Glaydson de Farias Lima (2016, p. 135), se algum material estiver em ambiente inacessível pelos buscadores convencionais, ele estará na *Deep Web*.

O navegador TOR torna mais difícil que as atividades do usuário sejam detectadas, uma vez que utiliza uma matriz mundial de milhares de servidores que mascaram a origem e o destino da conexão. Sem o TOR, atividades online do usuário se tornam simples de serem detectadas, uma vez que o acesso a sites comuns geralmente revelam a localização do indivíduo. (GOODMAN, 2015, p. 211)

Assim, o TOR se mostra ferramenta importante na proteção da privacidade, uma vez que permite estabelecer conexões de maneira anônima. Nesse sentido, países que vivenciam realidades de censura, a exemplo da China e Irã, têm a *Deep Web* como importante instrumento de comunicação com o restante do mundo.

Segundo especialistas, a Primavera Árabe, série de manifestações e protestos ocorridos no Oriente Médio e no Norte da África no ano de 2011, somente foram possíveis graças à existência de fóruns de discussões privados na *Deep Web,* que viabilizaram a comunicação dos manifestantes sem a interferência do governo. (SOUZA, 2015)

De acordo com estudiosos, a *Deep Web* é aproximadamente quinhentas vezes maior que a *Surface*, utilizada diariamente pela maioria das pessoas. Conforme Goodman (2015, p. 214), na medida em que a *Deep Web* possui em torno de 7.500 terabytes de informação, o conjunto pesquisável pelo Google e outros buscadores da *Surface* são de de 19 terabytes.

Nesse sentido, mencionando um estudo da revista americana *Nature*, o autor relata que uma pesquisa no Google ignora 99% de todos os dados existentes na rede mundial de computadores. Nas palavras do escritor: "uma pesquisa na web equivale a pescar apenas nos 50 centímetros de profundidade dos vastos oceanos do mundo. Embora seja possível pegar algo na rede, estar-se-á perdendo enorme recompensa disponível abaixo desses 50 centímetros".

Partindo da lógica que os criminosos estão sempre um passo à frente das autoridades policiais, a *Deep Web* não é exceção à regra. Dentro desse ambiente, existe uma realidade deturpada, onde livremente ocorre a oferta dos mais diversos crimes. Trata-se da *Dark Net* ou *Dark Web*.

4.1. DARK NET

A *Dark Net* é o nome dado a parte da *Deep Web* onde ocorre a compra e venda de produtos e serviços ilícitos. Devido a essas características, criminosos passaram a se fazer presente nesse ambiente. O exemplo mais popular foi o site *Silk Road*, conhecido como o Ebay das drogas.

Fazendo uma referência à antiga rota de comércio asiática (a rota da seda), o *Silk Road*, de forma resumida, tornou possível a comercialização de todo tipo de material. O site era dividido em diferentes categorias de produtos ilícitos, a exemplo da venda de drogas, armas, remédios controlados, moedas falsas, cartões de créditos roubados, vírus de computador, assassinos de aluguel e até mesmo pornografia infantil. (GOODMAN, 2015, p. 207)

O *Silk Road* tem a fama de ter sido o maior mercado criminoso do mundo, até o seu encerramento em 2013, quando Dread Pirate Roberts (pseudônimo usado por Ross William Ulbricht), dono do site, foi preso em uma operação do FBI. De acordo com Goodman (2015, p. 209), o site contou com mais de 950 mil usuários, possuindo aproximadamente 600 mil mensagens privadas trocadas mensalmente e um sistema sólido de avaliação de reputação on-line, que possibilitava um maior índice de credibilidade para vendedores e compradores.

Vale ressaltar que o *Silk Road* é apenas um exemplo de "supermercado ilícito online", existindo diversos, como o Open Market, Agora, Sheep Marketplace, Atlantis, dentre outros. Vários sites semelhantes são criados e apagados diariamente.

A *Dark Net* utiliza criptografia e meios *peer-to-peer* (P2P) de retransmissão criados com o propósito de esconder endereços IP dos usuários, criando uma rede anônima, irrastreável e segura para que os cibercriminosos possam realizar suas operações sem interferência do Estado ou de outras organizações. (GOODMAN, 2015, p. 215)

Assim, a *Deep Web* é um ambiente anárquico, e quem resolve desbravar o seu conteúdo está sujeito a ver diversas barbaridades; ainda que sirva como importante instrumento de interlocução para países que vivenciam realidades antidemocráticas e de censura, permitindo comunicação sem interferências governamentais, a *deep web* também favorece a atividade cibercriminosa. Se em meados de 2012 existia o *Silk Road*, até então o maior *marketplace* de produ-

tos ilícitos, hoje em dia existem diversos outros domínios ocultos, bem como diversos sites de vendedores individuais que ofertam seus produtos para quem queira comprá-los.

Nesse sentido, o indivíduo, com o conhecimento mínimo de como navegar na *deep web*, poderá encontrar, sem maiores problemas, sites de vendas de drogas, moedas falsas, armas, explosivos, documentos, contas bancárias, cartões de crédito, dentre outros.

5. MERCADO PARALELO

Como visto, a *deep web* permitiu a consolidação do mercado paralelo online, de modo que se tornou possível a aquisição de uma variedade de bens, lícitos e ilícitos.

É normal que em um novo mercado em ascensão, os indivíduos direcionem suas energias e estratégias para ingressar neste meio, de modo a poder extrair todas as vantagens de um mercado pouco explorado. Assim, é possível encontrar tanto na *surface* quanto na *deep web*, organizações cibercriminosas especializadas em "antissegurança", responsáveis pela venda de *malwares* e de *exploits kits* para vulnerabilidades *0-day*, visando indivíduos que desejem adquiri-las.

Diante de tal situação, existe um atual movimento de migração dos crimes patrimoniais e dos criminosos para o ambiente em rede, permitindo que até mesmo indivíduos sem conhecimento prévio em informática possam adquirir esses *softwares* e utilizá-los. Mais à frente será visto como está ocorrendo essa nova prática.

É possível dizer também que houve uma profissionalização do *hacking*. Sites e programas em sua grande maioria possuem vulnerabilidades, e os responsáveis por estas aplicações contratam hackers para detectar estas vulnerabilidades em seus sistemas. Neste cenário, constatou-se também o aumento no número de venda dessas vulnerabilidades no mercado paralelo, oferecendo a falha de segurança em troca de um pagamento.

Os mundos *offline* e *online* estão se juntando cada vez mais, ocasionando o cruzamento dos fluxos criminosos. Segundo Marc Goodman (2015, p. 186), a sociedade já se encontra na era dos crimes cibernéticos. O autor menciona que a tecnologia insere um nível maior de eficácia no crime e, assim, os criminosos são os primeiros a adotarem os mais variados tipos de tecnologia.

5.1. ORGANIZAÇÕES CIBERCRIMINOSAS

Os criminosos estão renunciando as antigas estruturas hierárquicas e se adaptando cada vez mais às organizações empresariais modernas. Grupos de

criminosos considerados tradicionais, como a Yakuza japonesa, as Tríades chinesas, a Cosa Nostra italiana, criaram divisões cibercriminosas para desbravar a criminalidade em um mundo cada vez mais globalizado. Nas palavras do autor: "o crime cibernético não tem fronteiras, oferece grande anonimato, e os processos criminais são extremamente raros, talvez ocorrendo em menos de um milésimo de 1% de todos os casos". (GOODMAN, 2015, p.186)

Somado a isso, houve a profissionalização dos próprios *hackers*. Antigamente, por volta de 1980, os *hackers,* em sua maioria, apenas manipulavam sistemas de computadores por curiosidade ou para provar sua perícia técnica. Atualmente, o *hacking* é um negócio altamente rentável, pois houve a percepção pelo criminoso que era possível ganhar dinheiro com a corrupção da tecnologia, acessando sistemas informáticos de outras pessoas. (GOODMAN, 2015, p. 187)

Diante desse cenário, as organizações criminosas estão estruturalmente cada vez mais semelhantes a organizações empresariais, havendo divisão de trabalhos, gestão de suprimentos, chefes de setores e serviços, consultores, dentre outros.

O organograma de uma organização criminosa apresenta funções como CEO (Chief Executive Officer), CIO (Chief Information Officer), programadores, engenheiros, desenvolvedores, diretores, gestão de qualidade, suporte técnico e outros cargos diversos. (GOODMAN, 2015, p. 190)

Um CEO de uma organização criminosa é o indivíduo responsável pela tomada de decisões e pela supervisão. Como grande parte dos empresários convencionais, o CEO do crime possui o "produto intelectual" da atividade ilícita e o capital necessário para colocá-lo em prática. Comumente é um indivíduo bem relacionado no meio do crime e funciona como um recrutador, que monta a equipe para praticar a atividade. Geralmente não é o indivíduo com o conhecimento específico necessário, mas é o responsável por contratar os indivíduos com habilidades em programação e *hacking* imprescindíveis para realizar a tarefa. (GOODMAN, 2015, p. 190)

O CIO é responsável por manter o funcionamento da infraestrutura informática da organização criminosa. O indivíduo neste cargo tem a atribuição, dentre outras, de cuidar dos servidores "ilocalizáveis" e contratar com serviços de hospedagem duvidosos para garantir que o "*crimeware*" permaneça fora do alcance das agências policiais de todo o mundo. O CIO também é responsável por manter o banco de dados dos "clientes", o exército de *botnets* e cuidar da parte de segurança da informação. Por fim, ocupa-se da criptografia dos dados criminais, garantindo que estejam ilegíveis e não possam ser utilizados pelas forças policiais nem por organizações cibercriminosas concorrentes. (GOODMAN, 2015, p. 191)

A equipe de gestão de qualidade é a responsável por fazer com que os *shells* de criptografia (local onde os *malwares* dos codificadores estão ocultos) sejam eficientes para driblar os sistemas de segurança mais atuais, como antivírus e *firewall*. Os programadores da gestão de qualidade fazem o teste do "*crimeware*", submetendo-o às definições dos antivírus mais populares, para que se possa garantir que *malware* passe despercebido por eles antes de seu lançamento. É necessário observar que os sistemas de detecção são diariamente atualizados de maneira automática. Os responsáveis pela gestão de qualidade podem, ainda, realizar um cadastro para receber notificações se algum de seus *malwares* forem identificados por empresas de cibersegurança, permitindo a alteração da codificação do *malware* para torná-lo oculto novamente. (GOODMAN, 2015, p. 192)

Ainda existe a figura dos afiliados. No mundo on line, o marketing de afiliados é algo muito forte e popular. Segundo Bruno Gomes Dias (2018), constitui-se em uma forma de publicidade digital, onde o afiliado divulga no seu site anúncios de parceiros em troca de um pagamento. O pagamento pode ser estabelecido pela quantidade de cliques, vendas ou por outros tipos de condutas que possam gerar redirecionamento.

As redes de afiliados formam uma espécie de "coluna vertebral" do crime cibernético, e segundo Goodman (2015, p. 193) as melhores estão na Rússia. Os *Partnerkas*, como são chamados, trabalham vinte e quatro horas por dia para fazer o maior número de redirecionamentos possível para os sites de seus clientes cibercriminosos. Esse tipo de criminoso cuida da divulgação do produto, que pode ser desde um antivírus falso, até a venda de pornografia infantil.

Assim, a organização cibercriminosa faz o pagamento aos afiliados de acordo com a quantidade de cliques, quantidade de instalação, quantidade de tráfego gerado para o site indicado ou quando o *malware* objeto da publicidade for baixado no computador da vítima. Conforme indica Goodman (2015, p. 193), ironicamente, os líderes das organizações criminosas avisam aos afiliados em seus sites ilegais que "o uso de *spam* ou outros métodos de infecção são estritamente proibidos". A indústria do crime passou a utilizar termos de serviços e acordos de licença para se resguardar de eventuais alegações de culpabilidade penal perante os "executivos do crime".

Estes foram apenas alguns exemplos de como o modelo de estrutura das organizações empresariais modernas está sendo aplicado nas organizações cibercriminosas. A essência da função continua sendo a mesma nos dois cenários, o que vai mudar é o propósito ao qual se destina a função.

5.2. COMÉRCIO DE *MALWARES* E VULNERABILIDADES

É correto enunciar que a sociedade vive hoje o momento da desmaterialização. Conforme menciona Kevin Kelly (2015, p. 117), cofundador da revista norte-americana de tecnologia *Wired*, "o Uber, maior empresa de taxis do mundo, não tem nenhum veículo. O Facebook, a empresa de mídia mais popular, não cria conteúdo. O Alibaba, varejista mais valioso, não conta com estoque". Como já dito anteriormente, a sociedade passa por um período de mudança, algo novo.

A posse atualmente possui mais relevância que a propriedade. A Netflix, uma das maiores empresas de filmes e series, permite que o indivíduo assista a sua programação sem ter que comprar nada (apenas ter o acesso). O Spotify, de maneira semelhante, viabiliza que o usuário escute uma infinidade de músicas, sem necessidade de comprá-las. Com Playstation Now, é possível jogar uma ampla quantidade de jogos que estão disponíveis no catálogo, sem a necessidade de possuí-los. Com o tempo, o indivíduo está possuindo menos do que ele usa. (KELLY, 2015)

Segundo Kelly (2015, p. 119), "a tecnologia digital acelera a desmaterialização e apressa a migração dos produtos para os serviços". Nesse sentido, o *software* foi um dos primeiros produtos a se tornar serviço, surgindo a modalidade de venda SaaS (*Software as a Service*).

Diversos aplicativos já utilizam essa modalidade de venda SaaS, a exemplo do Adobe Photoshop. Atualmente, não se vende mais esse programa levando em consideração as suas versões (possibilidade de compra de uma versão 7.5 por exemplo). O que ocorre hoje é o pagamento de uma assinatura, geralmente mensal, que proporciona a constante atualização do aplicativo, viabilizando constantes upgrades de melhoria e segurança, sem ter que pagar nada a mais por isso, além da assinatura.

Seguindo a tendência, a criminalidade também se adequou à nova realidade. O *Crime as a Service* (CaaS) é um modelo de negócio que viabiliza que um determinado crime ou partes dele sejam realizados por outras pessoas, mantendo o empreendedor (aquele que investiu e organizou o golpe) afastado do "campo de batalha" e com seu lucro garantido. (GOODMAN, 2015, p. 227)

É possível que a indústria cibercriminosa contrate programadores para desenvolver sites e aplicações. Segundo Goodman (2015, p. 228), as *Crime Enforcers* (trocadilho com "*Law Enforcer*", que em tradução livre seria aplicador da lei) se descrevem como: "organizações privadas para pedidos especiais de desenvolvimento [...] se você necessita de hardwares [...] ou *softwares* especiais que não podem ser criados ou discutidos em seu país [...] oferecemos o

desenvolvimento absolutamente anônimo e *offshore* para os projetos. Não nos importa o que será feito com os *hardwares* ou *softwares* encomendados".

Considerando esse cenário, os criminosos são os primeiros a utilizar as novas formas de tecnologia e de negócios a seu favor. Assim como existe o SaaS e CaaS foi criado também o conceito de RaaS, que significa *Ransomware as a Service*, onde cibercriminosos fornecem todo o suporte necessário para que o indivíduo tenha acesso ao *malware* e possa utilizá-lo de maneira eficaz.

Nesse sentido, todos os dias milhares de aplicativos e programas novos são criados, com constantes *upgrades*. São tantas as atualizações, que o ser humano tem que reaprender todos os dias a usar os *softwares*, tendo em vista o acréscimo constante de novas funções.

Assim, na grande maioria das vezes, quando uma determinada aplicação é lançada ou atualizada, existem vulnerabilidades em seu sistema que não foram percebidas pelo desenvolvedor. Em alguns casos, *hackers* são contratados para detectar essas vulnerabilidades e permitir a correção pelos criadores, sendo uma atividade plenamente lícita quando há a contratação deste serviço.

Porém, o grande problema reside quando *hackers* mal-intencionados (conhecidos como *crackers*) exploram essas vulnerabilidades sem prévia ciência do desenvolvedor ou dono da aplicação. Desse modo, as vulnerabilidades serão utilizadas para fazer chantagem, derrubar o sistema e, inclusive, vendidas para outros indivíduos que podem fazer o que desejarem com essa informação.

5.3. VENDA DE MALWARES PARA LEIGOS EM INFORMÁTICA

A venda dos chamados *kits* de *malwares* não é uma novidade do século XXI. No início dos anos 90, já era possível encontrar na rede algumas ferramentas baseadas no sistema DOS (*Disk Operating System*), a exemplo do VCL (*Virus Creation Laboratory*). Nessa época, o propósito principal destes *kits* era permitir que os "*non techies*", como eram chamados os leigos, pudessem entrar no movimento da contracultura de codificação de *malwares*. Hoje em dia, o propósito principal é o dinheiro. (PELOTAY, 2017, p. 3)

Em 2017, o mundo presenciou ataques em escala global pelo popular *ransomware WannaCry*, que criptografou todos os dados das máquinas infectadas, solicitando um pagamento para que as informações trancadas, se tornassem novamente disponíveis.

O ransom *WannaCry* utilizou em sua configuração a ferramenta usada pela NSA (*National Security Agency*) vazada no ano de 2017 e tornada disponível graças a atuação do grupo russo de *hackers* chamado *Shadow Brokers*. (PELOTAY, 2017, p. 3)

Essa ferramenta, utilizada pela NSA, chamada *EternalBlue*, é o mesmo nome dado também a vulnerabilidade encontrada nos sistemas operacionais Windows, foco da atuação do *WannaCry*.

O *EternalBlue* explora uma vulnerabilidade no *Windows Server Message Block*, um protocolo de transporte responsável pela comunicação dos sistemas operacionais *Windows*, dos serviços remotos e outros *hardwares* conectados a uma mesma rede. (NEWMAN, 2018).

Segundo o autor (NEWMAN, 2018), a velocidade com que o *WannaCry* se propagou foi resultado da união de dois fatores. O primeiro fator foi a utilização da habilidade do *EternalBlue* de se infiltrar em sistemas; e o segundo foi o incremento do código responsável pela rápida disseminação do *ransom*, como se fosse uma espécie de *worm*.

Ainda que a agência americana não confirme que tenha criado o *EternalBlue*, conforme Newman, editor da revista *Wired*, existem diversas evidências pela rede disponibilizadas pelo grupo *Shadow Brokers* que corroboram para a versão que a NSA utilizou este *tool kit* para fins de espionagem e vigilância em massa. (NEWMAN, 2018).

O *WannaCry* é apenas um exemplo dos vários tipos de *malwares* criados e existentes no mercado paralelo, comercializados principalmente na *deep web*. Pelo exposto, fica claro o potencial destrutivo dos *ransomwares*, que estão cada vez mais acessíveis aos indivíduos, ainda que não tenham conhecimento específico em informática.

A empresa Sophos, uma das maiores do mundo na área de desenvolvimento e fornecimento de *softwares* de segurança, fez um relatório no ano de 2017 chamado *Ransomware as a Service (RaaS): desconstructing the Philadelphia*. Este relatório evidencia como ocorre a venda de diversos RaaS kits, que permite a qualquer um o controle de um *ransomware*.

Segundo o site *Security Report*, especializado em segurança da informação, o relatório foca no estudo do *Philadelphia*, um "produto de antissegurança" disponibilizado pela *Rainmaker Labs*, uma organização cibercriminosa localizada na Rússia. (2017)

Conforme menciona James Lyne, pesquisador chefe de segurança global da Sophos, o *Philadelphia* é o exemplo de como as estratégias de marketing e as vantagens oferecidas pelo modelo RaaS estão sendo tão populares. Segundo este pesquisador, a combinação das práticas de uma legítima indústria de *software*, como a existência de documentações, *updates* constantes dos *malwares*, assistência técnica e interface convidativa do *website*, faz com que pessoas sem conhecimento técnico consigam praticar ciber ataques de elevada qualidade. (PELOTAY, 2017, p. 3)

O relatório explora o *Philadelphia* em diferentes tópicos, a exemplo das estratégias de marketing utilizadas pela *Rainmaker Labs* e na análise de *ransomware*, onde se vislumbra como é possível gerar e operacionalizar o *malware* em questão de maneira eficaz.

Pelotay menciona que a Rainmaker Labs não utiliza somente o próprio site para alcançar clientes. Segundo o autor, existem materiais explicativos desenvolvidos pela empresa na *deep web*, bem como vídeos, anúncios em artigos e *posts* em *blogs* de profissionais da área de segurança da informação, exaltando o "*ransomware market*". (PELOTAY, 2017, p. 4)

Existem diferentes estratégias de precificação entre os fornecedores de RaaS. A mais popular para a definição do preço é o modelo onde o desenvolvedor mantém um percentual dos pagamentos que foram feitos pelas vítimas, enviando o restante para o cliente, a exemplo do *Satan* e do *Mac ransom*. Uma outra estratégia é a venda do acesso ao servidor de comando e controle durante um período de tempo, nos moldes do *Ranion* e *RaasBerry*. (PELOTAY, 2017, p. 5)

Em relação ao *Philadelphia*, os clientes pagam apenas uma vez o valor de 400 dólares. Em troca, vão receber um arquivo executável onde poderão gerar ilimitadas quantidades do *ransomware*. No anúncio deste produto, os desenvolvedores justificam o alto preço com uma série de benefícios, como acesso vitalício, atualizações constantes, ausência de taxas ou comissões pelo uso e a disponibilização de material completo em inglês para ajuda (*Help file*). (PELOTAY, 2017, p. 5)

A *Help file* é essencial pois é onde contém todos os passos instrutórios para um ataque bem-sucedido. Vai trazer o conhecimento necessário para configuração do servidor de comando e controle (*command-and-control server*) para que seja possível a comunicação com os alvos, ensina a criar e enviar as amostras do *ransomware* para confecção dos ataques, bem como gerenciá-los, permitindo o recolhimento de informações estatísticas, checar pagamentos, dentre outras condutas para um ciberataque exitoso.

A *Rainmaker Labs* é uma organização criminosa que se encaixa no modelo de organização empresarial. O *Philadelphia* é somente um exemplo de produto oferecido, existindo uma gama de opções, a exemplo do segundo mais popular, o *Stampado*. Por todas as facilidades oferecidas por este tipo de "empresa", como o acesso vitalício, atualizações e assitência, está crescendo o número de pessoas aptas a praticar cibercrimes, já que possibilita que um indivíduo sem alto conhecimento técnico em informática, possa praticar ciber ataques de qualidade, tendo em vista que são previamente instruídos com o conhecimento necessário para performar as ofensivas virtuais.

5.4. VENDA DE VULNERABILIDADES 0-DAY

Ao ouvir a palavra *hacker*, é comum a maioria das pessoas pensarem em indivíduos que invadem sistemas, roubam informações e visam causar prejuízos diversos a sociedade. Para melhor compreender o que significa, de fato, o *hacking*, é necessário o esclarecimento de alguns conceitos.

Atualmente, o *hacking* não se trata necessariamente de algo criminalizado. Muitos profissionais têm como fonte de renda o exercício do *ethical hacking* que, como o nome já diz, seria uma espécie de *hacking* que possui ética. Diversas organizações contratam esse tipo de *hacker* para realizar testes de penetração (*pentest*) em seus sites e aplicações, visando detectar vulnerabilidades que possam comprometer a seguridade e a usabilidade destes, de modo que possam ser corrigidas antes que haja algum prejuízo.

Por outro lado, existem *hackers* que realizam intrusões de segurança em sites e aplicativos sem o consentimento prévio do responsável pela aplicação. Visam através da busca de *0-days*, obter informação indevida ou vender a vulnerabilidade no mercado paralelo para quem tiver a pretensão de explorá-las.

Essas vulnerabilidades são chamadas de *0-day,* pois ainda não foram descobertas, não existe ainda por parte dos seus desenvolvedores e da sociedade a ciência da falha, somente pelo cibercriminoso.

Segundo Goodman (2015, p. 230), antigamente (quando a internet iniciava a sua expansão), os *hackers* costumavam vender vulnerabilidades (*exploits*) para empresas como Google, Microsoft e Yahoo, por programas de "caça aos bugs" criados por essas próprias empresas. Devido à baixa recompensa que era paga por detectar essas falhas de segurança, os *hackers* começaram a perceber que a venda dessas vulnerabilidades seria muito mais rentável quando feita a governos e criminosos, criando, assim, uma ampla rede de vendedores, compradores e desenvolvedores de *exploits*, gerando o "complexo industrial do *malware*".

Logo, em se tratando de buscas de vulnerabilidades, *hackers* podem ser classificados de três formas: *white hats*, *gray hats* ou *black hats*.

White hats são os que praticam *ethical hacking*. Trabalham quando contratados, realizando diversos testes de segurança para detectar vulnerabilidades e possibilitar a correção delas antes que sejam exploradas por indivíduos mal-intencionados.

Os *gray hats* integram a categoria de *hackers* que estão em um meio termo entre a legalidade e a ilegalidade. Eles não são previamente contratados pelas companhias, mas realizam intrusões, visando detectar falhas para mostrar à organização a sua capacidade de *hacking*, de modo que possa obter alguma recompensa ou até mesmo um emprego.

Em sequência, os *black hats* são *hackers* maliciosos (também chamados de *crackers*) e são o foco principal deste tópico. Tal categoría de *hacker* busca detectar vulnerabilidades *0-day* antes de qualquer pessoa, seja para pessoalmente explorá-la e obter vantagem indevida, ou criar *exploit kits* e vendê-los no mercado paralelo, onde os compradores variam entre organizações criminosas, empresas de cibersegurança e quem mais tiver o capital suficiente para a aquisição.

Conforme definição de Lenny Zeltser (2018), cientista da computação especialista em cibersegurança, um *exploit kit* é um conjunto de ferramentas que automatizam a exploração de vulnerabilidades em aplicações e websites.

Nesse sentido, para utilizar um *exploit kit* o indivíduo não precisa ter conhecimento específico em tecnologia da informação ou cibersegurança, já que ele não está buscando criar o *exploit* em si. Essa falha já foi identificada pelo *black hat* e convertida em um *exploit kit* automatizado.

Essa automatização quer dizer que o *exploit kit* já vem estruturado com o caminho pré-definido para alcançar a vulnerabilidade, além de apresentar uma interface intuitiva e fácil para que o criminoso possa acompanhar o progresso de seu ataque. (ZELTSER, 2018)

Assim como a venda de *malwares*, a venda de *exploit kits* é um negócio altamente lucrativo que tem atraído, cada vez mais, os cibercriminosos pela facilidade de ganhar dinheiro com baixa exposição. São vendidas, na grande maioria das vezes, na *deep web*, e oferecem ao comprador do *kit* toda a assistência necessária para configurar o ataque.

Exploit kits são vendidos a preços altos e expõem falhas de diferentes características que, em mãos erradas, podem causar grande estrago. O fato de esses *kits* necessitarem de habilidades simples para serem operacionalizados e uma interface fácil e intuitiva viabilizam indivíduos comuns a explorarem vulnerabilidades.

Dessa forma, tanto a venda de *malwares* quanto a venda de vulnerabilidades representam uma ameaça real a diferentes tipos de estruturas, a exemplo de escolas, hospitais, agências e órgãos do governo, bem como as residências das pessoas. É extremamente necessário que a sociedade tenha ciência desses fatos para que possa se prevenir corretamente e evitar complicações, como a perda ou roubo de dados pessoais e sensíveis.

6. DIFICULDADES INVESTIGATIVAS

Muitas são as dificuldades relativas à investigação de crimes digitais nos meios jurídicos-policiais. Questões como falta de legislações adequadas para a boa fruição da investigação; a necessidade de ordem judicial até para as coisas

mais simples em um processo do tipo; a dependência das empresas na guarda dos registros cadastrais de autoria ilícito, associado aos curtos prazos para a realização dos pedidos investigativos, somando a isso ainda o tempo de espera na resposta; investigações de materiais com um grau maior de dificuldade, como materiais criptografados, esteganografados e materiais na nuvem, a chamada *cloud computing*.

Deste modo, catalogamos aqui as 5 (cinco) principais dificuldades enfrentadas no que diz respeito à investigação de crimes digitais:

6.1. NECESSIDADE DE ORDEM JUDICIAL

Uma das grandes dificuldades por parte de entidades investigativas no Brasil inteiro, relacionada à investigação de crimes digitais, é a constante necessidade de ordem judicial para a grande maioria das requisições feitas na fase investigativa.

É praticamente certo que, em algum momento das investigações, será necessário ao assistente das vítimas e/ou órgãos policiais investigativos a feitura de uma requisição de autorização ou pedido judicial, no sentido de obrigar as empresas responsáveis pelo armazenamento das informações dos usuários, como dados cadastrais e ips, imprescindíveis, em grande parte das vezes, para a conclusão da investigação, a colaborarem com a identificação do indivíduo por detrás da prática criminosa em questão.

Nesse sentido, discorrem Jorge; Wendt (2013) que o requisito de ordem judicial para obtenção das informações relativas a um crime digital é uma questão que além de atravancar a investigação, se apresenta como das facetas do excesso de burocracia, que segundo os autores apenas prejudica e retarda as investigações desse tipo de delito.

De acordo com os autores: "A solução ficaria na necessária diferenciação entre os acessos aos dados cadastrais e aos *logs* de conexão e/ou de acesso". Exemplo desse processo, consoante os autores, seriam as *hotlines*, espécies de plataformas de contato direto entre empresas portadoras dos dados cadastrais e os órgãos de investigação policial mundo afora, baseadas na busca pela facilitação da obtenção de dados cadastrais sem ordem judicial, por exemplo.

Deram como modelo a seguir, as plataformas *hotline* da Microsoft do Brasil, em pedidos relacionados ao *outlook (hotmail*), *Live* etc, o Mercado Livre, com sua plataforma de compra e venda de bens de consumo e a gigante do mundo digital Google, e suas dezenas de serviço.

Conforme Jorge; Wendt (2013), ainda, esta prática, adotada pelos administradores de tais sites, relaciona-se com seu aspecto contratual, ou seja, todos os que se cadastram e usam os serviços aceitam os "Termos de Uso" e as "Políticas

de Privacidade" e, no contexto dos contratos, conforme as suas determinações próprias, esses sites podem fornecer as informações aos órgãos públicos da lei, *law enforcement,* em inglês, independentemente de ordem judicial. Deste modo, segundo os autores, esse fornecimento de dados por parte da empresa, sem a necessidade de determinação judicial, seria absolutamente legal.

Infelizmente, consoante os autores, poucos são os administradores de sites e demais plataformas de serviços que adotam entendimento semelhante ao abordado, de modo que prevalece o posicionamento sobre a necessidade de determinação judicial para essas informações sejam fornecidas.

Desse modo, informações imprescindíveis para a elucidação de crimes digitais, como os denominados *logs*, sobre os quais discorremos a seguir, ficam muito mais difíceis de se obter.

6.2. GUARDA DE *LOGS*

Conforme Jorge; Wendt (2012, p. 177): "Quando se fala em investigar um crime cometido com a utilização de um dispositivo de acesso a uma rede, é necessário considerar que um dos principais elementos que permitem a identificação do seu autor é o denominado log".

Esses *logs* são dados identificativos gerados pela conexão de determinada aplicabilidade à internet ou a algum serviço disponibilizado na rede mundial de computadores por parte dos chamados provedores de conteúdo e/ou provedores de correio eletrônico (email).

Nesse contexto, Jorge; Wendt (2012, p. 177) descreve o *log* de conexão como: "um conjunto de informações sobre a utilização de internet pelo usuário, contendo data, horário, fuso horário, duração da conexão e número do protocolo de internet, mais conhecido como IP (Internet Protocol)".

Ainda segundo os mesmos o *log* de acesso seria "um conjunto de informações sobre a utilização de determinado serviço na internet (relativo aos provedores de conteúdo) pelo usuário, contendo data, horário e número do IP".

Essas são as informações que, estando os órgãos de investigação em posse, possibilitam a identificação do criminoso digital.

De modo que, como visto no capítulo anterior, essas informações são requeridas em geral através de um pedido judicial, para que se obrigue que o provedor de acesso à internet, tais quais os provedores de conexão, as lan houses ou os administradores de rede privada, que se informe os dados identificativos do computador e do indivíduo a quem foi atribuído o IP, conforme consta nas informações apresentadas pelo provedor e requeridas pela autoridade policial.

De forma que, esses provedores são obrigados a preservar os *logs* de acesso e conexão por um prazo mínimo (6 meses para provedor de conteúdo e 12 meses para provedor de acesso), circunstância esta que muitas vezes inviabiliza ou dificulta a comprovação da autoria do delito. Vez que são prazos muito exíguos, muitas vezes insuficientes para a conclusão da investigação a priori, diante das estruturas policiais cada vez mais sobrecarregadas.

Tal previsão legal, conforme Jorge; Wendt (2013) foi trazida pela Agência Nacional de Telecomunicações (ANATEL), que editou novo regulamento do Serviço de Comunicação Multimedia (SCM), prevendo a obrigação dos provedores em custodiarem "*logs*" por 1 (um) ano (art. 53 da Resolução 614/2013), além de firmar conceitos, como o de "Conexão à Internet" e "Registro de Conexão" e posteriormente pela aclamada Lei 12.965, denominada de Marco Civil da Internet, que consolidou os prazos nos rol de responsabilidades das empresas de conexão e aplicação de internet, quando do tratamento de dados dos usuários brasileiros.

Em respeitos aos prazos previstos em lei no entanto, não são raros os casos em que a demora na resposta ao pedido das informações passa de sessenta dias (prazo previsto em lei para as respostas).

Diante disso, muitas autoridades policiais então optam por comunicar o não fornecimento das informações ao judiciário e solicitar que haja requisição do cumprimento da ordem judicial anteriormente expedida, sob pena de crime de desobediência, conforme Jorge; Wendt (2013).

Outras, no entanto, solicitam ao juiz que fixe obrigação de pagar multa por dia ou hora de retardo.

Desse modo, outra grande dificuldade no tocante às investigações de crimes digitais se refere a necessidade de os entes investigativos terem acesso às informações armazenadas pelas empresas de conexão e de aplicação, a fim de bem executarem o papel de investigação dos crimes digitais.

6.3. INVESTIGAÇÃO DE MATERIAIS COM CONTEÚDOS CRIPTOGRAFADOS OU ESTEGANOGRAFADOS

Consoante Jorge; Wendt (2013) o uso de ferramentas que possibilitem a criptografia e a estenografia por entre os criminosos, de modo a não ser identificados quando do cometimento de crimes, representa uma tendência bastante preocupante no Brasil. Conforme os autores, essas práticas são utilizadas, inclusive, por criminosos para no cometimento de delitos não tecnológicos.

Neste contexto, cabe considerar que criptografia é um procedimento utilizado para misturar ou codificar dados e garantir que apenas o destinatário possa ter acesso ao conteúdo produzido.

Da mesma maneira, a estenografia é um procedimento utilizado para esconder informações de interesse das partes envolvidas na comunicação no interior de uma mensagem. Geralmente, elas são inseridas em vídeos, textos, áudios ou em imagens, sem que terceiros que tenham contato com o material consigam perceber o conteúdo oculto em suas estruturas.

De acordo com os autores, a solução para esta problemática, a qual os orgãos investigativos enfrentam, viria de uma regulamentação do uso de softwares com criptografia, os quais só poderiam ser utilizados se devidamente registrados junto ao órgão competente e com depósito da chave correspondente. Com relação à estenografia, a solução viria através do treinamento focado na detecção de materiais do tipo, junto ao trabalho de perícia forense computacional.

6.4. CLOUD COMPUTING

Cloud computing, ou computação em nuvem, se configura como um meio de armazenamento e partilhamento de informações, que permite ao usuário externalizar funcionalidades de um computador pessoal, como por exemplo a guarda, a edição e o compartilhamento de conteúdos textuais e/ou audiovisuais, para uma plataforma digital, possibilitada pela locação de espaço em servidores físicos de empresas prestadoras deste tipo de serviço, e que, para tanto, utiliza como meio operacional o meio digital, sendo necessário apenas a disponibilização de um computador com acesso à internet.

Sendo assim, conforme Jorge; Wendt (2013), "todo o conteúdo que for produzido ficará disponibilizado "na nuvem", ou seja, em servidores hospedados no Brasil e/ou em outros países. Segundo os autores, um usuário padrão, em geral, sequer sabe fazer a avaliação sobre se os seus dados estão na nuvem ou não, principalmente os que utilizam serviços gratuitos disponibilizados na web.

Deste modo, de acordo com os mesmos, esse é um tema que merece a adequada atenção, principalmente no tocante às dificuldades enfrentadas por parte dos órgãos que realizam a investigação criminal em casos que tenham relação com esse tipo de serviço. Nesse contexto, grande problema advém quando da apreensão de computadores cujos dados essenciais para a elucidação do crime encontram-se em servidores localizados em outro país pois, segundo eles, a perícia forense computacional tem seu papel diminuído em razão dessa prática.

Outro grande problema relacionado à prática de crimes relacionados à utilização das plataformas em questão seria a demora ou impossibilidade do servidor localizado no exterior de fornecer as informações necessárias para a investigação criminal, principalmente se considerarmos que o Brasil não assinou a

Convenção de Budapeste, que prevê a colaboração investigativa por entre entes dos mais diversos países do mundo. De tal modo, conseguinte aos dizeres dos autores, existe a grande dificuldade para garantir o respeito à cadeia de custódia e determinar que o provedor de outro país tire do ar o site e/ou forneça as informações solicitadas para a prática investigativa.

7. FORMAS DE COMBATE À CIBERCRIMINALIDADE PATRIMONIAL

Muito se fala da busca de meios cada vez mais eficazes para o combate à cibercriminalidade. Esses meios perpassam por investimentos maciços em questões estruturais, investimentos em capacitação de pessoal, metodologias e técnicas investigativas, bem como conscientização das vítimas.

Deste modo, catalogamos aqui os 5 principais meios vislumbrados para a melhora de eficiência no que diz respeito a investigação de crimes digitais:

7.1. CAPACITAÇÃO DOS ENTES ESTATAIS

O combate à cibercriminalidade, em todas as suas searas, passa por uma necessidade cada vez mais proeminente da capacitação de policiais, membros do Ministério Público e Judiciário, na produção e reprodução de conhecimentos ligados à investigação, entendimento legal e procedimental do combate a tais tipos de crimes.

O combate aos crimes digitais representa um grande desafio, na medida em que grande é a abragência dos cibercrimes, e a falta de capacitação dos entes estatais imbuidos da aplicação da punição para a prática de crimes pode impedir a punição dessa espécie de criminosos e, por consequência, gerar a impunidade dos mesmos. Vez que, além dos conhecimentos investigativos padrão, se faz necessário, ainda, o entendimento de questões técnicas computacionais, voltadas ao rastreio e identificação do criminoso digital.

Nesse sentido, muitos são os casos que acabam emperrando ou ficando sem solução, por falta de uma capacitação técnica dos entes investigativos. Desse modo, se faz extremamente necessária a capacitação desses entes investigativos, como forma de permitir que questões técnicas referentes à investigação dos crimes digitais estejam dentro de seu rol de conhecimentos, possibilitando a fluidez investigativa e a elucidação de pontos investigativos.

Neste contexto, de acordo com Jorge; Wendt (2013):

> [...] a capacitação deve ser realizada continuamente, por profissionais especializados, de modo que os órgãos da persecução possam reprimir e acompanhar a evolução desses crimes."

Segundo os autores, os integrantes desses órgãos devem ser estimulados por políticas internas e externas a participarem destas capacitações e treinamentos relacionados ao trabalho investigativo e atuação ostensiva relacionadas ao tema. Defendem que devem ser implementadas políticas públicas nacionais, voltadas aos órgãos de segurança pública, de modo a incentivar os entes estatais a investirem na qualificação de seus quadros jurídico-policiais.

Em outras palavras, somente com treinamentos exaustivos acerca do tema poderemos ter profissionais de excelência, treinados adequadamente, que trarão como também como retorno a prevenção aos crimes cibernéticos, fator fundamental em virtude da falta de educação digital do usuário de internet brasileiro.

7.2. DESAPARELHAMENTO DE ORGANIZAÇÕES CRIMINOSAS ATUANTES NA REDE

Os atuais recursos tecnológicos informáticos permitem que os criminosos digitais, espalhados por diversas localidades, comuniquem-se e realizem as suas ações criminosas em parceria e organizadamente, muitas vezes de maneira orquestrada e pouco chamativa.

Por essa razão, tem sido muito comum, na investigação de crimes cibernéticos, com exceção aos de menor potencial ofensivo, tais quais crimes contra a honra e afins, constatar a existência de criminosos espalhados em diversas localidades do país e/ou do mundo, que muitas vezes conhecem apenas pelo intermédio da rede, e cuja comunicação ocorre apenas por meio dela, de maneira a configurá-la como ferramenta principal na preparação e prática dos crimes.

Conforme Jorge; Wendt (2013), essa interação do mundo criminoso com o uso dos recursos informáticos tecnológicos tem dificultado cada vez mais e mais a investigação de crimes, não pelo desconhecimento dos processos investigativos em si, mas também pela encriptação dos dados realizada pelo próprio criminoso ou pelas ferramentas utilizadas por ele, tais quais os navegadores da *Deep Web*, comunicadores instantâneos e afins.

7.3. INTEGRAÇÃO DOS ENTES INVESTIGATIVOS

De acordo com Jorge; Wendt (2013) é de consenso da grande maioria dos orgãos que promovem a investigação e processamento de crimes praticados pela internet que, diferentemente dos criminosos, não existe uma atuação integrada entre os responsáveis pela investigação e processamento da prática de tais modalidades criminosas, mesmo entre aqueles pertencentes ao mesmo setor.

Conforme os autores, tal afirmativa se comprova, inclusive, por entre os setores pertencentes ao mesmo órgão que não possuem a cultura do comparti-

lhamento do conhecimento operacional e das informações quantitativas e qualitativas sobre os cibercriminosos e as atuações em território nacional. O que, segundo eles, faz-se com que a falta de conhecimento e atuação padronizada seja sentida em um mesmo Estado.

O modelo que exemplifica, no entanto, a forma de atuação que deveria ser adotada pelos demais orgãos, contrariando o cenário geral, vem do estado do Paraná, que possui uma estrutura que em um único órgão de persecução penal concentra todos os entes atuantes nos procedimentos de crimes relacionados à internet.

Conforme os autores, tal metodologia

> [...] facilita a compreensão do problema em âmbito macro e favorece, inclusive, a adoção de práticas padronizadas de combate e prevenção aos crimes cometidos através da internet.

Ainda conforme informações quantitativas, o Brasil possui, no âmbito das polícias judiciárias estaduais, menos de cinquenta por cento de seus Estados com órgãos especializados. Nesse contexto, conforme informações do site safenet.org, dispomos de Delegacias de Polícia Especializadas apenas em 15 dos 27 estados da federação.

7.4. COOPERAÇÃO INTERNACIONAL

Conforme Jorge; Wendt (2013), foi criada, na Hungria, no ano de 2001, a Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, pelo Conselho da Europa, a qual detinha entre suas principais finalidades: a busca pelo incremento da cooperação internacional entre os órgãos investigativos no âmbito criminal; a previsão de novas condutas criminais causadoras de prejuízo e transtornos para a vítima mediante o uso da internet; pressionar a aprovação de legislação específica sobre o tema por entre os seus signatários etc.

O Brasil não é signatário do referido tratado, e a tendência é que crimes do tipo que ultrapassam as barreiras nacionais continuem aumentando, bem como a necessidade de obtenção de informaçôes que permitam esclarecer a autoria dos crimes, estando as provas de sobremaneira no exterior, de modo que a cooperação internacional se torna imprescindível para a busca da verdade, ou seja, para que se atinja o absoluto esclarecimento sobre o crime em apuração, suas circunstâncias, autores e verdades sobre as condutas apuradas.

Segundo Jorge; Wendt (2013), no ano de 2010 o, à época, chefe interino da Unidade de Crimes Cibernéticos do FBI, James Harris, foi entrevistado pela Agência Brasil e expôs sua preocupação com o fato de o Brasil se tornar alvo

de cibercriminosos do Leste Europeu. De acordo com seu entendimento, como a economia brasileira estava crescendo mais do que a do resto do mundo, certamente atrairia os mesmos tipos de criminosos que atuavam/atuam contra as instituições financeiras sediadas nos Estados Unidos. Sendo que, sabidamente, a maioria desses criminosos vive no Leste Europeu, para onde o dinheiro roubado pela internet é levado.

7.5. EDUCAÇÃO DIGITAL

De maneira geral, diz-se que os usuários de internet não conhecem a dimensão dos perigos e riscos que correm com a utilização da internet; desconhecem as ameaças que enfrentam ao receber e abrir arquivos provenientes de e-mails, acessar sites ou ao instalar programas em seu computador.

Tem-se, ainda, que a utilização de redes sociais também representa um grande perigo para os internautas desavisados e um campo muito fértil para que os cibercriminosos possam dispersar seus arquivos maliciosos para agregar informações sensíveis, como dados pessoais e financeiros e/ou causar problemas para as vítimas, ao relacioná-la como fonte de dispersão de vírus de computador.

Dessa maneira, no caso de um usuário de uma rede social ser contaminado, por exemplo, há o risco de enviar os arquivos maliciosos para todos os seus contatos, e aqueles que receberem as mensagens possivelmente irão acreditar no conteúdo recebido e, por consequência, também serão contaminados, reforçando o ciclo de vida útil do malware ali utilizado. Sobremaneira, esse alerta deve ser dado a crianças e adolescentes, tendo em vista que são mais vulneráveis a esse tipo de fraude, vez que, de acordo com Jorge; Wendt (2013), "mais importante do que munir o usuário de recursos tecnológicos avançados visando tornar a utilização da internet mais segura é a sua conscientização". Pela tomada de consciência, o usuário consegue vislumbrar a necessidade de inserir no seu dia a dia boas práticas de uso responsável da internet, para que torne o uso dos serviços online muito mais seguro e proveitoso.

Tem-se ainda que, segundo os autores, o processo de conscientização e aprendizado dos usuários de internet, a denominada educação digital, deve partir não só dos órgãos de prevenção, mas também dos de repressão. Pois, conforme eles, a partir do momento em que os policiais informam os usuarios sobre como ocorre, por exemplo, determinada fraude, existe a possibilidade de o usuário passar a se precaver e não ser mais uma vítima de crimes do tipo.

8. PREJUÍZOS CAUSADOS PELOS CRIMES CIBERNÉTICOS PATRIMONIAIS

Segundo Mattos *apud* IDC Brasil (2017), "a quantidade de fraudes que ocorrem no Brasil é alarmante". Conforme o autor, de acordo com pesquisa realiza-

da pela empresa: "De um universo de 290 pequenas e médias empresas, quase 60% (sessenta por cento) mencionaram a ocorrência de vírus em seus servidores." E afirma, ainda, que "os incidentes de segurança no Brasil cresceram 71% (setenta e um por cento) apenas no primeiro semestre de 2004." Para ele,

> O tipo de ocorrência que mais cresceu, percentualmente, foi a fraude, que aumentou 856% (oitocentos e cinquenta e seis por cento) no primeiro semestre de 2004 passando de 142 fraudes nos primeiros seis meses de 2003 para 1.358 até outubro de 2004.

De acordo com o autor, a Pest Patrol, outra empresa do setor de segurança de redes de computadores: "identificou cerca de 22,7 mil programas que roubam informações pessoais e alteram as configurações dos programas de navegação na internet, os browsers."

Ainda segundo o autor, em conformidade com esta empresa, a gigante do setor informático, a Microsoft, revelou que: "um único vírus, o MSBlast, infectou mais de 9,5 milhões de computadores no mundo, no período compreendido entre os meses de setembro de 2003 e setembro de 2004."

E por último, consoante o autor, conforme a mi2g Intelligence Unit, a empresa londrina de consultoria em risco digital:

> (...) de um total de 125 mil ataques a computadores em todo o mundo, o Brasil é o responsável por 95,5 mil deles, ou seja, 76,2% (setenta e seis virgula (sic) dois por cento). Em seguida vem a Turquia, com 14,7 mil ataques, ou seja, 11,8% (onze virgula (sic) oito por cento). (grifo nosso)

Ainda conforme o autor, tal qual relatórios da mesma empresa, os invasores brasileiros se especializaram nas mais diversas formas de crimes digitais: "desde furto de dados e identidade, a fraudes com cartão de crédito, pirataria e vandalismo on-line", pois o Brasil não possuiria legislação com punições específicas para esses tipos de delitos. "Em 2004 um estudo feito pelo governo norteamericano (sic) indicou que 8 (oito) em cada 10 (dez) *crackers* da internet na época eram brasileiros." (grifo nosso)

Essas informações representam o potencial destrutivo dos cibercriminosos brasileiros, de modo que cabe às forças policiais e entidades de segurança digital se munirem de meios de combate a tal ameaça.

Conforme o autor:

> Mais recentemente o Cert (Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores do Brasil) informou em seus relatórios anuais que as fraudes da internet saltaram de cerca de 85 mil em 2013 para mais de 460 mil em 2014, ou seja, um crescimento de cerca de 500%. (grifo nosso)

Nesse contexto, vemos que a expoente de crescimento de cibercrimes no Brasil nos dá um panorama geral dos prejuízos causados pelos crimes digitais, em especial os patrimoniais e o potencial futuro, que abordaremos no próximo capítulo.

9. FUTURO

A tecnologia se desenvolve de maneira exponencial. Todos os dias, novas ferramentas são criadas e aprimoradas com o intuito de facilitar a vida das pessoas. Uma dessas ferramentas que tem apresentado forte crescimento é o *cloud computing*, como abordado anteriormente.

Isso tem favorecido uma migração cada vez mais acentuada de técnicas *hackers,* no intuito de defraudar essas novas ferramentas de armazenamento online. Nesse sentido, vemos que grande parte das empresas que atuam no mercado utilizam servidores próprios para armazenar dados seus, de clientes e fornecedores. Pessoas comuns armazenam em seus dispositivos uma quantidade cada vez maior de informação, incluindo fotos, e-mails, documentos de trabalho, dentre outros.

Ao armazenar esse tipo de informação em uma estrutura física própria, como um HD de um computador, o responsável por essas informações deve manter o dispositivo sempre configurado nos corretos padrões de segurança e realizar o monitoramento constante dos dados, para verificar a integridade deles.

Ocorre que nem sempre é dado o devido tratamento à proteção dessas informações, seja por falta de investimento na área de tecnologia da informação ou negligência do responsável por essa atribuição. Assim, quando se trata de segurança da informação, tem crescido o número de indivíduos que optam por fazê-la através da infraestrutura em *cloud*.

Ainda que em um primeiro momento possa parecer imprudente terceirizar a segurança, deve-se analisar o caso concreto. Por exemplo, ao terceirizar a segurança da informação, uma empresa teria mais tempo para se dedicar a sua área principal de atuação, sem se preocupar em tomar medidas diretas para esse tipo de questão, já que as medidas de segurança da informação estariam sendo aplicadas pelos responsáveis da estrutura em *cloud*.

Porém, aquele que adotar essa opção deve ficar atento a certos critérios na hora de contratar os serviços de um provedor de *cloud*, buscando fazer um comparativo daquele que melhor se enquadra para as necessidades do contratante.

Atualmente, existem multinacionais que oferecem o serviço em *cloud* para as mais diversas finalidades como Google, Amazon, Dropbox, Microsoft, dentre outras. Além dessas, há diversos provedores de estrutura menor, voltados

para suprir particularidades do mercado nacional. Segundo Antonio Carlos Pina (2015), diretor da Mandic Cloud Solutions, aquele que busca utilizar serviços em *cloud*, deve analisar alguns pontos para evitar situações penosas em seus processos.

Conforme menciona o autor, é importante saber há quanto tempo a empresa está no mercado. Isso pode evitar que o contratante tenha que migrar de provedor, porque o seu atual fechou. É interessante buscar provedores consolidados e estáveis, visando evitar esse tipo de situação. Além disso, o provedor deve ser um especialista. A sua atividade principal deve ser o fornecimento de estrutura em *cloud*, pois se assim não for, dificilmente será dada a atenção necessária a manutenção da qualidade. (PINA, 2015)

Deve-se verificar, ainda, se o provedor possui uma plataforma de *cloud* flexível, disponibilizando diferentes modalidades de contratação, se por preço fixo ou preço variável. O preço variável é mais indicado para indivíduos ou organizações que estão testando algum novo projeto. Nesse sentido, o preço aumenta ou reduz conforme o projeto é testado. O preço fixo é recomendado para indivíduos ou organizações que já possuem um projeto construído em funcionamento, de modo a evitar variações de preço e poder contar com uma maior segurança e previsibilidade.

São muitas as opções de provedores de *cloud* hoje em dia. Diante de tantas variáveis e particularidades dos negócios e projetos, a parte interessada deve dialogar com a equipe técnica do provedor, de modo a obter informações que o ajudem a escolher a alternativa que mais se enquadre a suas necessidades, com a maior segurança possível.

CONCLUSÃO

Já há algum tempo passou-se a sentir frente a economia de grande parte das economias dos países do mundo, incluindo o Brasil, uma grande mudança de meio na realização de transações comerciais e financeiras. O que despertou o interesse da criminalidade quanto à possibilidade do cometimento de ilícitos patrimoniais nos meios digitais.

Desse modo, passou a haver uma forte migração dos crimes patrimoniais para os meios digitais, em específico para a internet, tendo em vista se buscar uma maior lucratividade e uma maior facilidade na aplicação de golpes financeiros. Temos presenciado o avanço cada vez mais contundente de indivíduos com conhecimento técnico-informático, os conhecidos *hackers*, e até de empresas especializadas, no fornecimento de serviços e mecanismos que propiciem a prática de atividades criminosas no ambiente digital, o que vem auxiliar os criminosos que não dispõem de conhecimento técnico na área.

Dentre tais mecanismos, podemos citar as plataformas Saas, de vendas de *malwares*, de vendas de vulnerabilidades zero-day e afins, bem como plataformas Raas, que têm transformado a venda dos *Ramsomwares*, agora popularmente conhecidos como ferramentas de "sequestro de dados", em um negócio extremamente lucrativo. Esses passaram a despertar o interesse das organizações criminosas mundo afora, e no Brasil.

Ocorre que esse é um mercado em franco crescimento, que conta com a vantagem de atuar em um ambiente propício a anonimização dos envolvidos, que é a *Deep Web*, dificultando, e muito, o enfrentamento a tais práticas criminosas.

Sendo assim, necessário se faz a promoção de medidas para superação dos problemas ligados a essa realidade e ao combate ao crescimento da criminalidade nos meios digitais, através do aparelhamento, união, troca de experiências e capacitação dos entes investigativos, bem como das próprias vítimas.

A previsão é que essa migração ocorra de forma cada vez mais evoluída, contribuindo na expansão da criminalidade tanto no mundo digital quanto no mundo físico. Sendo assim, pôde-se chegar à conclusão de que a principal medida de combate à criminalidade nos meios digitais, não só a criminalidade patrimonial como outras afins, é a capacitação dos operadores do direito, dos entes investigativos e das próprias vítimas no combate a tais práticas criminosas.

REFERÊNCIAS

AMOROSO, Danilo. **Aprenda a diferença entre vírus, trojan, spyware, entre outros**. 2008. Disponivel em: https://www.tecmundo.com.br/phishing/853-aprenda-as-diferencas-entre-virus-trojans-spywares-e-outros.htm. Acessado em: 15 jun. 2018;

BARRETO, A. G.; BRASIL, B. S. **Manual de Investigação Cibernética: à luz do Marco Civil da Internet.** [S.l]: Brasport, 2016.

BARRETO, A. G..; CASELLI, G.; WENDT, E. **Investigação Digital em Fontes Abertas.** [S.l.]: Editora Brasport Livros e Multimídia Ltda. 2017;

BRASIL. **Decreto Lei nº 2.848, de 7 de dezembro de 1940.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acessado em: 26 set. 2018;

CASSANTI, M. D. O. **Crimes Virtuais, Vítimas Reais.** [S.l]: Editora Brasfort Livros e Multimídia Ltda. 2014;

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte especial**. 6ª ed. Salvador: Editora Jus Podium. 2014;

FEDERAL BUREAU OF INVESTIGATION. **2017 Internet Crime Report**. 2017. Disponivel em: https://pdf.ic3.gov/2017_IC3Report.pdf. Acessado em: 10 jun. 2018;

FRUHLINGER, Josh. **What is Ransomware? How it works and how to remove it**. 2017. Disponivel em: https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html. Acessado em: 17 jun. 2018;

GOODMAN, Marc. **Future Crimes**. 1ª ed. São Paulo: HSM, 2015;

HOFFMAN, Chris. **What is a Botet?**. 2016. Disponivel em: https://www.howtogeek.com/183812/htg-explains-what-is-a-botnet/. Acessado em: 15 jun. 2018;

HOPPING, Clare; MCCALLION, Jane. **What is a Trojan virus?** Disponível em: http://www.itpro.co.uk/security/30081/what-is-a-trojan-virus. Acessado em 15 jun. 2018;

JESUS, Damásio de. **Direito Penal: Parte especial**. 2004. 26ª ed. Sao Paulo: Saraiva. v. 2;

JORGE, H. V. N.; WENDT, E. **Crimes Cibernéticos, Ameaças e procedimentos de investigação.** 1ª ed. Editora Brasfort Livros e Multimídia Ltda. 2012;

JORGE, H. V. N.; WENDT, E. **Crimes Cibernéticos, Ameaças e procedimentos de investigação.** 2ª ed. Editora Brasfort Livros e Multimídia Ltda. 2013;

LIMA, Glaydson de Farias. **Manual de Direito Digital**. 1ª ed. Curitiba: Editora Appris. 2016;

NEWMAN, Lily Hay. **The leaked NSA spy tool that hacked the world**. 2018. Disponivel em: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/. Acessado em: 10 set. 2018;

PELOTAY, Dorka. **Ransomware as a Service (RaaS): Deconstructing Philadelphia**. 2017. Disponivel em: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/RaaS-Philadelphia.pdf. Acessado em: 20 ago. 2018;

PINA, Antonio Carlos. **Como escolher um provedor de cloud**. 2015. disponivel em: http://cio.com.br/tecnologia/2015/08/17/como-escolher-um-provedor-de-cloud/. acessado em: 22 out. 2018

PINHEIRO, Patrícia Peck. **Direito Digital.** 6ª ed. São Paulo: Editora Saraiva. 2016;

RANKIN, Bert. **A Brief History of Malware - Its Evolution and Impact**. 2018. Disponivel em: https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/. Acessado em: 15 jun. 2018;

RANKIN, Bert. **Malwares Types and Classifications**. 2018. Disponivel em: https://www.lastline.com/blog/malware-types-and-classifications/. Acessado em: 15 jun. 2018

LI, Ray. **What is Cryptojacking?**. 2017. Disponivel em: https://hackerbits.com/programming/what-is-cryptojacking/. Acessado em 19 set. 2018;

RICHARDSON, Robert. **Ransomware**. 2017. Disponivel em: https://searchsecurity.techtarget.com/definition/ransomware. Acessado em: 17 jun. 2018;

Scientific American. **When did the term "computer virus" rise?**. 2001. Disponivel em: https://www.scientificamerican.com/article/when-did-the-term-compute/. Acessado em: 17 jun. 2018;

SOUZA, Bernardo de Azevedo. **Ainda sobre a *Deep Web*: O lado positivo da rede.** 2015. Disponível em: https://canalcienciascriminais.com.br/ainda-sobre-a-deep-web-o-lado-positivo-da-rede/. Acessado em: 10 set. 2018;

TAGIAROLI, Guilherme. **Considerada uma das maiores pragas da Internet, vírus "I Love You" completa 10 anos**. 2010. Disponivel em: https://tecnologia.uol.com.br/ultimas-noticias/redacao/2010/05/04/considerada-uma-das-maiores-pragas-da-internet-virus-i-love-you-completa-dez-anos.jhtm. Acessado em: 15 jun. 2018;

ZELTSER, Lenny. **What is an Exploit Kit?**. 2018. Disponivel em: https://zeltser.com/what-is-an-exploit-kit/. Acessado em: 12 set. 2018.

4

O AVANÇO DAS FACÇÕES CRIMINOSAS TRADICIONAIS PARA A INTERNET, OBJETIVANDO A VENDA DE PRODUTOS ILÍCITOS

Daniela Dias[1]
e Livanilda Meneses[2]

Resumo: Este artigo se propõe a analisar o avanço das facções criminosas tradicionais para a internet, oportunizado em razão da massiva utilização de meios de dispositivos e plataformas eletrônicas. Aliado a isso, conta-se com a vulnerabilidade dos usuários e a facilidade de se obter dados pessoais por meio do que se costuma classificar como engenharia social. A metodologia utilizada foi embasada em fontes de publicação jornalísticas encontradas no meio eletrônico. A análise do resultado faz acreditar que o PCC, hoje, é a facção tradicional com mais habilidades de atuação no suporte físico, o que faz crer que haverá uma continuidade delitiva de igual êxito no espaço cibernético. Conclui-se que essa prática adquirida no decorrer das atividades delitivas fez com que as facções viessem se fortalecendo, antevendo, desde cedo, a possibilidade de vender produtos ilegais através dos meios eletrônicos. Os produtos ofertados se diversificam quando passam a ser comercializados no lado obscuro da internet, a chamada *deep web* ou mesmo a *dark web*, lugares até então pouco conhecidos de muitos, mas caracterizado por uma intensa interface comercial. E o PCC vem apostando suas fichas neste novo ambiente velho.

PALAVRAS CHAVES: Organização Criminosa; Pluralidade de Facções; Fortalecimento e Estruturação; Ambiente Físico e Virtual; Crimes Naturais; Cibercrimes.

---

1 Advogada, pós-graduada em Direito Público, Diretora Regional do SEMPRES/BA- Sindicato das Empresas Privadas de Resíduo Sólido do Estado da Bahia.

2 Servidora Policial Civil, Graduada em Direito, Pós-graduada em Direito Público e em Política, Estratégia e Planejamento Estratégico, Professora da disciplina Direito Penal e Processo Penal da Faculdade de Tecnologia e Ciências – FTC.

1. INTRODUÇÃO

O avanço da tecnologia traz grandes vantagens para facilitar a vida de todos, muito embora se saiba que ainda é necessário solidificar uma consciência digital, a fim de que se faça um bom uso da internet. E esse bom uso não se resume apenas à navegação em si, mas, sobretudo, em como proteger os dados pessoais a fim de não se tornar vítima fácil de uma engenharia social arquitetada com o intuito de auferir vantagens e causar prejuízos.

Isso porque é possível visualizar que a criminalidade vem se utilizando de recursos tecnológicos para a prática de crimes, intentando, por certo, migrar de um panorama de um mundo real para o mundo virtual sabedores, por certo, que nossa legislação é frágil e desatualizada para lidar com questões desta natureza. Esta incipiência favorece a prática de delitos cibernéticos.

Os bens de necessidade e os serviços essenciais para a vida em sociedade são fartamente oferecidos por meio virtual, fazendo com que a internet facilite as atividades rotineiras que vão desde pesquisas de assuntos diversos até a aquisição de bens através do comércio eletrônico ou realizações de transações financeiras por meio de dispositivos e plataformas eletrônicas, como computadores e celulares.

Por conta da utilização massiva de computadores é que vem ganhando força o cometimento de delitos através da internet, justamente por conta da vulnerabilidade nesta rede de informação global. A natureza da ameaça cibernética nos padrões de hoje é muito mais avançada no sentido de obter vantagem econômica, na medida em que o agente se sente protegido, por se considerar escondido atrás das máquinas.

Crimes que antes eram executados *facie ad faciem*, a exemplo do delito de extorsão, hoje vem sendo praticado na rede mundial de computadores através, por exemplo, de um código malicioso que torna inacessíveis os bancos de dados de empresas ou mesmo de particulares, o chamado *ransomware* e outros congêneres, valendo-se da criptografia dos arquivos e exigindo o pagamento de um resgate desses dados para que o seu proprietário possa restabelecer seu acesso.

O que surpreende é que, não obstante se valer de um apossamento ilegal de dados ou arquivos e não mais do sequestro da pessoa física em si, o pagamento geralmente se dá através das chamadas moedas eletrônicas, a exemplo do *bitcoin*. E a preferência por esta forma de pagamento é por conta do seu anonimato e por não ser, em tese, rastreável. São espécies de arquivos digitais armazenados em "carteiras digitais", em um celular ou computador.

A criptografia também evoluiu, tornando cada vez mais difícil o acesso a tais comunicações, e o combate a esse meio de cometimento de crimes tem se

revelado de difícil manejo, o que se deve, em boa parte, às exigências e certa má vontade dos provedores de conexão ou de aplicação para fornecer as informações que são solicitadas pelos Órgãos da persecução penal, dificultando, sobremaneira, a investigação.

Para além da falta de colaboração no sentido de fornecer o acesso quando solicitado, tais empresas vêm buscando formas de criptografar o tráfego interno de seus sites, com o argumento de preservação do direito à privacidade dos seus usuários e, com isso, fortalecer o argumento da negativa em atender às solicitações feitas.

Essa dificuldade é um obstáculo no combate aos crimes cibernéticos, visto que um grande passo seria dado se houvesse essa cooperação entre órgãos públicos e os provedores de aplicação e de conexão. Como não há uma forma de filtrar o usuário criminoso do não criminoso, fica-se à mercê daqueles, que se valem dessa proteção em forma de criptografia para planejar e executar condutas criminosas.

As variáveis de cometimento desses crimes são extensas, cite-se aí a clonagem de cartões bancários, crime que vem ganhando o espaço cibernético, através de transferências e pagamentos de boletos bancários feitos de formas fraudulentas. Outros crimes não usuais também encontram espaço, exemplificados no uso de mensagens enxertadas, modificando-se os *bits* das imagens coloridas, técnica conhecida como esteganografia.

São modalidades não tão recentes, porém desconhecidas de muitos, ocorrendo cada vez mais novas formas de cometimento de crimes e alocadas de forma tão rápida no ambiente virtual, que faz com que a legislação não acompanhe com a mesma rapidez essa trajetória, criando, assim, um significativo descompasso entre essas inovações e a segurança pública como um todo, já que a legislação não manteve e nem mantém o mesmo ritmo do avanço tecnológico.

O que se percebe é que a criminalidade organizada vem se valendo de profissionais de tecnologia de informação para utilizar seus conhecimentos na disseminação de links e e-mails falsos, aplicando golpes em sites bancários ou disseminando programas maliciosos, os chamados *banloads*, *malwares* específicos para transações bancárias via internet.

O recrutamento desses *hackers*, ou *crackers*, pode se dar de diversas formas, inclusive quando estes são presos através de pequenas investigações não ligadas ao crime organizado propriamente, mas que quando desbaratadas essas associações criminosas, uma vez condenados e cumprindo pena, passam a interagir com aqueles que posteriormente vão cooptá-los, intentando usar conhecimentos de informática para a execução de novas modalidades de crime.

Não há mais como retroceder, entramos na era digital, isso é fato. E as organizações criminosas estão harmonizadas com a atualização tecnológica, em uma grandeza diretamente proporcional, dando origem ao que se denomina crimes cibernéticos, tendo como meio de execução um computador ou uma rede de computadores, entretanto, em uma escalada e organização muito maior do que se possa supor.

E o combate a essa modalidade de crimes também tem de acompanhar as mudanças, pois agora de nada adianta armas de fogo de grande poder de parada ou técnicas inovadoras de incursão em ambientes sensíveis. A prevenção, análise, investigação e punição contra os crimes cibernéticos exigem mudanças.

Isso passa por treinamentos e capacitação no ramo da informática, bem como utilização de programas específicos para rastreio do caminho utilizado pelos criminosos. Neste panorama se torna primordial mais conhecimento e mais capacidade de elucidação e prevenção dos crimes.

É um tema que precisa ser enfrentado pois, hodiernamente, já se vislumbra a utilização maciça do uso da internet para o cometimento de delitos. A criminalidade organizada tende a, em um futuro muito próximo, adotar essa modalidade como a melhor e mais apta alternativa a ser utilizada, a fim de dar continuidade às práticas delitivas pois, como dito, o confronto e combate pelos órgãos da Segurança Pública tendem a dificultar o processo de práticas e comércio de bens ilícitos no ambiente físico. A migração é inevitável.

2. AS ORGANIZAÇÕES CRIMINOSAS NO BRASIL

O crime organizado ocupa o espaço e dita o regulamento para o convívio social. Os maiores exemplos no Brasil são dois grandes grupos voltados para o narcotráfico, a exemplo do Primeiro Comando da Capital (PCC) e do Comando Vermelho (CV), os quais são apontados, há décadas, pelo meio jornalístico, sociólogos e cientistas políticos, como autênticas e poderosas organizações criminosas.

Com efeito, as ações realizadas por esses grupos, com ostensivo recurso à violência, emprego de meios tecnológicos e notório poder de barganha perante as autoridades públicas, sobretudo após os ataques levados a cabo pelo PCC no Estado de São Paulo em maio de 2006, revelaram *modus operandi* bastante peculiar, centralizando em rígido núcleo de comando e internamente hierarquizado.

Na atualidade, continua-se falando muito sobre esses dois grupos, à sombra dos quais teriam se desenvolvido as demais organizações criminosas no país. Há de se asseverar que o próprio conceito de organização criminosa era uma lacuna no ordenamento brasileiro. Mesmo com a edição da primeira lei a tra-

tar sobre o assunto, a 9.034/95, não se definiu o que viria a ser organização criminosa no Brasil, ficando a cargo e empréstimo da conceituação trazida pela Convenção Internacional de Palermo.

Apenas no ano de 2012 foi apresentada uma conceituação; não obstante, no ano seguinte, por um descuido do legislador, novo conceito legislativo foi adotado, sem revogar o anterior, acontecendo, assim, uma inaceitável ocorrência da existência de duas conceituações quase similares.

À luz de uma ótica garantista, o conceito de organização criminosa pode ser lido a partir da lei 12.850/13, que definiu organização criminosa como sendo a associação de quatro ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a quatro anos, ou que sejam de caráter transnacional.

3. PRINCIPAIS ORGANIZAÇÕES CRIMINOSAS

Segundo dados de especialistas em segurança pública no Brasil pode haver no país mais de trinta organizações criminosas muito poderosas com atuação dentro e fora dos presídios. Não há como validar essa afirmação, posto que muitas facções vêm crescendo e se desenvolvendo de forma muito rápida. Na mesma velocidade, há o seu esfacelamento e os respectivos dissidentes logo se unem, formando novos grupos entre si.

No Brasil, como dito, o Primeiro Comando da Capital e o Comando Vermelho, são as principais facções brasileiras que disputam o poder dentro dos presídios, a fim de manter a liderança na venda de drogas ilícitas e na aquisição de armas de grande poderio bélico.

O Comando Vermelho, que tem sua origem na ditadura militar, sendo composto inicialmente por presos políticos, é considerada hoje uma espécie de governo paralelo numa parte considerável da geografia do Estado do Rio de Janeiro, onde ali ocupa extensa porção das favelas existentes. Seus gerentes e colaboradores costumam ser vistos em plena luz do dia fortemente armados e impondo, à força, suas normas de organização naquela sociedade.

O fundador do Comando Vermelho, William da Silva Lima, conhecido como o Professor, é autor de uma obra intitulada Quatrocentos Contra Um - uma História do Comando Vermelho, na qual narra como convenceu e organizou o presídio para a boa convivência com determinações de liderança.

Uma das características do Comando Vermelho é formar parcerias com facções regionais, em troca oferecem proteção, almejando fortalecer e quantificar

seu exército de homens. A estrutura de liderança do CV (sigla da organização) é linear, em vez de um chefe, a organização conta com uma espécie de "conselho", mesmo assim, atualmente, alguns líderes se destacam, que é o caso de Fernandinho Beira Mar e Marcinho VP.

O Primeiro Comando da Capital, o PCC, por sua vez, não precisou subir os morros cariocas para sua formação, surgindo nos presídios paulistas sob o argumento de lutas contra a opressão e as injustiças do sistema carcerário daquele Estado. Tornou-se uma das maiores lideranças no mundo do crime. Teve editado um bem elaborado e respeitado estatuto do crime, redigido por um dos seus integrantes, o presidiário Mizael Aparecido da Silva, e marca como lema a Liberdade, Justiça e Paz.

O estatuto prega a obrigatoriedade de um compromisso entre os seus integrantes, inclusive aqueles que ganharem a liberdade, devendo sempre ajudar e colaborar com seus irmãos que continuarem na cadeia, sendo tal compromisso a regra, passível de morte aquele que descumprisse o estatuto.

A facção PCC está presente em quase todos os estados da Federação e tem ramificações em países fronteiriços com o Brasil, dedicando-se atualmente a ser o principal fornecedor de drogas, evitando confrontos com outras facções, preferindo a harmonia e a liderança nas vendas. Em verdade, o PCC tem uma inegável habilidade em se estruturar em forma de verdadeira empresa do crime e se habilitar como uma espécie de *holding*.

Por óbvio que com algumas peculiaridades que fogem à regra do verdadeiro conceito de *holding*, posto que não se enquadra apenas na questão de deter a maior parte das ações dessas empresas do crime, mas que produz bens e serviços que traçam e determinam a própria distribuição, não sem perder o controle das suas subsidiárias.

Outras organizações criminosas têm se revelado proeminentes, a exemplo da Família do Norte - FDN, como é conhecida. Trata-se de facção com sede no Amazonas. Seus membros são tratados como irmãos, em referência aos dois irmãos que fundaram a facção, criada como uma espécie de reação ao controle exercido pelo Primeiro Comando da Capital (PCC) nas atividades do tráfico.

Apontada hoje como a terceira maior facção criminosa do Brasil e contando com um efetivo de mais de duzentos mil membros, já demonstrou seu poder de força dentro do Presídio de Pedrinhas no Estado do Maranhão. Embora a FDN seja aliada ao CV, a aliança decorre em razão apenas de serem rivais do PCC, pois que a FDN tem estrutura autônoma e nunca aceitou ser subordinada a nenhuma outra organização.

A exemplo do PCC, a FDN criou sua própria Constituição, chamada de Doutrinas da Família; contando com apenas três páginas, o documento apre-

senta a ideologia da facção, suas normas de comportamento e as respectivas punições. Essa facção se caracteriza, peculiarmente, por se voltar para o mundo tecnológico com ações de contra-inteligência e *modus operandi* próprios.

Outra facção que surgiu dentro dos presídios do Rio de Janeiro é a Amigo dos Amigos, ou A.D.A, formada por dissidentes e em reação ao poderio do Comando Vermelho. Tantas e outras foram nascendo e se revelando, constituindo um considerável número de facções em território brasileiro. Note-se a facção Sindicato do Crime, que atua dentro dos presídios e redutos de narcotráfico do Rio Grande do Norte.

Impende pontuar acerca das facções que vêm ganhando força no território baiano, pode-se falar que são marcadas pela desorganização e falta de estrutura escalonada entre seus membros, mas que vem dominando bairros e comunidades baianas, em verdadeira guerra por domínio de territórios.

Já se tornaram conhecidas e vêm ganhando relevo, fazendo com que a Bahia se revele como um dos Estado com mais facções no país, a exemplo da Ordem e Progresso (OP), do Bonde do Maluco (BDM), Katiara, Bonde do Ajeita e Mercado do Povo Atitude (MPA), em sua grande parte aliados do PCC. As facções Caveira e Comando da Perna têm proximidade com o CV. São pequenas facções aliadas às grandes facções.

Em razão desse crescente número de facções criminosas que atuam no tráfico de drogas no Estado da Bahia, houve um considerável e nefasto aumento no número de Crimes Violentos Letais Intencionais (CVLIs) no primeiro semestre de 2018, em comparação com o mesmo período no ano de 2017. Bairros em Salvador têm o domínio completo ou demarcado em áreas de determinadas facções.

Na Bahia não há uma facção hegemônica. As facções surgem por causa do alto nível de repressão do sistema carcerário e buscam sua inspiração nas organizações criminosas bem estabelecidas, como o Comando Vermelho e o Primeiro Comando da Capital, muito embora não possuam um terço da estrutura organizacional daquelas.

A Katiara é uma das facções com maior relevo no solo baiano, domina grandes e populosos bairros em Salvador, assim como cidades do Recôncavo, tais como Maragogipe, Nazaré das Farinhas e Amargosa, sendo esta última cidade seu berço natal. Seu meio de vida baseia-se não só no narcotráfico, mas também no cometimento de furtos e roubos a instituições bancárias, práticas que vêm se disseminando no interior e na capital da Bahia.

Em um breve resumo pode-se pontuar acerca da existência de outras fações baianas, a exemplo do Comando da Paz, ou CP, que iniciou abraçando o mesmo discurso de melhorias das condições prisionais.O Bonde do Maluco

teve seu surgimento no presídio Complexo Mata Escura, tem parceria com o Primeiro Comando da Capital e é a facção com um pouco mais de organização no estado baiano.

A facção Caveira guarda maior proximidade com o PCC; e o grupo paulista montou uma espécie de centro de distribuição de cocaína em Feira de Santana. A facção Bonde do Neguinho tem sua criação na cidade de Vitória da Conquista e conta com o apoio do PCC. A Comando do Boqueirão (CB) surgiu em um bairro que hoje conta com três bases comunitárias, mas, ainda assim, conseguiu se erguer.

Outras facções têm surgido, podendo exemplificar com Vida Loka, que vem ganhando adesão com a juventude baiana. A DMP, cuja sigla faz menção a três bairros da cidade de Itabuna - Daniel Gomes, Maria Pinheiro e Pedro Jerônimo. A MPA, Mercado do Povo Atitude, que vem ganhando expressão na cidade de Porto Seguro, no sul do estado.

Infelizmente, esse é o cenário que vem sendo desenhado por parte da criminalidade, que não chega a se revelar com a estrutura de uma empresa criminosa, mas cujas existências contribuem para o fortalecimento das já estruturadas organizações criminosas.

4. A MIGRAÇÃO DO CRIME ORGANIZADO PARA O AMBIENTE VIRTUAL

Há uma dinamização dos fluxos de informações ao redor do mundo, e o crime organizado está ciente disso. Existe no mercado consumerista um termo conhecido como Fisital, que trata sobre a complexidade do varejo atual, significando a utilização pelas empresas de modelos de negócios da junção do Físico com o Digital, contemplando esses dois ambientes: offline e online.

Comparando o termo utilizado no mercado de consumo tem-se que a criminalidade organizada vai se utilizar igualmente dos dois ambientes, trabalhando de forma ilícita com a tendência de se especializar, cada vez mais, no ambiente virtual. Há, portanto, uma tendência de união entre o mundo físico e o virtual, ou seja, os mesmos crimes naturais podem também ser cometidos através da internet.

Com isso, toda a captação de dados qualificativos ou experienciais das prováveis vítimas, que os criminosos procuram se utilizar antes de aplicarem seus golpes, pode também acontecer através da internet. É o que vem sendo chamado de engenharia social.

A engenharia social nada mais é do que um método de ataque, onde o engenheiro social, no caso o criminoso, se utiliza de fraudes para obter informações de pessoas, por vezes abusando da sua ingenuidade ou boa-fé, para depois uti-

lizar essas informações em acesso não autorizado a computadores ou objetos congêneres, com o fim especial de causar danos ou obter vantagem econômica.

À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltam, cada vez mais, para a exploração do elemento humano. Quebrar a "*firewall* humana" quase sempre é fácil, não exige qualquer investimento além do custo de uma ligação telefônica e envolve um risco mínimo.

Daí a necessidade de entender que a aquisição de conhecimentos e uma educada forma de transitar pelo mundo guiado pela internet é uma obrigação de todos. Seria a única forma de ganhar uma guerra em um espaço guerreado pelos cybercriminosos, que tendem a se expandir sempre mais.

A intenção não é ensinar as melhores técnicas de segurança digital e nem de como evitar ser vítima de um golpe digital, mas sim de demonstrar que o crime organizado está se organizando para cometer ilícitos no espaço cibernético e a forma de que estão se valendo é a da combinação do conhecimento da arte de manipular com o uso da tecnologia.

Mas a questão envolve saber por que se entende que o ambiente virtual seria seguro para a prática de crimes. Decerto, por causa da facilidade no recrutamento de profissionais peritos em cada área do conhecimento que, juntos, compilariam seus conhecimentos e estabeleceriam uma estrutura organizacional com verdadeira divisão de tarefas e esforço comum.

A dificuldade consistiria em se identificar cada especialista na empreitada criminosa e a prova de que formariam vínculos permanentes, uma vez que agiriam como terceirizados do crime, ofertando seus serviços para outras facções ou para grupos rivais destas e, assim, afastar a questão da permanência e estrutura empresarial que caracteriza o crime organizado, atuando em uma verdadeira prestação de serviços criminais.

5. POTENCIALIDADE DESTA MIGRAÇÃO VIRTUAL: QUEM DETÉM O PODER

Circulam pela internet, através dos aplicativos de mensagens instantâneas, histórias que vêm se tornando habituais, dando conta de que as facções criminosas vêm se imiscuindo em questões políticas a fim de influenciar de forma decisiva no pleito eleitoral, alcançando, com isso, a vitória nas urnas daqueles candidatos por elas indicados.

E uma das organizações que vem se revelando nesta ingerência de forma ilícita, seria o PCC, cujo objetivo último é inserir seus membros nas instituições estatais, fortalecendo cada vez mais o seu poderio e, com isso, nas respectivas

casas legislativas onde estariam infiltrados seriam apresentados projetos de leis de interesse da organização criminosa.

Ao que parece o PCC intenta ser maior do que o próprio Estado, se arvorando a decidir pleitos eleitorais de acordo com seus interesses ilegais e, assim, age de forma impositiva e coercitiva. Essas publicações dando conta de que as facções criminosas vêm se imiscuindo em questões políticas a fim de influenciar de forma decisiva no pleito eleitoral, alcançando com isso a vitória nas urnas daqueles candidatos por elas indicados, vêm se espalhando cada vez mais nos aplicativos de mensagens instantâneas.

Mas não é apenas nesta seara que o crime organizado vem se destacando. A utilização de criptomoedas para a venda e circulação de produtos ilegais é uma outra oportunidade de expansão dos negócios. Trata-se de uma tecnologia digital rápida, barata e sem intermediários, podendo ser feita *peer-to-peer* (pessoa a pessoa), em qualquer lugar, sem limite mínimo ou máximo de valor e qualquer pessoa pode operacionalizar essa forma de pagamento.

Embora haja uma mistificação no sentido de entenderem que essas moedas eletrônicas não sejam rastreáveis, não há como se afirmar isso, uma vez que há um cadastro prévio exigido pelas corretoras e todas as operações são registradas no *blockchain*, uma espécie de livro contábil das moedas eletrônicas.

Essas operações, quando realizadas, possuem códigos de endereços que podem ser atrelados às identidades fornecidas. Bem verdade que é um trabalho que regride ao início das transações eletrônicas efetuadas, o que torna o serviço complexo, mas não impossível.

Para além da dificuldade de rastreio, há ainda a questão dessas criptomoedas serem usadas para lavagem de capital, o que torna mais difícil a investigação e facilita a vida criminosa, posto que no silêncio do legislativo, no tocante à regulamentação para os criptoativos, há, ainda, a dúvida jurisprudencial e doutrinária acerca da possibilidade de as criptomoedas valerem como forma de cometimento do crime antecedente, uma vez que não são regulamentadas pelo Banco Central.

Mas não é só. É sabido que o simples fato de transacionar com moedas eletrônicas não torna o fato caracterizador do delito de lavagem de dinheiro. O próprio COAF – Conselho de Controle de Atividades Financeiras, órgão competente no combate à lavagem de dinheiro no Brasil, determina que alguns setores específicos da economia informem as transações acima de determinado limite ou que se revelem suspeitas, e comuniquem essas operações aos órgãos competentes.

As empresas com atividades voltadas para a troca de criptomoedas, ao fazerem a conversão em moeda corrente nacional, embora ainda não constem no

rol das empresas obrigadas, algumas já o fazem, o que faz diminuir a chance da possibilidade desse tipo de moeda ser objeto de lavagem de capital.

A questão da criminalidade organizada se valer dessas transações eletrônicas não é, pura e simplesmente, pela sua inovação ou complexidade no rastreamento, mas sim, porque, como afirmado, tem-se buscado alternativas ou oportunidades de meios outros para o cometimento de delitos, e a internet é um campo fértil para isso. O PCC, diante da sua organização e delimitação de atuação, tem o aparato exigível para a utilização desses novos meios de operacionalização do crime.

6. TECNOLOGIA E NOVAS MODALIDADES DE CRIMES

Como dito, a tecnologia tornou-se o elemento facilitador da prática de crimes tradicionais e, também, para o surgimento de novos tipos de crimes. Hoje é necessário, para compor essa empresa do crime, especialistas em eletrônica, informática e de sistemas de serviços informáticos fornecidos através de uma rede de telecomunicações, criptografia, operações financeiras, dentre outros, adequando-se ao novo *modus operandi* das organizações criminosas.

A busca do aprimoramento e combate ao crime choca-se com a evolução rápida dos sistemas de proteção, flexibilidade de comunicação, facilidade de localização que proporcionando a segurança, o anonimato e rapidez em que não se localiza o usuário/criminoso. Os crimes são cometidos por causa da demora em se chegar a sua origem, quando não são, muitas vezes, desvendados.

Essas organizações criminosas atuam em meio à tecnologia de diversas formas; uma delas é através da criminalidade difusa que se caracteriza, normalmente, pela ausência de vítimas fisicamente individualizadas. Trata-se de pessoas indeterminadas, ligadas entre si por circunstâncias alheias, por exemplo, correntistas de um determinado banco, clientes de certa bandeira de cartão de crédito ou um grupo social específico, que se tornam vítimas dos golpes tecnológicos.

Tal aspecto revela a periculosidade da organização ante as dimensões e a quase irreparabilidade dos danos causados, bem como a morosidade da ação estatal posterior. Através dos meios eletrônicos os criminosos ocultam os atos preparatórios e de execução do crime, e quem os comete são pessoas com dedicação exclusiva e qualificação de ponta nas diversas áreas onde se faça necessária a sua atuação, contando com remuneração e equipamentos modernos, muitas vezes superiores aos da própria Segurança Pública.

As ações das organizações criminosas também se caracterizam por sua alta velocidade de realização. Impressiona a capacidade de adaptação dos agentes

às novas tecnologias, com modificação quase que instantânea da dinâmica para fazer frente a novos padrões de segurança de empresas ou instituições.

Os operários dessas organizações atuam em vários grupos e subgrupos que, por vez, se associam a outros grupos para a realização de negócios específicos, com tipo de crime específico, atravessando fronteiras e globalizando-se. Assim, as organizações criminosas formam alianças entre si, fomentando uma rede secundária de outras organizações criminosas de apoio e divisão de tarefas.

Ratificando o que vem sendo apontado neste trabalho, o PCC se associou aos criminosos paraguaios, à máfia boliviana e aos chineses, a fim de conseguir seus objetivos, ou seja, dominar o mercado brasileiro e internacional com a facilidade da obtenção de armas, drogas, cargas roubadas, munições e explosivos, bem como levantamento de informações, aprimoramento nas execuções e negociações, transporte de drogas e o arregimento de novos integrantes.

Mediante diversas investigações, descobriu-se a existência do chamado "Rebirth Program" - programa de renascimento - desenvolvido por organizações criminosas estrangeiras que fornecem aos seus clientes qualquer identidade de qualquer nacionalidade no mundo inteiro, com as devidas certidões de nascimento, carteira de identidade e passaporte, todos falsos, possibilitando que um criminoso de um determinado país torne-se um cidadão "de bem" em outro país.

Os mentores dessas organizações fazem uso de meios eletrônicos para vender virtualmente a seus clientes essa nova identidade, sendo o pagamento feito através de depósitos em conta, fazendo uso de moedas virtuais. O crime cibernético tem uma característica de futurismo e de aperfeiçoamento nas suas técnicas.

7. CONCLUSÃO

Existe, sim, um avanço das facções criminosas tradicionais para a internet com o objetivo de vendas de produtos ilícitos, e a facção com mais propriedade neste caráter de migração é o PCC. Mas, atente-se. Não é a presunção de impunidade que caracteriza essa migração e nova forma de atuação. É a inovação do *modus operandi,* característica peculiar do PCC de arriscar e de criar novos meios de cometimentos de delitos, ou seja, meios inovadores para delitos antigos.

Diante disso, questiona-se qual a maneira de se obter êxito na prevenção ou combate no avanço das organizações do crime. A maneira mais hábil é a aplicação de um eficaz serviço de inteligência com modernas estruturas de coleta de informações estratégicas e por vezes sensíveis. É uma ação que requer investimentos financeiros e um aprendizado dos integrantes da segurança pública para o correto manejo das ferramentas e das informações colhidas.

Não se pode olvidar que o mundo do crime migrou para o espaço cibernético, trazendo consigo toda a organização e planejamento estratégico que conquistou no mundo real. E as vítimas continuam sendo as mesmas, ou seja, os desavisados, alvos fáceis do que se denominou chamar de engenharia social.

A mudança do local de guerra apenas migrou para um mundo virtual e abstrato, seja pela presença da *Surface Web* ou das camadas mais escondidas da internet, a exemplo da *Deep Web*, composta por sites que não são indexáveis, ou mesmo da mais obscura de todas, a *Dark Web*, mas o que importa é que a luta não precisa ser desigual, o conhecimento é a chave.

Conclui-se que toda a habilidade do mundo do crime apresentada no trato com a sociedade física e real ratifica a impressão que vai se firmar no âmbito eletrônico e continuar a utilizar toda a expertise para bem atuar no suporte digital.

REFERÊNCIAS

AMORIM, CARLOS. **Comando Vermelho: a história secreta do crime organizado**. Rio de Janeiro: Record, 1993.

_____. **Código Penal**. Decreto-lei n. 2.848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 27/09/2018.

_____. **Lei nº 12.694**, de 24 de julho de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12694.htm. Acesso em: 27/09/2018.

_____. **Lei nº 12.850**, de 2 de agosto de 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 27/09/2018.

BARCELLOS, Caco. **Abusado - O dono do Morro Dona Marta.** Rio de Janeiro: Record, 2003.

CONSERINO, Cassio Roberto. **Crime organizado e institutos correlatos. São Paulo:** Atlas, 2011.

COSTA, Lurizam Viana. **A organização criminosa na lei 12.850/13**. São Paulo, 2017. Disponível em: http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/BUOS-ASHGA3/a_organiza__o_criminosa_na_lei_12.850_13__disserta__o___lurizam_costa__viana_.pdf?sequence=1 Acesso em: 10/07/2018.

FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião; MORAES, Maurício Zanoide de. **Crime organizado: aspectos processuais.** São Paulo: Editora Revista dos Tribunais, 2009.

GODOY, Marcelo. **PCC usa doleiros e já fatura mais de R$ 400 milhões,** de 03 de junho de 2018. Disponível em: https://www.terra.com.br/noticias/brasil/cidades/pcc-usa-doleiros-e-ja-fatura-mais-de-r400-milhoes,d3bcd9febdbceaa03cfd1f11984789f2rr2by2pt.html. Acesso em 05/11/2018.

LACERDA, Ricardo. **Facções Criminosas no Brasil.** São Paulo: Abril, 2017.

LIMA, William da Silva. **Quatrocentos Contra Um - uma História do Comando Vermelho.** Editora Vozes, 2010.

MENDRONI, Marcelo Batlouni. **Crime organizado: aspectos gerais e mecanismos legais.** São Paulo, Atlas, 2015.

PACHECO, Rafael. **Crime organizado: medidas de controle e infiltração policial.** Curitiba: Juruá, 2009.

SILVA, Eduardo Araújo da. **Crime organizado: procedimento probatório.** São Paulo: Atlas, 2003.

TRIBUNA. **Adelio teria ligação com o PCC, aponta investigação da PF,** de 19 de outubro de 2018. Disponível em: https://tribunademinas.com.br/noticias/politica/19-10-2018/adelio-teria-ligacao-com-o-pcc-aponta-investigacao-da-pf.html. Acesso em 02/10/2018.

VIANA, Severino Coelho. **O cangaço não acabou.** BuscaLegis.ccj.ufsc.br. Acesso em 27/04/2018.

ZIEGLER, Jean. **Os senhores do crime: as novas máfias contra a democracia.** Rio de Janeiro: Record, 2003.

5

VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS: CYBER ATAQUES E A NECESSIDADE DA OBRIGATORIEDADE DE "*REPORT*" NO BRASIL

Bárbara Emily Ribeiro de Oliveira[1]
e Eloah Lucena Bicalho[2]

Resumo: Este artigo é destinado à análise dos novos cenários atingidos pelo cometimento de crimes cibernéticos e, no caso em questão, referente às possibilidades de essas ocorrências já estarem convergindo para atingir as infraestruturas críticas nacionais, tendo em vista as comprovações e ataques que geraram grandes repercussões, possibilitando a relevância acerca da discussão sobre esse assunto. Desse modo, procurou-se examinar os mecanismos e vulnerabilidades do sistema operacional que possam levar as infraestruturas críticas, de fato, a serem os próximos e/ou possíveis alvos desses ataques, os quais, se ocorrerem, ensejarão prejuízos de grande escala para toda a sociedade.

Palavras-Chave: Infraestruturas críticas; Ataques; Vulnerabilidade; "*Report*"; Proteção.

1 Graduanda em Direito pela Faculdade Baiana de Direito e Gestão.
2 Graduanda em Direito pela Faculdade Baiana de Direito e Gestão.

1. INTRODUÇÃO

O escopo deste artigo é propor uma reflexão acerca da importância das infraestruturas críticas para a sociedade e para o Estado, bem como demonstrar a necessidade da divulgação dos ataques que sofrem, de forma a fazer com que tais vulnerabilidades sejam combatidas. Assim, como medida fundamental para tal finalidade faz-se necessária a obrigatoriedade legal da divulgação dos ataques, de forma a propiciar uma melhor cooperação e compartilhamento de informações, tanto por parte do setor público quanto do setor privado.

É perceptível, para grande parte da sociedade, a importância de empresas como Coelba, Embasa, Petrobrás, e a sua importância no cotidiano. É certo que essas empresas apresentam, junto com o seu sistema operacional, plataformas de defesa cibernética e protocolos que têm como foco a proteção das suas infraestruturas. Porém, apesar de a busca do aprimoramento dessas plataformas e a evolução dos sistemas operacionais resultarem em um aumento da potencialidade da defesa há, também, um caminho paralelo a esse, que é a qualificação dos *malwares,* espécie de vírus, que não atuam apenas invadindo e prejudicando os sistemas operacionais, mas como importante meio para a prática de atividades que não estão em consonância com os princípios legais e muito menos com a real finalidade dessas indústrias.

A situação vem gerando uma maior preocupação para especialistas na área porque, há alguns anos, em alguns países como Ucrânia e Reino Unido, foram divulgados ataques que ocorreram em suas infraestruturas críticas, o que despertou um alerta maior tanto para os especialistas quanto para os responsáveis do departamento de segurança desses países. Entretanto, esses acontecimentos não geraram grandes impactos no Brasil, o que de certa forma faz pensar quais os impactos, caso eventos como esses ocorressem. Porém, o que se sabe pela legislação brasileira é que as infraestruturas críticas não são obrigadas a reportar seus ataques cibernéticos, situação que gera uma insegurança para o poder público, para outros entes privados e, principalmente, para a população mais próxima dessas infraestruturas.

Dessa forma, o avanço dessas formas de atuação criminosa no âmbito cibernético, no que concerne à invasão das plataformas das infraestruturas críticas, não vem sendo acompanhado das devidas mudanças jurídicas, o que implica defasagem de sanções. Logo, esse problema há de ser abordado numa perspectiva que venha a estabelecer regramento que preveja, por sua vez, a necessidade de "*report*" dos ataques cibernéticos às autoridades competentes, o que repercutiria em um acompanhamento público desses ataques. Assim, essa seria uma nova atribuição de função para a Secretaria de Segurança Pública, que atuaria na prevenção e recuperação das infraestruturas críticas contra esses ataques cibernéticos.

2. INFRAESTRUTURAS CRÍTICAS

2.1. NOÇÕES PRELIMINARES

Preliminarmente, faz-se necessário compreender que a sociedade vem mudando e, atreladas a essa mudança, novas formas de facilitar a vida vêm surgindo. Muito disso se atribui à globalização que mudou o mundo e trouxe consigo significativas vantagens, mas como todo bônus ela também possui seus ônus. Pode-se comparar, de forma singela, a uma moeda, que possui duas faces, uma boa e outra má. Assim, se em uma face estão as vantagens, com destaque para as econômicas, que criam "oportunidades de comércio, contactos (sic) culturais e maior qualidade de vida"[3], do outro lado há uma incerteza desregulada pertencente às trevas. São nessas sombras que se faz presente o perigo.

A evolução dos meios de produção e de comunicação foi revolucionada com o advento da internet, fazendo com que houvesse uma maior dinamicidade nas relações pessoais e comerciais. Logo, o tamanho progresso nessas áreas envolve, de igual maneira, problemas que devem ser abordados e solucionados.

Assim, diante dessa nova realidade, que trouxe consigo uma melhor organização dos meios de produção e, portanto, uma nova forma de facilitar a aquisição e o gerenciamento de riquezas, surge, também, o interesse criminoso em tais oportunidades.

Isso, porque a globalização alterou a realidade econômica mundial de forma a fazer com que houvesse um "*boost*", uma nova propulsão, um novo mecanismo, que possibilitou às companhias terem uma nova forma de gestão de forma a reduzir custos e aumentar a sua eficiência. Logo, o que antes era mais demorado, o que antes era feito manualmente ou somente por humanos passou a ter para si uma nova forma de gestão, de produção, havendo, assim, o deslocamento de grande parte do gerenciamento de controle para um sistema informatizado.

Dessa forma, pode-se afirmar que houve considerável aumento na quantidade de transações o que fez com que as informações passassem a transitar pela internet, sendo que cada dado pode ser dotado de diversos níveis de proteção. Assim, a proteção dos "sistemas de controle tornou-se uma questão muito mais séria desde o advento da Internet e o aumento das ameaças terroristas"[4], até

3 PEREIRA, António Martins. As Ameaças Transnacionais e a Segurança Interna. **Revista de Ciências Militares**, v. 2, n. 1, 2014. Disponível em: <https://s3.amazonaws.com/academia.edu.documents/33924580/As_Ameacas_Transnacionais_e_a_Seguranca_Interna_AMP.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1526340741&Signature=5Xc87dVfaXyFYWKf8uV%2FfA8VBpY%3D&response-content-disposition=inline%3B%20filename%3DAs_Ameacas_Transnacionais_e_a_Seguranca.pdf >. Acesso em: 14 maio 2018, p. 307.

4 Tradução Livre. "*Securing control systems has be- come a much more serious issue since the advent of the Internet and the rise in terrorist threats.*" Original em: GEER, David. *Security of*

porque tanto o governo quanto os entes privados migraram o seu operacional para um sistema de controle conectado à internet.

Ocorre, assim, a migração dos crimes e daqueles que os praticam para um novo campo, para um novo território a ser conquistado, que é o mundo cibernético, em que, apesar de as ações serem virtuais, as consequências materializam-se no "mundo físico".

2.2. O ESPAÇO VIRTUAL COMO EXTENSÃO DO COMETIMENTO DOS CRIMES DO MUNDO REAL

É fato que os avanços tecnológicos trouxeram ferramentas bastante úteis para o cotidiano de qualquer pessoa/cidadão nos dias atuais. Entretanto, atreladas às facilidades e comodidades que essas inovações trouxeram, especificamente para o mundo virtual, atitudes criminosas criaram outra roupagem.

Admite-se, assim, as mesmas finalidades criminalísticas, mas em um território/espaço diferente, já que, muitos criminosos se utilizam dessas ferramentas virtuais, principalmente fazendo uso da própria internet, para atingir pessoas financeiramente, através de pedidos de dinheiro de resgate em moedas virtuais (sejam em *bitcoins, z-cash* ou *monero*)[5], o que traz consigo uma grande facilidade de transferência para todo mundo.

Então, a partir do momento em que se descobre e se consegue realizar esse modo de transação, há simultaneamente uma grande dificuldade de rastreamento, apesar do anonimato não ser total e de não possuírem o mesmo preço de moeda oficial[6]. Isso possibilita invadir computadores tendo como finalidade se utilizar de fotos intimas de terceiros, situação similar à que ocorreu com a atriz Carolina Dieckmann, que ensejou a lei dos crimes cibernéticos 12.737/2012.

Entretanto, apesar de essa lei já ser considerada um pequeno avanço para o controle de determinadas infrações penais virtualmente, ela apenas "tipifica como crimes infrações relacionadas ao meio eletrônico, como invadir computadores, violar dados de usuários ou "derrubar" sites"[7]. Vale considerar que,

---

Critical Control Systems Sparks Concern. **Computer**, v. 39, n. 1, p. 20-23, 2006. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1580377>. Acesso em: 14 maio 2018, p. 20.

5 Policia Civil de Santa Catarina. **Policia civil de SC é elogiada mundialmente pela solução rápida do caso de extorsão, mediante sequestro, com pagamento em moeda virtual**. Disponível em: < http://www.policiacivil.sc.gov.br/informacoes/noticias/38168-policia-civil-de-sc-e elogiadamundialmente-pela-solucao-rapida-do-caso-de-extorsao-mediante-sequestro-com-pagamento-em-moeda-virtual>. Acesso em: 18 jul. de 2018, p. 1-2.

6 Barbirato, Alex. **A Verdade Sobre Bitcoins**. Disponível em: <https://cryptoid.com.br/destaques/verdade-sobre-bitcoins/>. Acesso em: 18 jul. de 2018, p. 2-3.

7 [7] PINHEIRO, Fábio Ponte. **A Cibernética Como Arma de Combate**. Trabalho de Conclusão de Curso. Rio de Janeiro: Escola Superior de Guerra, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 25 jul. 2018, p. 14.

mesmo já sendo um pequeno avanço, muitos dos crimes que hoje ocorrem virtualmente já são previstos no ordenamento jurídico brasileiro, sendo essas penas aplicadas, independente de terem sido cometidos mediante a internet, por já haver previsão legal.

Uma curiosidade que poucos sabem a respeito da legislação Brasileira é que ela abrange, aproximadamente,

> [...] cerca de 90 a 95% os crimes praticados no âmbito virtual em nosso país, pois os crimes praticados por meio do computador para realização do delito mais conhecido como a modalidade de crimes próprios são normalmente já tipificados em nosso Código Penal.[8]

Dessa forma, percebe-se que enquanto a própria vivência humana está sendo transportada para diversos mecanismos cibernéticos, diversas infrações também estão se reformulando para adaptar-se a essa nova era social e digital. Assim, não é muito distante de se imaginar que muitos criminosos consigam se especializar melhor em determinados golpes e áreas e atinjam estruturas muito maiores que simples computadores e pequena parcela da população.

Com aprimoramentos, polos petroquímicos, usinas hidrelétricas, dentre outras infraestruturas, podem vir a se tornar o novo "campo minado" desses "cybercriminosos" e, dessa forma, mascarar ataques diretos contra estados e populações, de maneira a fazer com que eles se passem por acidentes esporádicos.

Para a prática de tais atos, esses sujeitos, utilizando-se da informática (as próprias máquinas), na realidade, estarão cometendo graves atos/infrações que necessitarão de rápida identificação por poderem constituir possíveis crimes impróprios, entendidos como: "aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática".[9]

Assim, a previsão legal dessas condutas é necessária e esperada, fazendo com que, seja possível sua aplicação pelas autoridades, devendo existir, também, a estipulação de sanções e de medidas de prevenção adequadas, capazes de lidar com essas situações.[10]

---

8 *Ibidem, loc. cit*.

9 ARAS, Vladimir. **Crimes de Informática: Uma Nova Criminalidade**. Jus Navigandi, Teresina, v. 5, 1998. Disponível em: <http://www.egov.ufsc.br:8080/portal/sites/default/files/anexos/13015-13016-1-PB.pdf>. Acesso em: 26 nov 2018, p. 08.

10 PINHEIRO, Fábio Ponte. **A Cibernética Como Arma de Combate**. Trabalho de Conclusão de Curso. Rio de Janeiro: Escola Superior de Guerra, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 25 jul. 2018, p. 12.

2.3. O QUE SÃO INFRAESTRUTURAS CRÍTICAS?

As facilidades que o desenvolvimento da tecnologia trouxe, como o baixo custo, a rapidez de acesso às informações e a melhoria no processamento de dados com o avanço das chamadas *Informations and Communication Technologies* (ICT), geraram uma dependência em relação às infraestruturas de informação, que são conhecidas, também, como *Information Infrastructures* e têm como uma de suas principias funções dar o suporte operacional a grandes empresas, organizações estatais e, em geral, nos outros setores da economia.

Dessa forma, com essa nova ferramenta à mão, o próximo passo foi a adequação, ou seja, fazer com que cada sistema concretizasse as soluções para as funções para as quais foi imaginado, de forma a corresponder às expectativas.

Assim, como sucedâneo dessa perspectiva, surgiram as chamadas infraestruturas críticas (Critical Information Infrastructure – CII).

Apesar das definições e conceitos diferentes, há o entendimento comum de que as infraestruturas críticas são aquelas consideradas de extrema importância para o país, pois o impacto do seu não funcionamento implica consequências sociais, econômicas, podendo, ainda, causar danos ambientais e para a segurança nacional. Logo, o impacto ocorre diretamente no bem-estar dos cidadãos, bem como, afeta o bom funcionamento das estruturas estatais e o desempenho das indústrias.

As infraestruturas críticas necessitam ter um bom desempenho das suas funções de forma a propiciar o resultado final pretendido. Assim como foi dito, essas infraestruturas possuem um importante papel na sociedade, e o seu mau funcionamento gera inúmeras consequências negativas.

Como exemplo, podem ser citadas como críticas as infraestruturas[11]:

I) Relacionadas ao setor de eletricidade, abastecimento de combustível e fornecimento de água;

II) Aquelas do sistema de transporte, comunicação, suprimento de comida e saneamento básico;

III) As diretamente ligadas ao sistema financeiro;

IV) As que suportam a defesa militar do país e que, também, contribuem na atuação da proteção dos cidadãos no âmbito civil;

V) As que proporcionam o bom funcionamento dos serviços de emergência, estejam eles relacionados à saúde, meio ambiente ou ao serviço de resgate;

11 NICKOLOV, Eugene. *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations*. **INFORMATION AND SECURITY**, v. 17, p. 105-119, 2006. Disponível em: <http://defencemanagement.org/system/files/17.07_Nickolov.pdf>. Acesso em: 14 maio 2018, p. 106.

VI) Aquelas que desempenham funções referentes ao bom funcionamento da Justiça, por exemplo, as que estão correlacionadas ao Poder Judiciário, Ministério Público, Defensoria Pública e OAB.

Além das que foram exemplificadas, existem outras, sendo que, o bom funcionamento delas é essencial; assim, a segurança e a proteção dessas infraestruturas são assuntos de extrema importância devendo, portanto, ocupar um maior espaço nas preocupações estatais.

2.4. NOVA FORMA DE ATAQUE ÀS INFRAESTRUTURAS CRÍTICAS E SEUS SUJEITOS

A maneira mais convencional de cometer um crime é presencialmente/fisicamente. Ocorre que a mudança na forma de gerenciar os serviços, a produção e a segurança que a internet pôde proporcionar acarretou uma mudança de cenário. Assim, o que está ocorrendo é uma mudança na forma de ataque, já que o ataque virtual envolve menores riscos para aqueles que atacam e causa os mesmos danos ou até mesmo maiores danos aos atacados.

Há que se frisar, também, que o foco anterior dos ataques às infraestruturas críticas estava centrado na sua destruição, ou seja, a finalidade era boicotar e dar um fim mesma, no entanto, o que se percebe, atualmente, é que passaram a existir novos objetivos relacionados a esses ataques.

Assim, quando há a invasão de um sistema operacional de uma infraestrutura crítica, os dados presentes naquele sistema ficam vulneráveis, sendo que cada informação ali contida possui um grau de proteção diferenciado. Então, ao acessar essas informações os atacantes podem roubar os segredos industriais como, por exemplo, a fórmula de um produto, eles podem roubar dados pessoais, tanto de funcionários quanto de fornecedores, podem sequestrar o *browser* da infraestrutura crítica, etc.

Os antigos sistemas operacionais se diferenciam dos atuais pelo acesso à internet, já que os antigos não possuíam esse acesso, essa porta de entrada, de forma que a sua vulnerabilidade estava centrada no acesso telefônico, que era projetado para permitir que fornecedores terceirizados trabalhassem com o software conforme necessário.[12] Com esses sistemas ligados à internet a situação se torna completamente diferente demandando novas soluções de segurança.

A concepção da preservação segura e íntegra em relação a esses sistemas está diretamente relacionada aos conceitos de ameaça, segurança, ataques e vulnerabilidade.[13]

---

12 GEER, David. *Security of Critical Control Systems Sparks Concern*. **Computer**, v. 39, n. 1, p. 20-23, 2006. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1580377>. Acesso em: 14 maio 2018, p. 22.

13 CZINER, Krisztina et al. *Critical Information Infrastructure Protection in the Baltic Sea Area: The Case of TETRA*. **CIVPRO Working Paper, Helsinki University of Technology, Communica-**

Afirma-se que "o termo "segurança" é usado no sentido de minimizar as vulnerabilidades de ativos e recursos. [...]. Uma vulnerabilidade é qualquer falha que possa ser explorada para violar um sistema ou as informações nele contidas. Uma ameaça é uma possível violação da segurança."[14] Já os ataques são considerados como sendo «um ataque à segurança do sistema que deriva de uma ameaça inteligente que consiste numa tentativa deliberada de burlar os serviços de segurança e violar a política de segurança de um sistema.»[15]

A evolução na forma de lidar com as infraestruturas críticas resultou, também, na mudança em relação àqueles que as atacam, de forma que passa a ser demandado uma melhor instrução, conhecimento e habilidade por parte desses sujeitos.

Muitas vezes as investidas contra as infraestruturas críticas podem ser feitas de forma direta pelo próprio interessado, de acordo com o seu objetivo. Quando não realizada dessa forma, os sujeitos invasores atuam de maneira patrocinada, ou seja, agem em prol do interesse de terceiros. Esses outros interessados podem ter os mais diversos objetivos, podendo ser uma empresa tentando invadir o sistema de outra, um Estado em relação a outro ou em relação a uma empresa, os grupos ativistas ou de terrorismo, bem como aqueles que se interessam em invadir e vender o conteúdo hackeado.

3. A VULNERABILIDADE DAS INFRAESTRUTURAS CRÍTICAS

Cronologicamente, é importante frisar que, por muito tempo, diversas empresas, principalmente as multinacionais, mantiveram seus sistemas operacionais básicos restritos a prevenções de ataques casuais de vírus menos complexos ou atos semelhantes. Entretanto, à medida que foram surgindo os avanços nas áreas de segurança, percebeu-se que "os investimentos em segurança contra riscos cibernéticos devem-se às constantes mudanças na gestão das empresas, em especial à automatização dos Sistemas de Controle (SDSC – Sistema Digi-

---

tions Laboratory, v. 6, 2007. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.466.488&rep=rep1&type=pdf>. Acesso em: 14 maio 2018, p. 2.

14 Tradução Livre. "*The term "security" is used in the sense of minimizing the vulnerabilities of assets and resources. […]. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.*" Original em: ITU-T 1991. **Security architecture for Open Systems Interconnection for CCITT applications**. ITU-T Recommendation X.800. Disponível em: <http://www.itu.int/rec/T-REC-X.800-199103-I/e>. Acesso em: 18 jul. 2018, p. 34.

15 Tradução Livre. "*An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system*." Original em: SHIREY, Robert. 2000. ***Internet Security Glossary***. IETF RFC 2828. Disponível em: <https://tools.ietf.org/html/rfc2828>. Acesso em: 18 jul. 2018, p. 12.

tal de Supervisão e Controle)."[16] Dessa forma, apreende-se que o aumento da inclusão de sistemas automáticos propiciou que o próprio sistema robótico instalado fosse responsável por realizar todas as funções programadas, inclusive aquelas de prevenção e de defesa de possíveis erros advindos de fatores externos.

Só que, apesar de esses sistemas serem programados para operarem a si próprios, ainda assim, há a necessidade de alguma intervenção humana, dos raciocínios e conhecimentos técnicos, seja trabalhando previamente, paralelamente ou posteriormente às máquinas. Porém, apesar de toda a atuação em conjunto, grande parte da população a qual é designada nessas empresas de grande porte ainda não detém a conscientização devida e os preparos técnicos para atuarem em casos cada vez mais sofisticados de ataques.

Além desses fatos, grande parte das vulnerabilidades das infraestruturas decorrem do seu próprio sistema. Assim, existem dados relativos ao Brasil, Chile e México, que evidenciam que as vulnerabilidades, em sua maior parte, estão relacionadas às configurações erradas feitas nos sistemas, atrelando-se os problemas de versões e aplicações desatualizadas. Ocorre que esses problemas são, em verdade, influenciados por um risco maior[17], pois

> 60% das vulnerabilidades que expõem brechas poderiam afetar a confidencialidade das informações. 30% das vulnerabilidades representam uma ameaça contra a integridade, enquanto 10% delas são fragilidades que podem ser aproveitadas por ataques contra a disponibilidade de informações e serviços.[18]

Ademais, a junção das configurações com o aprimoramento técnico dos seus operadores ainda representa um meio termo do que se espera em relação ao devido controle desses sistemas, e principalmente no que toca ao sistema SCADA, que será explicado mais à frente.

---

16 L.S. **Revista Apólice**. *80% das empresas de energia já foram alvo de ataques cibernéticos*. Disponível em: <http://www.revistaapolice.com.br/2017/02/empresas-de-energia-ataques-ciberneticos>. Acesso em: 14 maio 2018, p. 01.

17 Trend Micro Incorporated. **Novo Relatório Sobre Segurança e Infraestruturas Críticas nas Américas**. Disponível em: <http://www.trendmicro.com.br/br/inteligencia-de-seguranca/pesquisa-e-analise/seguranca-infraestrutura-critica/index.html?mkt_tok=eyJpIjoiTjJKbU5HRTRNREprWlRaaCIsInQiOiJZNEpwa0V4Q2RmMXRtakVjV1kxbVVJM09MWjg5dnB0SE1QUzAxb0pSUnJ1OG40ZGQ0WHBrdHBpU1ZmQk9XaWF6UVpsUEpYTWt3a0luSEd4N1Zpd0tnOUI4d3YrM3BaWjQ2VUhcLytyV2o0T0U9In0%3D>. Acesso em: 14 maio 2018, p. 18.

18 Trend Micro Incorporated. **Novo Relatório Sobre Segurança e Infraestruturas Críticas nas Américas**. Disponível em: <http://www.trendmicro.com.br/br/inteligencia-de-seguranca/pesquisa-e-analise/seguranca-infraestrutura-critica/index.html?mkt_tok=eyJpIjoiTjJKbU5HRTRNREprWlRaaCIsInQiOiJZNEpwa0V4Q2RmMXRtakVjV1kxbVVJM09MWjg5dnB0SE1QUzAxb0pSUnJ1OG40ZGQ0WHBrdHBpU1ZmQk9XaWF6UVpsUEpYTWt3a0luSEd4N1Zpd0tnOUI4d3YrM3BaWjQ2VUhcLytyV2o0T0U9In0%3D>. Acesso em: 14 maio 2018, p. 18.

Logo, há que se afirmar que, ao mesmo tempo em que diversos países e governos tendem a otimizar o uso das informações tecnológicas em favor do aprimoramento de serviços essenciais a toda a sociedade, não há uma estabilidade nesse aprimoramento de informações.

Isso significa dizer que os usos e avanços de instrumentos cibernéticos têm a propensão de se aperfeiçoarem numa velocidade muito grande, sendo essa evolução passível de ser considerada rápida demais, ou seja, em questão de dias e, com isso, consequentemente, poderão vir a ser desconhecidos em suas novas formas de atuação. [19]

Assim, a vulnerabilidade em relação aos ataques cibernéticos será constante, tendo em vista a dinâmica de evolução e aprimoramento de técnicas e softwares, correlatos com a falta de preparo de uma nova política de defesa, se utilizando do conhecimento humano juntamente com os instrumentos/programas tecnológicos.[20]

Muito disso se deve à própria questão cultural, especialmente brasileira. O Brasil não é alvo de possíveis guerras ou ataques militares e, ainda assim, seus preparos e esforços são voltados para prevenção aos ataques clássicos, seja por meio terrestre, marítimo ou espacial.

O que acontece é que qualquer acontecimento grave que venha a causar danos à população, só ganha a visibilidade e atenção necessária por parte do Governo após o ocorrido e, mesmo assim, a população segue um padrão de sugestão de regras, e não aplicação de um regramento, de um dever impositivo de ter que atuar de maneira preventiva, pensamento que países desenvolvidos trazem diante das suas vulnerabilidades já detectadas.

3.1. A PLATAFORMA SCADA

Para compreender como ocorrem os ataques às infraestruturas críticas faz-se necessário explicar o que é o sistema/plataforma SCADA e o porquê dessa compreensão ser tão importante na discussão sobre os ataques cibernéticos a essas infraestruturas.

Partindo-se do pressuposto de que houve a substituição, nas indústrias, da mão de obra humana pela maquinaria, mais especificamente pelo maquinário dotado de automação. Houve uma mudança de perspectiva, assim, o controle dos sistemas, o monitoramento e a coleta de dados das CIs (*Critical Infraes-*

19 PINHEIRO, Fábio Ponte. **A Cibernética Como Arma de Combate**. Trabalho de Conclusão de Curso. Rio de Janeiro: Escola Superior de Guerra, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 25 jul. 2018, p. 20.

20 *Ibidem, loc. cit.*

tructures) ficaram a cargo de processos automatizados que requerem menor participação humana.[21] É a esse sistema de controle e de supervisão que se dá o nome de sistema SCADA (*Supervisory Control and Data Acquisition*).[22]

Assim, os sensores do sistema SCADA são responsáveis por reunir os dados em tempo real, ou seja, simultaneamente, sendo que essa sua função é realizada a partir de locais remotos; assim, após recolher esses dados o sistema SCADA será responsável por alimentar/transferir essas informações para um computador que executa softwares especiais. Dessa forma, o sistema operacional vai identificar, processar e registrar os dados, bem como quaisquer outras ocorrências na rede, fazendo com que, na presença de alguma ameaça, seja disparado um alarme sobre o risco e sobre a situação.[23]

Esse tipo de tecnologia é utilizada normalmente nas infraestruturas críticas, como usinas de energia, refinarias de petróleo, sistema de telecomunicações, transporte, água e instalações de controle de resíduos.[24]

3.2. *MALWARES* E SEUS IMPACTOS PARA ALÉM DO MUNDO CIBERNÉTICO

Os *malwares* são tipos de software que visam acessar um sistema operacional de modo a poder ter conhecimento do que se passa nesse disposto, podendo interagir seja de modo positivo ou negativo, sem que o respectivo dono perceba a ação. São tipos de *Malwares*, mais conhecidos popularmente, os Cavalos de Troia, *ransomware*, *phishing*, sequestradores de navegação, dentre outros. Eles interferem no sistema de terceiros, e fazem com que possam ter um relativo domínio sobre as máquinas de qualquer humano.[25]

Conforme já se sabe, os sistemas operacionais com que diversas empresas e indústrias trabalham o fazem com base em sistemas de controle de segurança,

---

21 CZINER, Krisztina et al. *Critical Information Infrastructure Protection in the Baltic Sea Area: The Case of TETRA*. **CIVPRO Working Paper, Helsinki University of Technology, Communications Laboratory**, v. 6, 2007. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?-doi=10.1.1.466.488&rep=rep1&type=pdf>. Acesso em: 14 maio 2018, p. 29.

22 BRANQUINHO, Marcelo Ayres et al. **Segurança de Automação Industrial e SCADA**. Elsevier Brasil, 2014. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=FVkaBQAAQBAJ&oi=fnd&pg=PT28&dq=INFRAESTRUTURAS+CRITICAS+SCADA&ots=-uk0j65wbs&sig=i6Ak5SOMalPjpllx7cNfktJrrWo#v=onepage&q=INFRAESTRUTURAS%20CRITICAS%20SCADA&f=false>. Acesso em: 03 ago. 2018, p. 1.

23 GEER, David. *Security of Critical Control Systems Sparks Concern*. **Computer**, v. 39, n. 1, p. 20-23, 2006. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1580377>. Acesso em: 14 maio 2018, p. 01.

24 GEER, David. *Security of Critical Control Systems Sparks Concern*. **Computer**, v. 39, n. 1, p. 20-23, 2006. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1580377>. Acesso em: 14 mai. 2018, p. 02.

25 Sistema Avast Free Antivírus. **Malware e anti-malware**. Disponível em: <https://www.avast.com/pt-br/c-malware>. Acesso em: 18 jun. 2018, p. 01.

patenteados por plataformas SCADA. Dessa forma, muitos protocolos foram criados há muitos anos e foram projetados com base nos riscos de segurança apresentados na época. Um desses sistemas é o chamado *Triconex Safety Instrumented System* (SIS), criado pela empresa *Schneider Eletric*[26], o qual é responsável por analisar os sistemas críticos, de modo que, caso perceba alguma iminência de dano, consiga tomar as medidas necessárias, a fim de consertar e prevenir essas possíveis falhas.

Informações decorrentes de um episódio ocorrido nos Estados Unidos, com base em um relatório produzido pelo *Fireeye*, uma empresa responsável por prevenir e proteger sistemas contra ataques cibernéticos, relata que esse *malware* invade o sistema se conectando ao SIS, que tem como função monitorar os desempenhos dos sistemas críticos e agir caso haja algum dano iminente, usando códigos similares ao deste sistema e, com isso, conseguindo atravessar essa barreira e modificando o comportamento das máquinas.[27]

Dessa maneira, através desses tipos de *softw*are, quase que "inofensivos", vários sistemas operacionais e máquinas industriais acabam recebendo outras informações, de maneira que isso pode refletir no modo de atuação e produção, em certos casos. Como exemplo as usinas elétricas, as quais mesmo não estando presentes os funcionários em determinados turnos da noite, continuam com o seu sistema programado para continuar trabalhando e funcionando, com base em protocolos previamente ajustados.

Um possível ataque desses a uma rede de energia, por exemplo, poderá refletir em produção muito maior de energia, produzindo uma corrente muito maior do que o normalmente distribuída, congestionamentos em redes elétricas, queimas em eletrônicos que dependam de energia, bem como possíveis acidentes elétricos.[28] De igual forma, caso haja um rebaixamento muito maior de voltagem de energia, isso pode vir a resultar em apagões, cada vez mais constantes, ou danos maiores do que aqueles que já se conhecem quando ocorrem no Brasil.

Com a facilidade desse acesso, e visando outros intuitos além de provocar danos, várias informações podem ser obtidas, seja dos seus administradores, funcionários ou até dos consumidores. Por outro lado, esse meio pode ser utilizado

26 JOHNSON, Blake. et al. ***Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.*** Disponível em: <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html/>. Acesso em: 18 jun. 2018, p. 1-3.

27 *Ibidem, loc. cit.*

28 PINHEIRO, Fábio Ponte. **A Cibernética Como Arma de Combate**. Trabalho de Conclusão de Curso. Rio de Janeiro: Escola Superior de Guerra, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 25 jul. 2018, p. 21.

para infiltrar e emanar vírus que possam chegar até seus consumidores, chegando a prejudicar, de diversos modos, cada receptor dessa energia modificada.

4. PROTEÇÃO DAS INFRAESTRUTURAS CRÍTICAS

Sabe-se que, apesar de não parecer tão evidentes as questões referentes aos regulamentos cibernéticos no Brasil, principalmente em relação às infraestruturas críticas, eles existem e precisam ser melhor discutidos e aprimorados, junto à realidade mundial.

Existe hoje, no Brasil, o decreto nº 6.703, que foi publicado pelo Presidente da República em 18 de dezembro de 2008, no qual foi aprovada a Estratégia Nacional de Defesa (END), sendo que, no ano de 2012, ela foi remodelada, para prever certas medidas que devem ser adotadas visando à segurança de algumas áreas, especialmente, em relação às infraestruturas críticas, estando "inclusos os serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações".[29]

Foi estipulado, então, que a responsabilidade de monitoramento dessas atividades, bem como dos seus riscos seria do Gabinete de Segurança Institucional da Presidência da República.[30] A responsabilidade pela aplicação dessa estratégia seria do Comandante do Exército que, além de gerir toda a política de atuação, controlaria os organismos que atuam em conjunto com essa política.[31]

Atrelado a esse desenvolvimento histórico, foi criada, também, a chamada Politica Cibernética de Defesa (PCD), através da Portaria Normativa Nº 3.389/MD de 21 de Dezembro de 2012, a qual é composta por diretrizes, objetivos e responsabilidades que atuam em conjunto com o decreto nº 6.703/08, sendo que a PCD também foi responsável pela criação do Sistema Militar de Defesa Cibernética (SMDC) nas Forças Armadas, o que foi muito importante, contudo, não estabeleceu mecanismos de cooperação internacional no âmbito estratégico no que concerne ao tratamento das vulnerabilidades cibernéticas.[32]

Assim, dentro desse contexto relativo à Política Cibernética, ao entender esses dois atos normativos, percebe-se que há muito mais perspectivas e plane-

29 JUNIOR, Alcyon. STREIT, Rosalvo. **Segurança Cibernética: Política Brasileira e a Experiência Internacional.** Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/864/795>. Acesso em: 06 ago. 2018, p. 110.

30 *Ibidem, loc. cit*.

31 JUNIOR, Alcyon. STREIT, Rosalvo. **Segurança Cibernética: Política Brasileira e a Experiência Internacional.** Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/864/795>. Acesso em: 06 ago. 2018, p. 110.

32 *Ibidem, loc. cit.*

jamentos de diretrizes de que alguma medida efetiva, sendo que se deve compreender que a segurança cibernética, nesse ponto, é a responsável por garantir o funcionamento perfeito das infraestruturas críticas.

Dessa forma, através da análise dessa Política de Defesa Cibernética, entende-se que há um projeto com boas intenções de concretizar e uniformizar essas medidas de segurança. Entretanto, como está previsto no ponto 3.2.7, o qual trata sobre *o objetivo em* "VII - definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber"[33], *v*erifica-se que a mera previsão e recomendação são indefinidas, como consta nos quesitos abaixo:

> c) definir atribuições e responsabilidades para o exercício das atividades relacionadas à Defesa Cibernética;
>
> d) elaborar propostas de criação e adequação de legislação federal, a fim de amparar as atividades de Defesa Cibernética;

Consequentemente, o que se espera dessa política brasileira de combate de futuros conflitos cibernéticos é que se criem regulamentos complementares, com base nos atuais.

Não há qualquer confiabilidade nas projeções feitas através dos decretos e portarias aprovadas nos últimos anos, tendo em vista que se trata de combates a ataques cibernéticos de maneira geral, não trazendo especificações devidas para cada área, o que acarreta probabilidade significativa de ocorrência de ataque, tampouco é realizado um recorte especifico para áreas de grande impacto nacional.

Vale ressaltar que, em relação à responsabilidade, o Brasil utiliza uma proposta de divisão que estabelece que a responsabilidade pela Segurança cibernética é do Gabinete de Segurança Institucional (GSI) da Presidência da República e que a responsabilidade pela Defesa Cibernética é do Sistema Militar de Defesa Cibernética (SMDC) e do Centro de Defesa Cibernética (CDCiber)[34], os quais são de responsabilidade do exército brasileiro e do Ministério da Defesa.

Dessa forma, a realidade na qual o Brasil se encontra hoje em termos de proteção cibernética, especificamente no que se refere às infraestruturas críticas, não é algo tão longe de ser concretizado. Entretanto, ainda faltam mecanismos apropriados e adequados, especialmente em relação às definições exatas quanto à responsabilidade e atuação de órgãos federais e/ou estaduais.

---

33 MINISTÉRIO DA DEFESA. Estado-Maior Conjunto das Forças Armadas. **Política Cibernética de Defesa.** 1ª edição, 2012. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf>. Acesso em: 06 ago. 2018.

34 JUNIOR, Alcyon. STREIT, Rosalvo. **Segurança Cibernética: Política Brasileira e a Experiência Internacional.** Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/864/795>. Acesso em: 06 ago. 2018, p. 124.

4.1. NECESSIDADE DE UM REGRAMENTO ESPECÍFICO

Conforme já mencionado, a segurança das infraestruturas críticas tem a sua previsão em decretos e portarias, mas apenas identificam e apontam as atitudes que o governo brasileiro entende que devem ser tomadas a fim de estabelecer esse objetivo. Assim, apesar de o ponto inicial ser da segurança cibernética de modo geral, faz-se necessário uma atenção maior quando se trata de infraestruturas críticas em razão do impacto e essencialidade que demandam um outro tratamento.

Sabe-se que foi normatizado, no âmbito jurídico brasileiro, que as áreas prioritárias de proteção das infraestruturas críticas seriam: energia, transportes, telecomunicações, água, finanças e informações.[35] Dessa forma, através de um setor responsável pertencente ao Sistema Brasileiro de Inteligência (SISBIN), a Agência Brasileira de Inteligência (ABIN), dentre diversas atribuições em relação às estratégias de defesa para possíveis ataques ao Estado como um todo, possui, também, a atribuição de atuar na defesa cibernética de diversas áreas importantes, estando incluídas nesse rol as infraestruturas críticas.[36]

Entretanto, entendendo a importância da relação desses setores com as Forças Armadas, vale repensar o modo de atuação dos mesmos, de modo que suas estratégias não sejam voltadas apenas para prevenção de futuras cyberguerras, e sim atuando de acordo com um modo específico, se adequando ao que a demanda pede.

Ou seja, deve-se atentar para algumas questões de grande relevância na caracterização e identificação desses futuros crimes, de maneira que, por não estar caracterizado um crime específico envolvendo esses elementos, a própria referência aos sujeitos praticantes desses atos enseja dúvidas, de modo que, pelo contexto dessas situações, tanto uma pessoa física quanto uma máquina poderiam ser "autores".[37]

O próprio espaço cibernético e a própria atuação de máquinas influenciam a continuidade desse modelo operacional, fazendo com que as mesmas continuem respondendo e atuando no lugar humano. Obviamente, quem provoca o possível dano, será uma pessoa física, seja através de um erro – no próprio programa da máquina, ou intencionalmente – quando o foco é o ataque, tendo em vista o que já foi abordado quando apresentados os novos sujeitos.

---

35 CARVALHO, Paulo Sergio de Melo. **A Defesa Cibernética e as Infraestruturas Críticas Nacionais**. Disponível em: <http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf>. Acesso em: 19 ago. 2018, p. 10.

36 *Ibidem*, p. 11.

37 PINHEIRO, Fábio Ponte. **A Cibernética Como Arma de Combate.** Trabalho de Conclusão de Curso. Rio de Janeiro: Escola Superior de Guerra, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 25 jul. 2018, p. 14.

Entretanto, há que se atentar para o fato de que a resposta ou resultado que se encaminhará para a análise pode ser proveniente de indicações de diversas redes de informação, IP de terceiros, ou juntamente com outros maquinários virtuais os quais venham a dificultar a devida identificação.

Além disso, nosso ordenamento brasileiro não institui qualquer departamento ou órgão específico que seja responsável por monitorar e armazenar informações acerca de possíveis invasões aos sistemas das infraestruturas críticas, de maneira que possa alertar sempre quando houver qualquer anormalidade. Atrelada a essa concepção, não há, no Brasil, uma obrigação legal de reportar às autoridades qualquer irregularidade nesses sistemas. Tal circunstância é influenciada, provavelmente, pela própria organização do modelo de controle - que é basicamente submetido às pessoas jurídicas, sem ligação direta com poder público.[38]

Muitos desses possíveis "ataques" não são divulgados, sendo influenciados, ainda, pelo receio de expor fragilidades dessas companhias ou por mero desconhecimento ou falta de informação adequada para esse tipo de procedimento.[39] Dessa forma, percebe-se que há uma grande falha do mecanismo de atuação e defesa em relação ao funcionamento das infraestruturas críticas, tendo em vista o seu arcabouço potencial, que demanda um regulamento à altura.

4.2. RELEVÂNCIA DO ASSUNTO PARA O CENÁRIO BRASILEIRO

No Brasil existem diversas infraestruturas críticas, sendo que, a depender do material com que lidam e da finalidade a que se destinam podem acarretar maiores ou menores danos e/ou riscos à população. Assim, quando tratamos de infraestruturas críticas, a mais conhecida da população, mesmo que sem adotar esse termo, são as usinas hidrelétricas.

Há várias usinas hidrelétricas no país, mas as principais em termos de produção energética são as de Belo Monte e de Itaipu. Além, das usinas hidrelétricas, ao se tratar do setor de energia há, ainda, em solo brasileiro, usinas nucleares localizadas em Angra dos Reis.

Eventual ataque cibernético a essas infraestruturas pode causar danos inimagináveis, desde a falta de eletricidade, conhecida como "apagão" até danos maiores, como danos ambientais e, principalmente, envolvendo a vida das pessoas que moram na circunscrição avaliada como sendo uma área de risco.

---

38 CARVALHO, Paulo Sergio de Melo. **A Defesa Cibernética e as Infraestruturas Críticas Nacionais**. Disponível em: <http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf>. Acesso em: 28 ago. 2018, p. 17.

39 PINHEIRO, Fábio Ponte. **A Cibernética Como Arma de Combate**. Trabalho de Conclusão de Curso. Rio de Janeiro: Escola Superior de Guerra, 2013. Disponível em: <http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 25 jul. 2018, p. 14.

Não é preciso ir muito longe para lembrarmos do que ocorreu no rompimento da barragem de Fundão, localizada em Bento Gonçalves, Minas Gerais, em 05 de novembro de 2015, que resultou numa devastação das cidades próximas, impactando, principalmente, o meio ambiente, posto que a quantidade de lama que vazou pode ser considerada proporcional ao Pão de Açúcar, que possui um volume de 48 milhões de metros cúbicos.[40]

Apesar de o evento não ter decorrido de um ataque cibernético, o exemplo é válido para demonstrar o poder destrutivo que eventual ataque a infraestruturas de grande porte pode causar. Nessa senda, é preciso recordar o caso *Stuxnet*, relativo a um ataque cibernético muito famoso.

O nome "*Stuxnet*" foi atribuído a um vírus detectado no ano de 2010, por uma empresa bielorrussa de antivírus chamada *VirusBlockAda*. Esse vírus é chamado de "*worm*", que significa "verme", em inglês. Ele teve como foco infectar vulnerabilidades presentes nos sistemas operacionais das infraestruturas críticas[41], sendo considerado o primeiro capaz de espionar e alterar a programação dos sistemas industriais.[42]

Assim, seu objetivo era atacar sistemas operacionais que utilizavam a plataforma SCADA, através de falhas no sistema Windows. Esse caso tem posição de destaque, pois o "*worm*" atacou usinas nucleares de enriquecimento de urânio no Irã, sendo que foi descoberto que ele também teve atuação em outros países, como Índia, por exemplo.[43]

Além desse caso, que ficou bastante conhecido, não são raros os ataques cibernéticos relatados em diversos países; temos conhecimento acerca desses casos por conta da obrigatoriedade de "*report*" pelo governo, para que o mesmo possa avaliar a situação e adotar as medidas necessárias. Nos Estados Unidos, por exemplo, parceiros dos setores público e privado presentes nos dezesseis

40 GLOBO – GI MINAS GERAIS. **Quantidade de lama que vazou de barragem em Mariana equivale a um 'Pão de Açúcar', diz presidente da Fundação Renova**. Disponível em: <https://g1.globo.com/mg/minas-gerais/desastre-ambiental-em-mariana/noticia/quantidade-de-lama-que-vazou-de-barragem-em-mariana-equivale-a-um-pao-de-acucar-diz-presidente-da-fundacao-renova.ghtml>. Acesso em: 02 out. 2018.

41 ZETTER, Kim. ***How Digital Detectives Deciphered STUXNET, The Most Menacing Malware in History***, 2012. Disponível em: <https://www.wired.com/2012/04/exploit-for-quantum-plc/>. Acesso em: 02 out. 2018.

42 WENDT, Emerson. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. **Revista Brasileira de Inteligência. Brasília: Abin**, v. 15, 2011. Disponível em: <http://www.abin.gov.br/conteudo/uploads/2018/05/RBI6-Artigo2-CIBERGUERRA-INTELIG%C3%8ANCIA-CIBERN%C3%89TICA-E-SEGURAN%C3%87A-VIRTUAL-alguns-aspectos.pdf>. Acesso em: 02 out. 2018, p. 24.

43 GLOBO – G1 TECNOLOGIA E GAMES. **Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 02 out. 2018.

setores de infraestruturas críticas americanas, juntamente com o governo, criaram um plano específico a respeito da segurança cibernética, tendo como foco as condições operacionais específicas presentes nessas infraestruturas críticas, bem como os riscos próprios de cada setor.[44]

À título de informação, somente no ano de 2016, foram reportados 59 incidentes no setor de energia elétrica nos EUA. Assim, apesar de ser fácil a compreensão de que a operação das infraestruturas críticas por diversos sujeitos (em âmbito federal, estadual e municipal) acrescenta uma maior complexidade no compartilhamento e divulgação de informações, urge salientar que, na eventualidade de algum ataque cibernético mais significativo, é preciso que sejam adotadas medidas legalmente aplicáveis, possibilitando que o setor do governo responsável pelo suporte da defesa atue das mais variadas formas, ajudando de forma remota ou até mesmo no local do dano.[45]

Ninguém está livre de sofrer algum ataque cibernético. A própria Agência Espacial Norte-Americana, considerada símbolo de desenvolvimento tecnológico, sofre ataques cibernéticos, principalmente por se caracterizar como um alvo difícil e atraente a ser conquistado. A NASA, apesar de investir mais de 1,5 bilhões de dólares, anualmente, em atividades diretamente relacionadas com TI (Tecnologia da Informação), e mais de 58 milhões de dólares somente em segurança, reportou 5.408 ataques cibernéticos num período de dois anos.[46] Esses dados são alarmantes e contribuem para aclarar a realidade que nos cerca.

Ainda não foi dada a devida atenção, no Brasil, a essas questões relativas à segurança cibernética no âmbito das infraestruturas críticas, e faz-se necessário prever e solucionar os problemas futuros dessa ordem, principalmente se levarmos em consideração que as indústrias petroquímicas lidam com produtos altamente perigosos.

O setor petroquímico brasileiro possui três polos: Mauá/SP, Triunfo/RS e Camaçari/BA; esse último está localizado a 50 km de distância a capital da Bahia, Salvador, e teve as suas atividades iniciadas no ano de 1978, sendo o primeiro polo petroquímico planejado do país, além de ser o "maior complexo industrial integrado do hemisfério sul, tendo mais de 50 empresas químicas,

44 White House. 2017. ***Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure***. Disponível em: <https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf>. Acesso em: 02 out. 2018, p.19.

45 *Ibidem, loc. cit*.

46 MARTIN, Paul K.; GENERAL, Inspector. Nasa cybersecurity: *An Examination of the Agency's Information Security.* **US House of Representatives**, 2012. Disponível em: <http://www.csri.info/wp-content/uploads/2012/08/HHRG-112-SY21-WState-PMartin-20120229-1.pdf>. Acesso em: 02 out. 2018.

petroquímicas e de outros ramos de atividades, como: celulose, metalurgia de cobre, têxtil, bebidas e serviços."[47]

Nos deteremos aqui sobre a situação do polo de Camaçari, que é o que representa maior risco para a população, por ser o maior polo da América Latina. Assim, cabe afirmar que essa área que está localizada próxima ao polo é uma área de risco. A população que mora nas proximidades deveria ser alertada sobre os possíveis riscos que estão correndo, principalmente porque é totalmente possível a ocorrência de um ataque cibernético.

Para que medidas preventivas e repressivas possam ser tomadas pelo Estado, cabe adotar normas que obriguem as empresas a relatarem os ataques que estão sofrendo para, assim, contar com o apoio estatal na solução de eventuais problemas técnicos que possam vir a afetar a vida das pessoas que estão no raio de alcance de um possível desastre originado de um ataque cibernético bem sucedido.

5. CONCLUSÃO

Com base no contexto atual de civilização, não há como negar que os ataques cibernéticos já fazem parte da realidade de uma parcela da sociedade. De algum modo, embora não expostos e divulgados de maneira eficiente, ainda sim, são fatos que tendem a crescer cada vez mais em diversos lugares do mundo, principalmente em países de alto grau de desenvolvimento.

Ao mesmo tempo em que são incentivados e aperfeiçoados os mecanismos tecnológicos em todo o mundo, paralelamente, os crimes cibernéticos também se qualificam, permitindo que ocorra expansão das suas áreas de ataque para além do meio virtual. É nesse contexto que as infraestruturas críticas acabam se tornando alvos e/ou meios que possibilitam atingir seus novos objetivos. Tendo em vista o potencial vital essencial que essas infraestruturas admitem ter, não se pode duvidar que se configuram como uma porta de fácil acesso para atingir diretamente quase a totalidade de uma população de uma região.

Assim, da mesma forma como se dá a importância de atualizações de software para as máquinas e instrumentos tecnológicos, a mesma deve ser gerenciada e voltada também para a sua própria prevenção. A sofisticação dos crimes está acompanhada da sofisticação das estruturas tecnológicas e

47 DE SANTANA, Lindaura Maria; HASENCLEVER, Lia; DE MELLO, José Manoel Carvalho. Capacitação Técnica e Competitividade na Petroquímica Brasileira nos anos 1990: O Caso de Camaçari-BA. **Revista Brasileira de Inovação**, v. 2, n. 1, p. 147-177, 2009. Disponível em: <https://www.researchgate.net/profile/Jose_Mello6/publication/47659076_Capacitacao_Tecnica_e_Competitividade_na_Petroquimica_Brasileira_nos_anos_1990_O_Caso_de_Camacari_-_BA/links/0deec5188df54975df000000.pdf>. Acesso em: 03 out. 2018, p. 150.

de proteção em questão, porém considerar apenas isso como mecanismo não está sendo mais suficiente.

Tendo em vista os acontecimentos, deixar apenas os setores privados com a responsabilidade de se prevenir e se proteger, torna essas atitudes, no mínimo, irresponsáveis. Desse modo, as parcerias entre o público e privado devem se manter, de modo a resguardar ao máximo a eficácia da seguridade e proteção nacional.

O mecanismo de "*report*", como uma ferramenta obrigatória no Brasil, seria um instrumento que faria uma diferença alarmante, de maneira a demandar a criação de um centro estadual de reportagem de ataques cibernéticos, de forma a atribuir ao Governo Estadual, através da atuação da sua Secretaria de Segurança Pública (SSP), a responsabilidade de fiscalização e ação diante dessas informações, seja através de medidas repressivas ou preventivas.

Esse protecionismo repercutiria positivamente, para toda a população, seja regional ou nacional, de maneira que, ao permitir que agentes públicos tomem ciência prévia do que vem acontecendo ou pode vir a acontecer em termos de atingir essas infraestruturas, os mesmos podem providenciar ações protetivas, a fim de garantir e resguardar a saúde, integridade física e mental de uma parcela da sociedade. Isso ocorreria através de avisos prévios de evacuações das pessoas que morassem próximas a esses locais passíveis de eventos catastróficos, avisos de cautela ao consumir ou ter acesso a algum produto que possa ter sofrido alguma interferência ou mudança decorrente de algum ataque, dentre outras situações, as quais perpassam por setores que visam atender a extremas necessidades da população.

Desse modo, a ação em conjunto com o Governo deve ser preservada e intensificada, assim como os mecanismos que cada setor responsável de infraestrutura crítica se obriga a gerir, atualizar e aprimorar, a fim de evitar e combater as iminências de pequenos e médios ataques, os quais, em um futuro próximo, podem vir a atingir dimensões desproporcionais em razão de profissionais do setor privado e do próprio setor público despreparados, ocasionando efeitos muito mais devastadores para toda a sociedade.

REFERÊNCIAS

ARAS, Vladimir. **Crimes de Informática: Uma Nova Criminalidade**. Jus Navigandi, Teresina, v. 5, 1998. Disponível em: <http://www.egov.ufsc.br:8080/portal/sites/default/files/anexos/13015-13016-1-PB.pdf>. Acesso em: 26 nov 2018

BARBIRATO, Alex. **A Verdade Sobre Bitcoins**. Disponível em: <https://cryptoid.com.br/destaques/verdade-sobre-bitcoins/>. Acesso em: 18 jul. de 2018.

BRANQUINHO, Marcelo Ayres et al. **Segurança de Automação Industrial e SCADA**. Elsevier Brasil, 2014. Disponível em: <https://books.google.com.br/books?hl=pt-BR&lr=&id=FVkaBQAAQBAJ&oi=fnd&pg=PT28&dq=INFRAESTRUTURAS+-CRITICAS+SCADA&ots=-uk0j65wbs&sig=i6Ak5SOMalPjpllx7cNfktJrrWo#v=onepage&q=INFRAESTRUTURAS%20CRITICAS%20SCADA&f=false> Acesso em: 03 ago. 2018.

CARVALHO, Paulo Sergio de Melo. **A Defesa Cibernética e as Infraestruturas Críticas Nacionais**. Disponível em: <http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf>. Acesso em: 19 Ago. 2018.

CZINER, Krisztina et al. *Critical Information Infrastructure Protection in the Baltic Sea Area: The Case of TETRA*. **CIVPRO Working Paper, Helsinki University of Technology, Communications Laboratory**, v. 6, 2007. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.466.488&rep=rep1&type=pdf>. Acesso em: 14 maio 2018.

DE SANTANA, Lindaura Maria; HASENCLEVER, Lia; DE MELLO, José Manoel Carvalho. Capacitação Técnica e Competitividade na Petroquímica Brasileira nos anos 1990: O Caso de Camaçari-BA. **Revista Brasileira de Inovação**, v. 2, n. 1, p. 147-177, 2009. Disponível em: <https://www.researchgate.net/profile/Jose_Mello6/publication/47659076_Capacitacao_Tecnica_e_Competitividade_na_Petroquimica_Brasileira_nos_anos_1990_O_Caso_de_Camacari_-_BA/links/0deec5188df54975df000000.pdf>. Acesso em: 03 out. 2018.

GEER, David. *Security of Critical Control Systems Sparks Concern*. **Computer**, v. 39, n. 1, p. 20-23, 2006. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1580377 >. Acesso em: 14 maio 2018.

GLOBO – G1 MINAS GERAIS. **Quantidade de lama que vazou de barragem em Mariana equivale a um 'Pão de Açúcar', diz presidente da Fundação Renova**. Disponível em: <https://g1.globo.com/mg/minas-gerais/desastre-ambiental-em-mariana/noticia/quantidade-de-lama-que-vazou-de-barragem-em-mariana-equivale-a-um-pao-de-acucar-diz-presidente-da-fundacao-renova.ghtml>. Acesso em: 02 out. 2018.

GLOBO – G1 TECNOLOGIA E GAMES. **Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia**. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 02 out. 2018.

JOHNSON, Blake. et al. Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. Disponível em: <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html/>. Acesso em: 18 jun. 2018.

JUNIOR, Alcyon. STREIT, Rosalvo. **Segurança Cibernética: Política Brasileira e a Experiência Internacional.** Disponível em: < https://revista.enap.gov.br/index.php/RSP/article/view/864/795>. Acesso em: 06 Ago. 2018.

L.S. **Revista Apólice**. *80% das empresas de energia já foram alvo de ataques cibernéticos*. Disponível em: <http://www.revistaapolice.com.br/2017/02/empresas-de-energia-ataques-ciberneticos>. Acesso em: 14 Maio 2018.

MARTIN, Paul K.; GENERAL, Inspector. Nasa cybersecurity: *An Examination of the Agency's Information Security*. **US House of Representatives**, 2012. Disponível em: <http://www.csri.info/wp-content/uploads/2012/08/HHRG-112-SY21-WState-PMartin-20120229-1.pdf>. Acesso em: 02 out. 2018.

MINISTÉRIO DA DEFESA. Estado-Maior Conjunto das Forças Armadas. **Política Cibernética de Defesa.** 1ª edição, 2012. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf>. Acesso em: 06 Ago. 2018.

NICKOLOV, Eugene. *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations*. **INFORMATION AND SECURITY**, v. 17, p. 105-119, 2006. Disponível em: <http://defencemanagement.org/system/files/17.07_Nickolov.pdf>. Acesso em: 14 maio 2018.

PEREIRA, António Martins. As Ameaças Transnacionais e a Segurança Interna. **Revista de Ciências Militares**, v. 2, n. 1, 2014. Disponível em: <https://s3.amazonaws.com/academia.edu.documents/33924580/As_Ameacas_Transnacionais_e_a_Seguranca_Interna_AMP.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1526340741&Signature=5Xc87dVfaXyFYWKf8uV%2FfA8VBpY%3D&response-content-disposition=inline%3B%20filename%3DAs_Ameacas_Transnacionais_e_a_Seguranca.pdf >. Acesso em: 14 maio 2018.

PINHEIRO, Fábio Ponte. **A Cibernética Como Arma de Combate**. Trabalho de Conclusão de Curso. Rio de Janeiro: Escola Superior de Guerra, 2013. Disponível em: http://200.143.206.219/images/Monografias/2013/PINHEIRO.pdf>. Acesso em: 25 jul. 2018.

SANTA CATARINA, Policia Civil. **Policia civil de SC é elogiada mundialmente pela solução rápida do caso de extorsão, mediante sequestro, com pagamento em moeda virtual**. Disponível em: <http://www.policiacivil.sc.gov.br/informacoes/noticias/38168-policia-civil-de-sc-e elogiadamundialmente-pela-solucao-rapida-do-caso-de-extorsao-mediante-sequestro-com-pagamento-em-moeda-virtual>. Acesso em: 18 jul. de 2018.

SHIREY, Robert. 2000. ***Internet Security Glossary***. IETF RFC 2828. Disponível em: <https://tools.ietf.org/html/rfc2828>. Acesso em: 18 jul. 2018.

SISTEMA AVAST ANTIVÍRUS. **Malware e anti-malware**. Disponível em: <https://www.avast.com/pt-br/c-malware>. Acesso em: 18 jun. 2018.

TREND MICRO INCORPORATED. **Novo Relatório Sobre Segurança e Infraestruturas Críticas nas Américas**. Disponível em: <http://www.trendmicro.com.br/br/inteligencia-de-seguranca/pesquisa-e-analise/seguranca-infraestrutura-critica/index.html?mkt_

tok=eyJpIjoiTjJKbU5HRTRNREprWlRaaCIsInQiOiJZNEpwa0V4Q2RmMXRtakVjV1kxbVVJM09MWjg5dnB0SE1QUzAxb0pSUnJ1OG40ZGQ0WHBrdHBpU1ZmQk9XaWF6UVpsUEpYTWt3a0luSEd4N1Zpd0tnOUI4d3YrM3BaWjQ2VUhcLytyV2o0T0U9In0%3D>. Acesso em: 14 maio 2018.

WENDT, Emerson. Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos. **Revista Brasileira de Inteligência. Brasília: Abin**, v. 15, 2011. Disponível em: <http://www.abin.gov.br/conteudo/uploads/2018/05/RBI6-Artigo2-CIBERGUERRA-INTELIG%C3%8ANCIA-CIBERN%C3%89TICA-E-SEGURAN%C3%87A-VIRTUAL-alguns-aspectos.pdf>. Acesso em: 02 out. 2018.

WHITE HOUSE. 2017. ***Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure***. Disponível em: <https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf>. Acesso em: 02 out. 2018.

ZETTER, Kim. ***How Digital Detectives Deciphered STUXNET, The Most Menacing Malware in History***, 2012. Disponível em: <https://www.wired.com/2012/04/exploit-for-quantum-plc/>. Acesso em: 02 out. 2018.

6

DA UBIQUIDADE COMPUTACIONAL PARA A REALIZAÇÃO DE CRIMES CIBERNÉTICOS

Aline Mª Proence Pereira Lopes[1]
e Guilherme Celestino Conceição Tadeu[2]

RESUMO: Este artigo é destinado à análise da computação ubíqua, perpassando pelo conceito, evolução histórica e os ramos da computação que foram fundamentais para a origem da onipresença computacional; logo em seguida, a fim de elucidar, apresentar as áreas de aplicações da ubiquidade computacional contemporânea que impactam o cotidiano das pessoas. Verifica-se que a eficiência tecnológica tornou a internet um novo meio para a prática de novos delitos que não eram previstos na legislação, que são os crimes cibernéticos, emergindo, assim, novos paradigmas para o Direito e a sociedade. Além disso, apresenta um estudo sobre o tratamento dado pelo Direito Penal brasileiro aos crimes cometidos com o auxílio dos sistemas computadorizados. Por fim, aborda como a utilização da Computação Ubíqua pode expor o indivíduo aos problemas éticos e de cunho criminoso, abordando também os crimes futuros que poderão afligir nossa sociedade, além da proposição de medidas necessárias que previnam e atenuem esse tipo de prática criminosa.

PALAVRAS – CHAVE: Computação ubíqua, direito penal, legislação, crimes cibernéticos, crimes futuros.

1 Bacharel em Direito pela Faculdade Baiana de Direito e Gestão.

2 Advogado.

1. INTRODUÇÃO

O progresso de novas tecnologias da informação tornou a internet um meio favorável para a prática de novos delitos, que não eram previstos na legislação, emergindo, assim, novos padrões para o Direito e a sociedade. Com a evolução da computação ubíqua, equipamentos já são projetados para realizarem as tarefas cotidianas e, cada vez mais, dispositivos inteligentes estarão conectados à rede mundial de computadores, trazendo inúmeros benefícios; é diante desse novo cenário, no qual a computação é onipresente, que o sujeito se torna mais exposto e vulnerável ao aparato tecnológico, sendo vítima de conduta ilícita e atos criminosos.

Sendo assim, o presente artigo apresenta como a computação ubíqua pode expor o indivíduo aos problemas éticos e de cunho criminoso e como o sistema estatal está disciplinando a nova criminalidade que nasceu com os progressos tecnológicos aplicados à internet e ao computador. Para tanto, fez-se uma breve exposição do conceito de computação ubíqua e sobre o processo que conduziu a computação alcançar a ubiquidade, uma vez que não há como discutir os novos entornos criminológicos por meio da internet sem compreender seu funcionamento.

Visando uma abordagem mais clara sobre o tema será exposto de maneira elucidativa as áreas de aplicações que impactam a atividade diária das pessoas, como: os projetos na educação, na medicina, nos automóveis, nos negócios e no ambiente interno de suas próprias casas, mediante a conectividade da internet e os diversos dispositivos eletrônicos.

Em seguida, serão analisadas as definições do que se convencionou titular, neste trabalho, de Crimes Cibernéticos, buscando determinar os limites conceituais desses delitos, além das legislações nacionais que tratam sobre o tema.

Por fim, serão expostas condutas que já são uma realidade e carecem de tipificação penal adequada no Brasil, bem como diversos exemplos de crimes que podem ser cometidos à medida que a Internet das Coisas se torna cada vez mais parte da realidade da vida das pessoas, ratificando o risco que essa tecnologia oferece. Muitos problemas engrossam a fila dos novos desafios que o direito e as autoridades enfrentarão.

TODO O EXPOSTO DEMONSTRA COMO A TECNOLOGIA SE DESENVOLVE VELOZMENTE AO PASSO QUE O DIREITO PENAL GANHA NOVOS ENTORNOS CRIMINOLÓGICOS COM A INTERNET SENDO INSTRUMENTO DE PRÁTICAS DELITUOSAS QUE PRECISAM SER REGULAMENTADAS E AMPARADAS PELO ORDENAMENTO JURÍDICO. DIANTE DISSO, CONSTATA-SE QUE A SOLUÇÃO SERIA A ATUALIZAÇÃO DOS CRITÉRIOS DE SEGURANÇA DAS REDES COMO UM TODO, ALIADA A UMA EDUCAÇÃO DIGITAL MAIS FORTE, SENDO IMPRESCINDÍVEL O DINAMISMO ENTRE AS NOVAS CONDUTAS EM MEIO VIRTUAL E AS NORMAS JURÍDICAS, OBJETIVANDO A SEGURANÇA JURÍDICA E SOCIAL.

Diante da complexidade do tema, não iremos exaurir a temática nesse momento, visto que é um assunto em constante metamorfose com distintas ramificações que vão além das apresentadas neste artigo. Todavia, o objetivo é, pelo menos, incitar a discussão e trazer mais esclarecimentos sobre o assunto.

2. COMPUTAÇÃO UBÍQUA

Para uma análise sobre os crimes derivados da invasão das coisas não pessoais, é necessário, primeiramente, termos uma ideia da arquitetura por trás da funcionalidade das coisas, para que então possamos compreender a ação dos criminosos.

Para tanto, não pode passar despercebida a ideia da ubiquidade computacional, tão (oni)presente em nosso cotidiano, fazendo seus usuários – de forma tendente ao imperceptível – serem cada vez mais dependentes da tecnologia em seu dia a dia.

2.1. Conceito

O termo Computação Ubíqua foi definido pela primeira vez pelo cientista Mark Weiser, através de seu artigo *The Computer for the 21st Century*[3] (O Computador do Século 21). A Computação Ubíqua surge como novo paradigma, em consequência do progresso das tecnologias de informação sem fio e móveis, e do uso da internet, possibilitando que o usuário tenha distintos dispositivos de comunicação a sua disposição para interação de forma integrada e onipresente. Para Mark Weiser, Computação Ubíqua é a integração contínua de computadores no mundo em que vivemos[4].

Segundo George Roussos, outro autor de relevante contribuição à ubiquidade computacional, o que distingue a computação ubíqua dos padrões prece-

3 WEISER, Mark. **The computer of 21st century. Scientific American**, jan. 1991. < Disponível em: http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>. Acesso em: 12 de maio de 2018

4 *Ibidem.*

dentes é a possibilidade de a computação e as comunicações (*wireless*) estarem integradas nos locais, objetos e, inclusive, nas pessoas, sendo factível interatuar livremente com os mecanismos digitais[5].

Sendo assim, define-se Computação Ubíqua como pequenos dispositivos computacionais distribuídos e integrados, portáveis ou colocados em ambientes, que fornecem serviços e informações em qualquer lugar e momento. Esses serviços são introduzidos na vida cotidiana de modo que sua presença seja invisível, utilizando linguagens corriqueiras do dia a dia, como fala, toque, audição, gestos, e dispensando o uso de teclado e mouse.

A própria etimologia da palavra remete a sua função. A palavra "ubíquo" é originária do latim "*ubiquu*", que significa "estar em todos os lados", dando a ideia de onipresença computacional. A computação ubíqua também é conhecida alternativamente como inteligência ambiental (pela forma de interagir com o ambiente), além dos nomes "*calm technologyI"*, "*things that think"* e "*everyware"*[6]*, que, em tradução livre, dão a ideia de, respectivamente, "tecnologia calma", "coisas que pensam" e "software onipresente"*.

Portanto, ubiquidade significa a onipresença da tecnologia nos espaços de atividade de forma imperceptível pelos seus usuários. Para alguns autores a computação ubíqua é o novo paradigma do século XXI; conforme abordado posteriormente, a fusão da computação pervasiva e móvel resulta na computação ubíqua, o que termina diferenciando esses três termos[7].

Os dispositivos ubíquos cooperam entre si para construir a inteligência no ambiente. A diversidade de dispositivos que constituem a Computação Ubíqua vai desde sensores até os *Mainframes*.

Para melhor compreensão, destrinchar os conceitos de pervasividade e mobilidade da computação é um exercício necessário.

2.1.1. Evolução histórica

Para descobrir como chegamos até o presente, a melhor forma é observar o passado. De forma sucinta, apresentaremos um breve histórico da computação ubíqua, consolidando os ramos da computação que foram fundamentais para a origem da onipresença computacional.

---

5 ROUSSOS, George. Ubiquitous Computing for Electronic Business. In: ROUSSOS, G. (Ed.). *Ubiquitous and Pervasive Commerce*: New Frontiers for Electronic Business. Springer, 2006.p1.

6 SILVA, Débora. Computação ubíqua: a informática no cotidiano das pessoas. Disponível em:<https://www.estudopratico.com.br/computacao-ubiqua-a-informatica-no-cotidiano-das-pessoas>. Acesso em: 01 de jul. 2018.

7 ARAUJO, Regina Borges. Computação Ubíqua, Princípios, Tecnologias e Desafios - XXI Simpósio Brasileiro de Redes de Computadores. 2003. http://twiki.im.ufba.br/pub/MAT570/LivroseArtigos/045_AraujoRB.pdf. Acesso em 12 de maio 2018.

Para tanto, especial atenção merecem as computações móvel e pervasiva, vistas como cruciais para o surgimento da ubiquidade computacional – e, às vezes, até mesmo confundidas.

2.2. Computação Móvel

A computação móvel é um ramo da computação que foi – e ainda é – usada no desenvolvimento da Ubiquidade. De conceito pacífico em doutrina, é descrita por Antônio Loureiro et al, como:

> Um novo paradigma computacional que tem como objetivo prover aos usuários acesso permanente à rede independente de sua localização física. Esse acesso pode ser feito utilizando um dispositivo computacional portátil como computadores laptops ou palmtops, ou telefones celulares, até diferentes tipos de ''Personal Digital Assistants" (PDAs)[8].

Sua origem advém dos tempos de guerra. Nos anos 40, a necessidade de comunicação nos campos de batalha levou à criação de radiotransmissores, considerados como os primeiros dispositivos eletrônicos móveis. Para isso, crucial foi o surgimento da tecnologia *Spread Spectrum*, uma técnica de codificação para a transmissão digital de sinais.

Ela foi originalmente desenvolvida durante a segunda guerra mundial, com o objetivo de transformar as informações a serem transmitidas num sinal parecido com um ruído radioelétrico, evitando, assim, a monitoração pelas forças inimigas. Nessa tecnologia, são enviadas frequências diferentes em tempos diferentes; uma maneira rústica de criptografar mensagens[9].Após esse período, a comunicação passou por grandes revoluções em seu *modus operandi*. Destacáveis aqui, para a mobilidade computacional, duas grandes fases da comunicação: O Projeto Iridium, e o surgimento do Wi-Fi.

O projeto Iridium foi lançado em 1995, visando à cobertura terrestre de satélites de baixa órbita. Esse projeto foi um consórcio dirigido pela empresa norte-americana Motorola, que possuía, à época, um sofisticado sistema de telecomunicações, baseado numa grande e complexa constelação formada por 66 satélites "LEO" ou de órbita polar baixa. O objetivo aqui era o de fornecer um serviço mundial digital de telecomunicações por meio de dispositivos portáteis,

8 LOUREIRO, Antônio AF et al. Comunicação ao Sem Fio e Computação ao Móvel: Tecnologias, Desafios e Oportunidades. Disponível em: <https://homepages.dcc.ufmg.br/~loureiro/cm/docs/jai03.pdf>-. Acesso em 24 de jun. 2018.

9 SANTANA, Reinaldo Costa. Computação móvel, histórico da evolução. **São Paulo**, 2008. Disponível em:<http://grenoble.ime.usp.br/~gold/cursos/2008/movel/mono/HistoricoComputacaoMovel.pdf>. Acesso em 03 de jul. 2018.

e foi primaz para os moldes da comunicação e tecnologia que conhecemos hoje, onde os satélites são fundamentais para a mobilidade da internet[10].

Já o Wi-Fi surgiu nos anos 2000 com os seus primeiros "*hot spots*". Assim, foram criadas áreas públicas onde era possível acessar a Internet por meio das redes que obedecessem ao padrão de protocolo "IEEE 802.11". A Western Electrical Contractors Association (WECA) lançou o selo Wireless Fidelity (Wi-Fi) para os fabricantes que aderissem às 12 especificações necessárias para o padrão de protocolo de rede em seus produtos, onde o sucesso foi tão grande que mais tarde o termo Wi-Fi tornou-se um sinônimo de uso abrangente das tecnologias IEEE 802.11[11].

Assim, notamos que a computação móvel tem como sua principal característica a possibilidade de transferir o espaço físico do terminal de acesso, e mesmo assim continuar conectado, não necessitando limitar-se a estar preso em um local específico para esse fim. Entende-se que ela dá mobilidade aos dispositivos computacionais e aos serviços associados aos mesmos. O mecanismo de acesso à rede computacional ganha liberdade e acompanha o usuário, não se restringindo a um espaço físico fixo. É o caso visto hoje em *notebooks*, *smartphones*, *tablets* e outros exemplos.

2.3. Computação Pervasiva

A computação pervasiva é a parte da computação que cuida da interação do sistema com o meio ambiente ao qual ele está acoplado. Dos sensores que captam a temperatura externa e acionam o ar condicionado de forma automática, até os que captam a qualidade do sono – e acionam a emergência em caso de necessidade[12], todos eles compõem a pervasividade computacional.

Ela também está relacionada à perceptividade dos sistemas computacionais pelo usuário. Isso implica dizer que há uma preocupação desse ramo computacional em ser cada vez menos percebido pelos seres humanos. Você usa sem se preocupar com o *hardware*, o *software*, o sistema elétrico e os dados transmitidos; apenas configura a temperatura que deseja, por exemplo, e o sistema cuidará de ajustar pra climatização desejada[13].

---

10 Ibidem.

11 Wi-Fi Alliance. Disponível em <https://en.wikipedia.org/wiki/Wi-Fi_Alliance>. Acesso em 15 de jul. 2018.

12 VENTURA, Felipe. Cama inteligente monitora seu sono para ajustar o colchão e sugerir novos hábitos. Gizmodo Brasil,2016. Disponível em:< https://gizmodo.uol.com.br/cama-inteligente-ces-2016/>. Acesso em 27 de julho de 2018.

13 DREY, Ramiro Fetzne. Definição e princípios da Computação Ubíqua. **TI especialistas,2015**. Disponível em:<https://www.tiespecialistas.com.br/definicao-e-principios-da-computacao-ubiqua/>. Acesso em:27 de julho de 2018.

Como diz Regina Borges de Araújo:

> O computador tem a capacidade de obter informações do ambiente no qual ele está embarcado e utilizá-lo para dinamicamente construir modelos computacionais, ou seja, controlar, configurar e ajustar a aplicação para melhor atender as necessidades do dispositivo ou usuário. O ambiente também pode e deve ser capaz de detectar outros dispositivos que venham fazer parte dele. Desta interação surge a capacidade de computadores agirem de forma 'inteligente' no ambiente no qual nos movemos, um ambiente povoado por sensores e serviços computacionais[14].

Logo, temos que a computação pervasiva é a utilização da computação, unindo-a aos chips de diversos aparelhos, expandindo conectividade para além dos computadores pessoais, tais como: eletrodomésticos, carros, roupas, casas inteligentes com sensores de controle de luminosidade, temperatura, entre outros.

2.4. Computação Ubíqua

A junção desses paradigmas computacionais resulta na computação ubíqua, tornando a utilização do dispositivo móvel o mais imperceptível para o usuário[15].

O conceito de ubiquidade sozinho, não inclui mobilidade, mas os aparelhos ubíquos podem ser considerados móveis, a partir do momento que podem ser encontrados e usados em qualquer lugar. Tecnologicamente, a ubiquidade pode ser definida como a habilidade de se comunicar em qualquer hora e em qualquer lugar via aparelhos eletrônicos espalhados pelo ambiente[16].

Por fim, a Computação Ubíqua tem como características a pró-atividade, diversidade, descentralização, onipresença, imperceptibilidade, conectividade e naturalidade. Essas características são necessárias para uniformização dos dados e protocolos de comunicação para alcançar a conectividade sem prejuízo da operação onde quer que esteja o usuário[17].

---

14 ARAÚJO, R. B. (2003). Computação Ubíqua: Princípios, Tecnologias e Desafios. In: XXI Simpósio Brasileiro de Redes de Computadores. (Org.). 1 ed. Natal – RN: SBRC2003, p.45 – 115.

15 SILVA, Everton et al. Computação Ubíqua–Definição e Exemplos. **Revista de Empreendedorismo, Inovação e Tecnologia**, v. 2, n. 1, p. 23-32, 2015. Disponível em:< https://seer.imed.edu.br/index.php/revistasi/article/view/926 >. Acesso em: 20 de abril de 2018.

16 SANTAELLA, Lucia. **Comunicação Ubíqua - Repercussões na Cultura e na Educação.** São Paulo: Paulus, 2013.

17 KAHL, Marcelo; FLORIANO, Diogo. **Computação ubíqua, tecnologia sem limites**. Vale do Itajaí SC,2012. Disponível em:<http://www.ceavi.udesc.br/arquivos/id_submenu/387/diogo_floriano_marcelo_kahl_computacao_ubiqua.pdf>. Acesso em: 10 de maio 2018.

A Computação Ubíqua possui inúmeros fatores que podem ser explorados; ela contribui para determinadas atividades do cotidiano se tornarem mais simples e ágeis. A seguir, são apresentadas aplicações da computação ubíqua.

2.4.1. Ubiquidade computacional contemporânea

Essa tecnologia admite uma série de aplicações em objetos do cotidiano, facilitando sua ligação com o ambiente digital. A tendência é que, dada a velocidade da evolução das tecnologias digitais, a computação ubíqua está cada dia mais presente no dia a dia da população urbana, de tal maneira que muitas vezes passa despercebida, sendo empregada em atividades cotidianas e trazendo impactos em praticamente todos os setores da vida social e pessoal, mesmo daqueles que jamais usaram computador[18].

Dentre as áreas de aplicações que impactam a atividade diária das pessoas estão projetos na educação, na medicina, nos automóveis, nos negócios e no ambiente interno de suas próprias casas, mediante a conectividade da internet e os diversos dispositivos eletrônicos heterogêneos[19].

2.4.2. Na medicina

Na medicina, uma das grandes inovações é a chamada *Ipill,* a pílula inteligente da *Philips* que possibilita colocação exata do medicamento no local onde ele deve ser liberado no organismo. Também se destaca o hospital virtual, que se estende para casa dos pacientes e lugares onde estão sendo monitorados e comunicam-se via *wireless* com outros médicos para auxiliar nas tomadas de decisões[20].

No âmbito da insuficiência cardíaca, o modelo *UbHeart* faz um diagnóstico prévio usando as informações de sensores, onde um alerta é encaminhado ao paciente quando ocorre situação de risco, comunicando aos responsáveis pelo paciente e ao hospital que aciona o médico[21]. Dispositivos protéticos, como a mão biônica; marca passos com *wi-fi*; variedade de dispositivos médi-

---

18 PINHEIRO, Mauro; SPITZ, Rejane. **O design de interação em ambientes de ubiqüidade computacional**. In: Congresso Internacional de Design da Informação. 2007. Disponível em:<http://www.academia.edu/801383/O_design_de_intera%C3%A7%C3%A3o_em_ambientes_de_ubiq%C3%BCidade_computacional >. Acesso em: 05 de maio 2018.

19 SILVA, Everton et al. Computação Ubíqua–Definição e Exemplos. **Revista de Empreendedorismo, Inovação e Tecnologia**, v. 2, n. 1, p. 23-32, 2015. Disponível em:< https://seer.imed.edu.br/index.php/revistasi/article/view/926 >. Acesso em: 20 de abril de 2018.

20 MIKA, Niclas. Philips desenvolve "pílula inteligente". **G1,2008**. Disponível em:<http://g1.globo.com/Noticias/Ciencia/0,,MUL858085-5603,00-PHILIPS+DESENVOLVE+PILULA+INTELIGENTE.html>. Acesso em: 05 de maio 2018.

21 Rocha, C. L., Costa, C. A., Righi, R. R. ***Um modelo para monitoramento de sinais vitais do coração baseado em ciência da situação e computação ubíqua.*** VII Simpósio Brasileiro de Computação Ubíqua e Pervasiva, Pernambuco, 2015.

cos implantáveis, como desfibriladores, bombas de insulina, implantes coleares e neuroestimuladores, tomógrafos, raio x, bombas intravenosas, dispositivos terapêuticos; pernas robóticas e órgãos biônicos implantáveis, como o pâncreas biônico, exoesqueletos ou robôs vestíveis, entre outros avanços tecnológicos[22].

2.4.3. Educação

No campo educacional um dos primeiros projetos lançados foi a *Classroom,* "que grava as aulas e possibilita buscar materiais e seções da aula, através de interfaces multimídias customizadas pelos próprios docentes[23]". Há também o projeto *M-SEA,* que adequa o ambiente às características individuais dos alunos, disponibilizando para cada um sugestão de sequência compatível ao seu perfil e nível de conhecimento[24].

2.4.4. Habitação

Já no âmbito residencial temos as *Smart Houses*, que são as casas inteligentes, onde o ambiente é controlado de forma harmônica: controle de luminosidade dos ambientes de acordo com seu uso, controle dos principais equipamentos da casa, controle de temperatura, chave digital e biométrica, sensor de incêndio entre outros. Os equipamentos e eletrodomésticos são programados para pensar de acordo com a vontade de seus usuários[25]. Há, também, a *Quietcare,* projetada para monitorar as atividades domésticas de quem precisa de acompanhamento médico constante. Assistentes virtuais conectados com outros aplicativos cuidam de detalhes domésticos, lembram reuniões e alertam o morador usuário sobre chuva. Destacam-se também as geladeiras que detectam os alimentos que faltam e criam uma lista para ser acessada no aplicativo do *smartphone* ou do relógio[26].

---

22 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.p. 279-285.

23 Abowd, G.D. *Classroom 2000:* ***An experiment with the instrumentation of a living educational environment.*** IBM Systems Journal, v. 38, 1999.

24 Piovesan, S, D. et al. **Modelagem de um Framework para M-Learning**. In: *XXI Simpósio Brasileiro de Informática na Educação*, Paraíba, Brasil, 2010. PERTMED - Sistema de TeleMedicina Móvel, disponibilizando a informação onde ela é necessária. Disponível em:<http://pertmed.wkit.com.br/pertmed/doku.php>. Acesso em 12 de maio 2018.

25 SILVA, Everton et al. Computação Ubíqua–Definição e Exemplos. **Revista de Empreendedorismo, Inovação e Tecnologia**, v. 2, n. 1, p. 23-32, 2015. Disponível em:< https://seer.imed.edu.br/index.php/revistasi/article/view/926 >. Acesso em: 20 de Abril de 2018.

26 RODRIGUES, Mauro Pinheiro. PINHEIRO, Mauro. **Design de interação e computação pervasiva: um estudo sobre mecanismos atencionais e sistemas de informação ambiente**. 2011.Tese de Doutorado, Programa de Pós-graduação em Design, PUC-Rio. Disponível em: < https://www.maxwell.vrac.puc-rio.br/21718/21718_1.PDF >. Acesso em:20 de abril.2018

Válido ressaltar que o ambiente inteligente é o conjunto de tecnologias que trabalha de maneira integrada, ativando instruções ou respondendo comandos pré-programados, mesmo sem instruções explícitas do usuário, evitando que necessite ir até o computador ou dispositivos, fazendo com que diversos dispositivos funcionem a distância.

2.4.5. Automóveis

No campo automotivo, o setor é atrativo para a Computação Ubíqua, visto que os dispositivos de comunicação estão integrados nos veículos e utilizam as fontes de energia do mesmo[27]. As aplicações no âmbito automotivo têm se expandido para além de ouvir música e assistir a filmes.

Hoje, os carros têm computadores de bordo - que são as unidades de controle eletrônico - gerenciando o motor do automóvel, o piloto automático, freios ABS, ar-condicionado, sistema de transmissão, entretenimento, sistema de travamento, navegação, acionamento de *airbag*, monitoramento de combustível etc.

Algumas montadoras de veículos irão lançar, até 2020, veículos totalmente autônomos. A maior proponente dessa tecnologia tem sido a *google*, cujos carros autônomos de teste já circulam; e a *Uber*, que tem automóveis circulando em fase de teste. A maior parte dos automóveis autônomos são fabricados com sensores de radar e de *LIDAR* (sigla em inglês para Light Detection And Ranging), que utilizam *lasers* para detectar barreiras em torno do veículo[28].

Há um cenário próspero em termos de computação ubíqua, proporcionando novas experiências e avanços em todas as áreas, se integrando e auxiliando nas diversas tarefas cotidianas, contudo, com o aspecto de segurança em evidência, visto que qualquer dispositivo pode ser hackeado, com consequências imprevisíveis.

3. ESTUDO DOS CRIMES

A era digital vem acompanhada do progresso de novas tecnologias da informação e toda essa eficiência tecnológica tornou a internet um meio propício para a prática de novos delitos, que não eram previstos na legislação, emergindo novos paradigmas para o Direito e a sociedade. De acordo com o Professor Irineu Francisco Barreto Junior:

---

27 Herrtwich, R. G. **Ubiquitous Computing in the Automotive Domain**. Proceedings of the Pervasive Computing – First International Conference, 2002.

28 Indústria de carros autônomos enfrenta problemas após acidente com Uber. **Exame, 2018**.Disponível em:<https://exame.abril.com.br/tecnologia/industria-de-carros-autonomos-enfrenta-problemas-apos-acidente-com-uber/>. Acesso em: 20 de abril 2018.

> Com o advento da Internet e da Sociedade da Informação, surgiu uma nova modalidade de crimes cometidos no espaço virtual da rede através de e-mails (correio eletrônico), web sites (sítios pessoais, institucionais ou apócrifos) ou mesmo ocorridos em comunidades de relacionamento na Internet. As transações comerciais eletrônicas, envolvendo compras que exigem a identificação do número de cartão de crédito, as transações bancárias, que solicitam registro de dados referentes às contas correntes bancárias, além do uso de senhas e demais mecanismos de segurança, assim como a profusão de novas modalidades relacionais mantidas em sociedade, através da Internet, propiciaram o surgimento de novas modalidades de crimes na web, batizados de crimes virtuais[29].

As condutas de cunho criminoso por meio da internet possuem muitas terminologias. Neste estudo, optamos pela mais utilizada atualmente (crimes cibernéticos), por entendermos a abrangência mais adequada aos crimes cometidos virtualmente[30].

Nos crimes cibernéticos, assim como nos crimes comuns, a conduta deve ser típica, antijurídica e culpável, entretanto, cometida contra ou com a utilização dos sistemas da informática.

Para Fabrizio Rosa,

> Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.31

Constata-se, portanto, que a criminalidade informática é responsável pelo surgimento de novos comportamentos ilícitos praticados com o auxílio de um computador, redirecionamento de facções criminosas e associação de novos núcleos de práticas tecnológicas para cometer crimes[32].

---

29 BARRETO Junior, Irineu. Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica. *In*: PAESANI, Liliana Minardi (Coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007. p. 71.

30 CRESPO, Marcelo Xavier de Freitas. ***Crimes Digitais***. São Paulo: Editora Saraiva, 2011, p. 46.

31 ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002. p. 53.

32 CAMARGO SANTOS, Coriolano Alberto de Almeida; FRAGA, Ewelyn Schoots. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico**. .ed.SãoPaulo.OAB/SP, 2010.Disponível em:< http://www.oabsp.org.br/comissoes2010/direito-eletronico-crimes-alta-tecnologia/livro-sobre-crimes-eletronicos/livro.pdf/download+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em 10 jul. 2018.p.09

3.1 TIPOLOGIA

Como relatado, a internet tornou-se um ambiente para o cometimento de novos crimes, até então não previstos na legislação e, além disso, é instrumento para a prática de condutas ilícitas já tipificadas, que atualmente podem ser executadas através do sistema de informática.

Não há consenso na doutrina quanto aos crimes cibernéticos; Ivette Senise Ferreira, Vicente Greco Filho e Damásio os classificam como crimes digitais próprios e impróprios. Os crimes cibernéticos próprios são cometidos contra bens jurídicos informáticos, e os crimes impróprios, condutas exercidas contra os bens jurídicos tradicionais por meio da internet[33].

Nas palavras de Vicente Greco Filho:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador do resultado morte, qualquer que tenha sido o meio ou a ação que o causou[34].

Segundo Damásio Evangelista de Jesus, os crimes próprios são praticados por computador e se realizam ou se consumam no meio eletrônico. Neles, o objeto jurídico tutelado será a titularidade das informações, a segurança dos sistemas, integridade dos dados, dos periféricos e das máquinas. Os impróprios são aqueles em que o agente utiliza o computador como meio para causar resultado naturalístico, lesando ou ameaçando outros bens, diversos da informática[35].

Já no dizer de Luiz Flávio Gomes, os crimes virtuais subdividem-se em: crimes por meio do computador (este, instrumento para atingir o objetivo pretendido) e contra o computador. O uso ilícito do computador ou de um sistema informático, será o meio para a consumação do crime-fim[36].

---

33 CRESPO, Marcelo Xavier de Freitas. ***Crimes Digitais***. São Paulo: Editora Saraiva, 2011. p. 60.

34 GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim IBCCRIM, v. 8, 2000, p. 95.

35 JESUS, Damásio E. de**. Manual de Crimes Informáticos**. 1 ed. São Paulo: Saraiva, 2016.1 ed. p.50-52.

36 GOMES, Luiz Flávio. Crimes informáticos. 10 dez. 2000. Disponível em:< http://www.ibccrim.org.br>. Acesso em: 14 jul. 2018.

Para classificar os crimes cibernéticos, ainda que não seja consenso na doutrina, devem-se considerar as condutas tipificadas no ordenamento jurídico, atualmente cometidas com o auxílio da tecnologia, como também aquelas práticas cujos bens jurídicos atingidos são somente os sistemas informatizados e não são tipificadas no ordenamento brasileiro[37].

Portanto, diante da diversidade de categorizações, adotamos a mais utilizada pela doutrina brasileira que classifica os crimes cibernéticos como: "condutas perpetradas contra um sistema informático (crimes próprios) e condutas perpetradas contra outros bens jurídicos não-computacionais (crimes impróprios) [38]".

3.1.1. Instrumentos de proteção no sistema jurídico

Com o advento da internet, o crescimento das inovações tecnológicas, vislumbramos o aumento da criminalidade neste meio, surgindo novas condutas delitivas, demandando respostas do operador do direito. Nesse contexto, verifica-se a necessidade de uma legislação penal para a proteção de bens jurídicos informáticos e de outros que possam ser ofendidos por meio de computadores.

Para Ivette Senise Ferreira, a crescente informatização de variadas atividades desenvolvidas na sociedade, colocou novas ferramentas nas mãos dos delituosos, surgindo a cada dia novas categorias de lesões aos mais diversos bens que compete ao Estado tutelar. Essa velocidade tecnológica possibilitou a formação de uma criminalidade exclusiva da informática, cuja propensão é aperfeiçoar os seus métodos de execução[39].

No Brasil, de acordo com os princípios constitucionais da reserva legal e da legalidade previstos no art. 5º, XXXIX da Constituição Federal Brasileira de 1988[40], é obrigatório previsão legal para punição de uma conduta proibida; sendo assim, condutas que não estão na lei não são consideradas crimes. E o Código Penal Brasileiro, no seu artigo 1º, ratifica essa previsão, ao asseverar: "Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal[41]".

---

37 MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova – A investigação criminal em busca da verdade**. Curitiba: Juruá Editora, 2012. p. 60.

38 CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011. p. 62.

39 FERREIRA, Ivete Senise. *A criminalidade informática*. In Direito & internet: aspectos jurídicos relevantes. Bauru: Edipro, 2000, p. 207.

40 CF/88, art. 5º, XXXIX: "Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 jul. 2018.

41 BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 20 agosto 2018.

Até o ano de 2012, os crimes cibernéticos próprios não eram punidos porque não havia qualquer legislação no nosso ordenamento jurídico para puni-los. Já em relação aos crimes virtuais impróprios, a legislação penal existente permitia sua punição, posto que eram crimes já tipificados no ordenamento brasileiro, com a peculiaridade de o computador ser o meio para cometer o crime. No entanto, em consequência de alguns fatos, como os ataques de negação de serviço a sites do governo brasileiro que saíram do ar, e a divulgação na internet de fotos da atriz Carolina Dieckmann, roubadas de seus arquivos pessoais por *hackers*, no ano de 2012, foram sancionadas e promulgadas a lei 12.735/12[42] (conhecida como Lei Azeredo), que trata da necessidade de instalação de órgãos investigativos especializados, e a lei 12.737/12[43] (conhecida como "Lei Carolina Dieckmann), pela qual foram incluídos o tipo penal invasão de dispositivo informático, no seu art. 154-A[44], e a regra da ação penal para esse crime, prevista no art. 154-B[45], ambos no Código Penal Brasileiro.

A lei 12.737/12, além de incluir esses dois dispositivos citados acima, alterou a redação dos artigos 266 e 298 do Código Penal Brasileiro. No tipo penal do artigo 266[46] passou a abranger serviços telemáticos ou de informação de

---

42 BRASIL. Lei nº12.735, de 30 de novembro de 2012.Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 20 agosto 2018.

43 BRASIL. 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 >. Acesso em: 20 de agosto 2018.

44 "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. §1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. §2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. §3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. §4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. §5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.".

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

46 Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

utilidade pública. Já no artigo 298[47] que prevê falsificação de documento particular, a lei inseriu a equiparação do cartão de crédito ou débito a documento particular. Assim, devido às alterações e inclusões realizadas pela lei, todas essas condutas passaram a ser punidas.

No ano de 2014, mais uma lei foi sancionada, a Lei 12.965/2014[48], oficialmente chamada de Marco Civil da Internet, a qual estabelece princípios, garantias, direitos e deveres para os usuários da internet no Brasil. O Marco Civil da Internet foi um grande progresso para o país, pois instituiu um rol de direitos fundamentais a serem respeitados na rede em conjunto com os que já existiam no mundo físico e estabeleceu diversos princípios reguladores para o exercício da internet para proteger o usuário e para a conservação das atividades na rede. O Marco passou a discriminar algumas obrigações para quem atua no mundo digital, como respeito ao fluxo de dados através da neutralidade da rede, guarda de dados e à manutenção da privacidade do usuário. Em 11 de Maio de 2016, a ex-Presidenta Dilma publicou o Decreto nº 8.771[49], o qual veio para complementar a Lei do Marco Civil que, conforme seu artigo 1º, trata:

> [...] das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indica procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelece parâmetros para fiscalização e apuração de infrações contidas na Lei no 12.965, de 23 de abril de 2014.

Verifica-se que, além dessas legislações citadas, tem-se a Lei nº 9.296/1996[50], que disciplinou a interceptação do fluxo de comunicações em sistemas de telemática e informática ; Lei nº 9.609/1998[51], que trata da proteção da propriedade intelectual de programa de computador e sua comercialização no Brasil; a Lei nº 9.983/2000[52], tipificou os crimes de inserção de dados falsos, modifica-

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

48 BRASIL. 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 >. Acesso em 20 de agosto 2018.

49 BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm >. Acesso em 20 de agosto 2018.

50 BRASIL. Lei nº 9.296, de 24 de Julho 1996. Disponível em:<http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em 20 de agosto 2018.

51 BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em 20 de agosto 2018.

52 BRASIL. Lei nº 9.983. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm>. Acesso em: 20 de agosto 2018.

ção ou alteração não autorizada de sistema de informações da Administração Pública e divulgação, sem justa causa, de informações sigilosas ou reservadas, definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.; a Lei nº 11.829/2008[53], que combate a pornografia infantil na internet; a Lei nº 12.034/2009[54], que delimita durante as campanhas eleitorais os direitos e deveres dentro da rede mundial de computadores; e a Lei nº 10.764/2003[55], que alterou o artigo 241[56] do Estatuto da Criança e do Adolescente.

Isto posto, aplica-se as normais processuais previstas genericamente no Código de Processo Penal e em leis especiais nas infrações penais com emprego de informática, já que no ordenamento jurídico não existem normas próprias de ordem processual dispostas em lei.

Diante da ausência de legislação própria, afiança-se que, na maioria dos exemplos de condutas delituosas virtuais que podemos imaginar, os infratores eletrônicos serão punidos com base nos tipos já previstos em lei. Nesse contexto, Fernando de Almeida Pedroso assevera que:

> Não basta, consequentemente, que o fato concreto, na sua aparência, denote estar definido na lei penal como crime. Há mister corresponda à definição legal. Nessa conjectura, imprescindível é que sejam postas em confronto e cotejo as características abstratas enunciativas do crime com as características ocorrentes no plano concreto, comparando-se uma a uma. Se o episódio a todas contiver, reproduzindo com exatidão e fidelidade a sua imagem abstrata, alcançará a adequação típica. Isso porque ocorrerá a subsunção do fato ao tipo, ou seja, o seu encarte ou enquadramento à definição legal. Por via de consequência, realizada estará a tipicidade primeiro elemento da composição jurídica do crime.[57]

As soluções jurídicas apontam que as invasões de sistemas como crimes meio serão absorvidos pelos delitos mais graves, quais sejam: roubos, extorsões, homicídios, furtos, entre outros. Contudo, as condutas lesivas ou potencialmente

53 BRASIL. Lei nº 11.829, de 25 de Novembro 2008. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 20 de agosto 2018.

54 BRASIL. Lei nº 12.034, de 29 de setembro de 2009. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12034.htm>. Acesso em: 20 de agosto 2018.

55 BRASIL. Lei nº 10.764, de 12 de Novembro de 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/L10.764.htm. Acesso em: 20 de agosto 2018.

56 Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou *Internet*, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: Pena – reclusão de 2 (dois) a 6 (seis) anos, e multa.

57 PEDROSO, Fernando de Almeida. Direito Penal - Parte Geral: Estrutura do Crime. LEUD: São Paulo, 1993. p. 45.

lesivas que venham a ser cometidas através da Internet e não se adequarem ao rol de delitos existentes no Código Penal e a leis especiais brasileiras não terão solução no direito brasileiro, podendo ser consideradas condutas atípicas. Ademais, constata-se que a legislação aplicável aos crimes cibernéticos será o Código Penal vigente; em alguns casos aplicação das leis infraconstitucionais e a Constituição Federal como norma base para proteger os bens jurídicos lesados por meio do computador[58].

3.2. CRIMES FUTUROS

A partir do progresso da computação ubíqua equipamentos já possibilitam a realização de quase todas as tarefas cotidianas sem sair de casa, e mais dispositivos estarão conectados à rede mundial de computadores. Por outro lado, o indivíduo se torna mais exposto a todo esse aparato tecnológico que facilita a vida de todos e, inelutavelmente, torna-se um instrumento para a prática de atos ilícitos e criminosos[59].

Os equipamentos que deveriam resguardar, facilitar tarefas cotidianas, salvar vidas, dar comodidade, podem ser utilizados para ameaçar, extorquir, roubar, matar; a lista de crimes é extensa, numa completa inversão da finalidade da tecnologia[60]. O emprego de *software* e *hardware*, para tornar as coisas inteligentes, condicionam-nas ao risco de seus sistemas de controle terem sua integridade corrompida; quanto mais dependentes de computadores, mais suscetíveis estaremos a ataques cibernéticos.

Para Ivette Senise Ferreira, assim como armas de fogo e explosivos são instrumentos utilizados por delituosos, o computador ou sistema de informática também é um meio para cometimento de crime, como tantos outros[61]. Os computadores e suas redes têm um aspecto negativo. que é a prática de delitos a distância, caracterizados pelo anonimato, e que possuem grande poder de lesividade[62], muitas vezes maior do que os crimes tradicionais.

Nesse novo cenário, no qual a computação terá sua onipresença, o indivíduo estará mais exposto a crimes sob novas formas até então desconhecidas.

---

58 ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out.2001. Disponível em: <https://jus.com.br/artigos/2250>. Acesso em: 01 set. 2018.

59 DEIVISON, Pinheiro Franco. *Investigação de Crimes Cibernéticos - A Carreira da Computação Forense. Revista da Sociedade Brasileira de Computação* - Horizontes, v. 5, 2012. p. 24-28.

60 PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Editora Saraiva, 2013. p. 308.

61 FERREIRA, Ivette Senise. **A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes**. Editora Edipro, 2011. p. 208.

62 LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. São Paulo: Editora Atlas, 2011. p.16.

Esses delitos criarão enorme impacto em toda a sociedade, o que nos leva a conjecturar como será o futuro[63].

Você talvez ache que situações como as citadas a seguir não passam de mera ficção, "mas uma coisa está clara: **a Crime S.A** já demonstrou sua disposição e capacidade de alavancar qualquer nova tecnologia para se beneficiar e hackear você[64]". Um estudo da Hewlett Packard Enterprise (HPE, 2014) mostrou que 70% dos aparelhos ligados à Internet das Coisas têm falhas graves de segurança e estão sujeitos a ataques de criminosos. Foram analisados, durante três semanas, dispositivos como TVs, *webcams*, termostatos, controladores de *sprinkler*, *hubs* para controle de vários dispositivos, fechaduras, balanças, alarmes e abridores de portas de garagem. A maioria deles tinha algum tipo de serviço de hospedagem na nuvem e todos eram integrados com *apps* que permitiam o controle remoto por dispositivos móveis. Em média, foram encontradas 25 falhas por dispositivo, totalizando 250 vulnerabilidades. Problemas de privacidade, autorizações insuficientes, falta de criptografia de transporte de dados, interface *web* insegura e *softwares* de proteção inadequados foram alguns dos erros encontrados[65].

Diante dessa vulnerabilidade dos dispositivos, os *cybercriminosos* podem facilmente hackear e usá-los para a finalidade que desejarem. *Os hackers* podem utilizar esses equipamentos como instrumentos capazes de ocasionar sérios danos não somente ao patrimônio, mas à incolumidade física dos utilizadores e, ocasionalmente, levar à morte.

Câmeras que monitoram o domicílio, transmitindo a informação em tempo real para o celular do morador, podem capturar imagens de sua família e transmiti-las justamente para assaltantes ou sequestradores. Segundo Camillo Di Jorge, gerente da ESET[66] no Brasil, "é possível ativar a câmera e o microfone internos de forma remota transformando os televisores em dispositivos de espionagem; assumir o controle de aplicativos de redes sociais incorporados para publicar informações em nome do usuário[67]"; lâmpadas inteligentes podem ser hackeadas para roubar senhas de conexões wi-fi[68] e servirem para espiona-

63 CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011. p. 27.

64 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015

65 BRADICICH, Tom. **HP**, 2017. *IoT Research Study*. Disponível em: <https://community. hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.U9exjfldXtt>. Acesso em: 10 jul. 2018.

66 ESET- Empresa de Segurança para internet sediada em Bratislava, na Eslováquia.

67 Sabia que sua smart TV também pode ser hackeada? **Revista Encontro, 2018.** Disponível em: https://www.revistaencontro.com.br/canal/atualidades/2018/04/sabia-que-sua-smart-tv-tambem-pode-ser-hackeada.html. Acesso em: 10 jul. 2018.

68 BARROS, Tiago. Lâmpadas inteligentes são hackeadas para furto de senhas de Wi-Fi**. Techtudo**, 2014.Disponível em: <https://www.techtudo.com.br/noticias/noticia/2014/07/lampadas-inteligentes-sao-hackeadas-para-furto-de-senhas-de-wi-fi.html>. Acesso em :10 jul. 2018.

gem. Uma cerca elétrica pode ser religada durante um serviço de manutenção ou desligada para facilitar um assalto nas residências. O *Google Glass* pode ser hackeado para tirar fotos e gravar vídeos em segredo e identificar na sua casa quais dispositivos têm vulnerabilidades conhecidas; um eletrodoméstico com falha de configuração pode ser um meio favorável para disseminar *spams* para outros usuários[69]. Babás eletrônicas modernas, que são equipadas com câmeras com vulnerabilidade de firmware, podem ser invadidas, permitindo que o invasor tenha acesso ao quarto do bebê.

Invadir dispositivos de gerenciamento das usinas de produção e distribuição de energia, promovendo *blackouts*; cancelar o fornecimento de água para as cidades, invadir os sistemas de trânsito rodoviário, ferroviário ou metroviário, apoderar-se dos sistemas que controlam os semáforos, acarretando acidentes e grandes transtornos no trânsito local.

Scott Lunsford, pesquisador do Sistema de Segurança de Internet da IBM[70], afirma que, ao invadir o sistema SCADA[71], verificou sua insegurança e uma variedade de probabilidades catastróficas que podem ocorrer se os *cyberterroristas* o invadirem, como por exemplo controlar a usina e causar *blackout* em uma cidade inteira[72].

Existem também os medidores inteligentes, utilizados para medir o consumo de gás e eletricidade de cada lar, que são vulneráveis a ataques *cibernéticos*, porque enviam informações via internet em tempo real para as companhias, repassam aos clientes o seu consumo de energia e auxiliam o governo a conter a demanda nacional com mais eficácia. Uma equipe da empresa *IOActive* de *cybersegurança* desenvolveu um *worm*[73] para verificar as falhas de segurança do sistema de medidores inteligentes e demonstraram que um *hacker* pode invadir esses sistemas e controlar a rede elétrica de todo um país, desligando a energia de milhares de lares ao mesmo tempo[74].

---

69 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.p.282-283.

70 International Business Machines (**IBM**) é uma **empresa** dos Estados Unidos voltada para a área de informática.

71 *Supervisory Control and Data Acquisition* -sistema particular que controla a maioria da infraestrutura americana.

72 CARVALHAL, Aline.8 coisas que você nunca acreditaria que hackers pudessem fazer**. Techtudo,2011.** Disponível em:<https://www.techtudo.com.br/noticias/noticia/2011/09/8-coisas-que-voce-nunca-acreditaria-que-hackers-podem-fazer.html >. Acesso em: 10 jul. 2018.

73 É um programa autorreplicante que pode ser projetado para tomar ações maliciosas após infestar um sistema.

74 CARVALHAL, Aline.8 coisas que você nunca acreditaria que hackers pudessem fazer**. Techtudo,2011.** Disponível em:<https://www.techtudo.com.br/noticias/noticia/2011/09/8-coisas-que-voce-nunca-acreditaria-que-hackers-podem-fazer.html >. Acesso em: 10 jul. 2018.

Podem adentrar no sistema de segurança de cassinos para espionar as instalações e as salas de jogos e passar instruções de apostas para determinado jogador[75].

Dispositivos médicos implantáveis, como marcapassos, desfibriladores, bombas de insulina, implantes cocleares e neuroestimuladores, além dos aparelhos de ressonância magnética, raios X, aparelhos de anestesia, bombas intravenosas, tomógrafos e respiradores mecânicos podem ser atacados e remotamente explorados por *hackers*, subvertendo-os para fins trágicos. Um *hacker* pode ser capaz de acionar remotamente um desfibrilador para aplicar choques elétricos no coração de uma pessoa; de ministrar dose cavalar de insulina de uma só vez através de uma antena de rádio especial; ou esgotar a bateria de desfibrilador necessária para controlar batimento cardíaco[76].

Dispositivos robóticos sem fio e sem bateria para microcirurgias e diagnósticos de doenças podem ser alterados e ser capazes de falsificar resultados e liberar medicamentos na corrente sanguínea quando não deveriam, ou atacar tecidos saudáveis ao invés de tumor. O futuro da biônica pode ser ameaçado por *hackers*, onde pernas robóticas podem ser infectadas por um vírus de computador e mãos biônicas hackeadas. Um *hacker* pode acessar máquinas que dosam automaticamente o medicamento que o paciente precisa receber por dia, podendo receber superdosagem ou não receber o remédio. Ataques a dispositivos médicos conectados à internet serão possíveis, surgindo novas maneiras de cometer homicídios ou outros crimes hackeando tais equipamentos[77].

Imagine também um laboratório que somente máquinas podem ou poderão manipular vírus, e o local onde o vírus se encontra em quarentena para a concepção de uma vacina seja totalmente monitorado pela internet. Um *hacker* poderá invadir o sistema de controle do laboratório, e ter a liberdade de fazer o que quiser, não é mesmo? Até causar uma epidemia ou infectar as pessoas que laboram no laboratório. É assustador. Parece cena de filme, mas pode ser uma realidade não tão distante[78].

---

75 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.p259.

76 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.p285-289.

77 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.p.289-290.

78 LÓSSIO, Claudio Joel Brito; SANTOS, Coriolano Aurélio Almeida Camargo. Breve comentário sobre a internet das coisas a luz do direito penal brasileiro. **E DE DIREITO**, p. 15, 2018.Disponível em:< http://www.portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/issue/download/274/42#page=16 >. Acesso em: 26 ago.2018.

Os *scanners* biométricos não são tão seguros; os marcadores biológicos podem ser copiados (digitais de olhos, rostos, dedos), assim como todos os outros sistemas de informação podem ser comprometidos, coletados sem nosso consentimento e serem vendidos. O futuro roubo de identidade envolverá roubar e comprometer indicadores biométricos. O reconhecimento facial, sensores de impressões digitais, escaneamento de íris permitem que *hackers* façam a engenharia reversa das informações biométricas armazenadas e imprima a imagem da íris para ludibriar *scanners* comerciais dessa parte do corpo humano. Dada a crescente onipresença de câmeras e *softwares* de reconhecimento facial, criminosos podem adotar essas ferramentas, a exemplo dos pedófilos usarem biometria para identificar uma criança[79].

Os avatares (representações virtuais de nós mesmos) podem ser infectados por *malwares*, e isso permitir que o outro assuma o controle para cometer, por exemplo, agressões sexuais e físicas[80].

Vimos diversos exemplos de como a tecnologia será cada vez mais utilizada sobre e dentro do nosso corpo. Dispositivos vestíveis, incorporáveis, ingeríveis e implantáveis levam-nos, de uma maneira ou de outra, a entrar na nação ciborgue, expondo nosso corpo físico a ataques cibernéticos. Nossa anatomia e nossa fisiologia agora, também, podem ser monitoradas a distância, com ou sem o nosso conhecimento, via biometria e biometria comportamental, uma tecnologia capaz de nos categorizar e nos identificar no meio de uma multidão[81].

Diante do exposto, é intrigante e assustador pensar sobre os crimes que podem ser cometidos à medida que a Internet das Coisas se torna cada vez mais parte da realidade da vida das pessoas. Muitos problemas engrossam a fila dos novos desafios que o direito e as autoridades enfrentarão[82].

3.2.1. Casos reais (Hard Cases)

Dispositivos inteligentes são uma das principais inovações da tecnologia e foram projetados para facilitar nossas vidas trazendo inúmeros benefícios, na medida que também oferecem riscos pois podem ser invadidos via internet,

79 Ibidem..

80 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.p 305-306.

81 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.p.307.

82 HPE. *HP IoT Research Study*. Disponível em: <https://community. hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.U9exjfldXtt>. Acesso em: 10 jul. 2018.

que é o meio para os *hackers/crackers* cometerem qualquer uma das condutas ilícitas citadas, e muitas outras inimagináveis.

A seguir veremos que já é uma realidade a invasão de *hackers/crackers* aos dispositivos inteligentes, ratificando o risco que a Internet das Coisas oferece e que os crimes cometidos por meio da internet s**ão** cada vez mais reais.

Em 2016 o Hollywood Presbyterian Medical Center, em Los Angeles, foi atacado por *hackers* que, através de *ransomware,* invadiram o sistema de computadores do hospital e os registros dos pacientes ficaram retidos como reféns, e o hospital pagou US $ 17 mil para desbloquear seus arquivos[83].

O hotel Romantik Seehotel Jäger foi vítima de cibercriminosos, que mantiveram o controle do sistema de computador do hotel e pediram US $ 1.603 em *bitcoins,* para liberar reservas e as chaves eletrônicas usadas pelos hóspedes para acessar seus quartos. E só após o pagamento do regaste exigido os sistemas foram desbloqueados e o hotel retornou às operações normais[84].

Uma família da Carolina do Sul, nos Estados Unidos descobriu que sua babá eletrônica estava sendo monitorada, quando a mãe da criança observou que a câmera estava fazendo movimentos de 360 graus, sendo controlada remotamente pelo aplicativo (porém somente os pais tinham acesso ao aplicativo e os dois estavam no local). Nesse caso, a câmera estava se movimentando para observar a mãe. Chamaram a polícia e informaram que o acesso ao aplicativo havia sido bloqueado, e nada poderiam fazer. Constataram, então, que os criminosos estavam ouvindo a conversa[85].

Muitos casos de invasão de babá eletrônica já aconteceram em diversos países; um dos que se tornou público foi o de Raquel Keppe (brasileira), mãe de dois filhos (um de quatro anos e o outro de um ano). A administradora observou que há oito meses o aparelho se comportava de maneira estranha (a câmera se mexia sozinha); ela achou esquisito, mas não deu a devida importância. Após esse episódio, meses depois, no meio da noite, Raquel ouviu uma música vinda do quarto do seu filho e percebeu que o som vinha da câmera. Ela não conseguiu desligar, até que, a música parou de tocar sozinha. Algumas semanas depois, Raquel constatou que o desempenho estranho de seu aparelho era uma ação de *hackers*, ao se deparar com uma matéria sobre invasão de babás eletrônicas nas redes sociais. O seu equipamento, comprado nos Estados Unidos, era da marca Foscam, que tem a opção de acesso remoto, por meio de um *login* e

83 SALMI, Deborah. *Ransomware ataca computador do hotel e sistema de cartão chave*. **Avast**, 2017. Disponível em:< https://blog.avast.com/ransomware-attacks-hotel-computer-and-keycard-system>. Acesso em: 10 de jul. 2018.

84 *Ibidem*

85 ROSA, Nathalie. *Família descobre que estava sendo observada por uma babá eletrônica***. Canaltech**, 2018.Disponível em: <https://canaltech.com.br/hacker/familia-descobre-que-estava-sendo-observada-por-uma-baba-eletronica-115350/ >. Acesso em: 10 jul. 2018.

senha. O outro caso notório foi relatado pelo casal Marc e Lauren Gilbert, nos Estados Unidos. Relataram que acordaram no meio da noite ao ouvir uma voz "de sotaque britânico ou europeu" vindo da babá eletrônica, gritando obscenidades para a filha que estava no quarto[86].

Em seis meses, dois criminosos furtaram 30 veículos da marca Jeep no Texas, Estados Unidos. Eles usavam um *laptop* e, com auxílio de um *software* pirata, entravam nos carros, decodificavam a chave e davam partida nos veículos[87].

Em 2014 foram furtados, em média, 17 carros por dia em Londres, no total de 6.000 unidades ao longo do ano. Por meio da chamada tecnologia *keyless* (identificada por sensores instalados na porta do veículo onde os motoristas, sem a necessidade de manusear a chave, entram e dão partida no carro somente com a presença dela). Para furtar carros com essa tecnologia, segundo o órgão que fez os testes, os ladrões seguem o proprietário e, com isso, ficam próximo e ativam o dispositivo eletrônico que aumenta o alcance do sinal da chave *keyless* do proprietário do veículo. Dessa maneira, um segundo ladrão aguarda o automóvel e usa o sinal da chave captado pelo dispositivo para furtá-lo[88].

Charlie Miller e Chris Valasek (dois *hackers*) invadiram e controlaram um Jeep Cherokee 2014, que era dirigido pelo jornalista Andy Greenberg, em uma rodovia a quilômetros de distância (...). O experimento mostrou que é possível dar comandos em sistemas de conforto, como rádio e ar-condicionado, mas também para os freios, acelerador, transmissão e direção do veículo(...). O jornalista relatou que até o momento em que eles estavam apenas brincando com o rádio, ar-condicionado e buzina foi divertido. A história mudou quando a transmissão foi desligada e o acelerador não funcionava no meio da rodovia; eles cortaram o sistema de freios, enquanto o SUV se encaminhava para uma vala à beira da estrada, em baixa velocidade[89].

Ainda sobre o furto de carros, hackers chineses conseguiram monitorar a distância um automóvel da marca Tesla. Acionaram o freio através de uma brecha no navegador do sistema multimídia. No dia 24 de setembro 2017, na cidade de Solihull – Inglaterra, dois *hackers* foram flagrados pela câmera da

86 MALACARNE, Juliana. *Hacker invade babá eletrônica de menino de 1 ano*. **Revista Crescer**, 2016. Disponível em: <https://revistacrescer.globo.com/Bebes/Seguranca/noticia/2016/01/hacker-invade-baba-eletronica-de-menino-de-1-ano.html>. Acesso em: 10 jul. 2018.

87 DIAS, Diego. *Quadrilha de hackers especializada no roubo de Jeeps é presa*. **Quatro rodas**, 2016. Disponível em: < https://quatrorodas.abril.com.br/noticias/quadrilha-de-hackers-especializada-no-roubo-de-jeeps-e-presa/>. Acesso em: 10 jul. 2018.

88 DIAS, Diego. *Teste mostra vulnerabilidade de carros com sistema keyless*. ***Quatro Rodas****, 2016.* Disponível em: https://quatrorodas.abril.com.br/noticias/teste-mostra-vulnerabilidade-de-carros-com-sistema-keyless/>. Acesso em: 12 jul. 2018.

89 *De longe, hackers 'invadem' e controlam carro com jornalista dentro*. **G1**,2015. Disponível em: <http://g1.globo.com/carros/noticia/2015/07/de-longe-hackers-invadem-e-controlam-carro-com-jornalista-dentro.html >. Acesso em: 12 jul. 2018.

residência furtando um carro. Não danificaram o automóvel, apenas utilizaram retransmissores de sinal, próximo ao portão da garagem e captaram o sinal da chave dentro da casa retransmitindo para outro dispositivo próximo ao veículo, que é "ludibriado" e abre as portas[90].

Cibercriminosos acompanham sistemas de empresas terceirizadas para conseguir informações de seus alvos. Para ter acesso **à** rede computacional de determinada empresa, os *hackers* infectaram com malware o cardápio online de um restaurante de comida chinesa muito usado pelos empregados. *Hackers* também já obtiveram acesso aos registros da loja Target (rede de lojas de varejo dos Estados Unidos) através do sistema de ar condicionado. Em outros episódios, *hackers* **já utilizaram termostatos, equipamentos de videoconferência e impressoras**[91].

A sede do Google, em Sidney, e o North Shore Private Hospital e seus sistemas de ventilação, iluminação e câmeras de vídeo foram invadidos por pesquisadores de segurança através de seu fornecedor de gestão predial. Esses mesmos estudiosos demonstraram que é possível, por meio do fornecedor de ventilação e aquecimento, invadir os disjuntores da área olímpica de Sochi. Felizmente, a invasão foi realizada por pesquisadores que estavam buscando falhas que pudessem ser descobertas por *hackers* reais[92].

O casal Alan e Jean, de Leeds, no norte da Inglaterra, instalaram sete câmeras de segurança em sua casa, todas elas com acesso remoto. Essas câmeras inteligentes tinham conexão com a internet, através da rede *wi-fi* da casa, captação eletrônica de imagens e processador para tratar os vídeos gravados. Todas essas funções permitem assistir às imagens pelo celular e armazená-las na nuvem, além de poder ativar e desativar os aparelhos pelo aplicativo do telefone. Através de uma investigação exclusiva, a pedido da BBC, o especialista em segurança Cal Leeming examinou o sistema de câmeras da residência do casal para saber quantas vezes as imagens registradas foram vistas por outras pessoas. Constatou-se que as gravações foram assistidas cerca de 5 mil vezes em 70 países. Um resultado aterrorizante[93].

---

90 *Vídeo: polícia flagra 'furto hacker' de carro sem as chaves*. **G1**,2017. Disponível em:< https://g1.globo.com/carros/noticia/video-veja-como-e-o-furto-hacker-de-carro-sem-as-chaves.ghtml>. Acesso em: 12 jul. 2018.

91 **Cibercriminosos monitoram sistemas de empresas terceirizadas para obter informações de seus alvos.** Disponível em: <https://tecnologia.ig.com.br/2014-04-26/hackers-exploram-falhas-em-sistemas-de-ar-condicionado-e-maquinas-de-salgados.html. Acesso em: 12 jul.2018.

92 **Cibercriminosos monitoram sistemas de empresas terceirizadas para obter informações de seus alvos.** Disponível em: <https://tecnologia.ig.com.br/2014-04-26/hackers-exploram-falhas-em-sistemas-de-ar-condicionado-e-maquinas-de-salgados.html. Acesso em: 12 jul.2018.

93 Aparelhos inteligentes são uma das principais novidades da tecnologia: eles oferecem controle remoto de nossas casas e carros e facilitam nossa vida, mas também trazem riscos, como mostra uma investigação exclusiva da BBC. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/milhares-viram-em-70-paises-as-imagens-das-cameras-de-seguranca-de-minha-casa-sem-que-eu-soubesse.ghtml>. Acesso em: 12 jul.2018

No dia 30 de julho de 2018, *hackers* invadiram o sistema da Santa Casa de Pirajuí, no interior do Estado de São Paulo e exigiram em *bitcoins* o resgate dos dados. O hospital se recusou a efetuar o pagamento e os criminosos destruíram os arquivos dos pacientes. Vários serviços foram lesados, precisaram inserir novamente na rede programas indispensáveis para o funcionamento de setores, a exemplo do raio-x, assim como os dados dos pacientes[94].

Diante do exposto, verifica-se que os crimes praticados através de dispositivos inteligentes não é mera ficção e com o aumento deles crescem também os possíveis ataques imagináveis e inimagináveis dos *hackers/crackers*. Quanto mais nos cercarmos desses dispositivos, mais motivações os cibercriminosos terão para tê-los como alvo, invadindo ou infectando-os para proveitos ilícitos.

Contudo, alguns bens já possuem um certo grau de popularidade muito maior em comparação com outros, que ainda estão em fase de pesquisa e desenvolvimento, entretanto, já existem vidas humanas adaptadas ao uso e manuseio da ubiquidade computacional para seus afazeres cotidianos e, como vimos, a tendência é que isto aumente nos mesmos passos largos em que a tecnologia avança. São eles os automóveis e as habitações.

3.3. Dos especiais – Automóveis e Habitações

Após virmos o quanto a computação ubíqua está presente no cotidiano humano, bem como os riscos e vulnerabilidades que o usuário dessa modalidade computacional está exposto, é mister notarmos também que a sociedade está em processo de adaptação a essas presenças.

Como visto, o uso dos sistemas computacionais onipresentes e imperceptíveis aumenta a cada dia; desde as etapas de criação do carro[95] até as casas com aparelhos interligados às já citadas *smart houses*, assim como as *smart homes*. Já se pode afirmar que os seres humanos estão em uma crescente dependência das dinâmicas tecnológicas, que avançam não só em inovações, como também em acesso e popularidade[96].

E, justamente, a interação da computação ubíqua com esses dois bens de consumo humano merecem destaques. Primeiro, porque é de notório saber que à medida que as tecnologias avançam, os criminosos também se atualizam e se

94 MOREIRA, Rene. Hackers atacam sistema de Santa Casa de Pirajuí (SP) e exigem bitcoins. **O Estadão**, 2018. Disponível em:< https://sao-paulo.estadao.com.br/noticias/geral,hackers-atacam-sistema-de-santa-casa-de-pirajui-sp-e-exigem-bitcoins,70002426223>. Acesso em: 10 agosto 2018.

95 LEME, José Antonio. Conheça os benefícios da indústria 4.0. **Estadão,2018.** Disponível em:<https://jornaldocarro. estadao.com.br/carros/conheca-os-beneficios-da-industria-4-0/> Acesso em 07 agosto 2018.

96 Casa inteligente: tecnologias que facilitam o dia a dia. Wef net. Disponível em:<http://www.weg.net/tomadas/blog/tecnologia/casa-inteligente/> Acesso em 07 agosto 2018.

adaptam a essas inovações tecnológicas. Depois, os bens não corpóreos – chamados assim os que estão externos ao corpo humano – estão com as inovações tecnológicas em maior grau de popularização e, ao mesmo tempo, maior grau de vulnerabilidade dos usuários.

Da mesma forma que não podemos deixar de aclamar as novidades da tecnologia e as melhorias que trazem à qualidade de vida humana, também devemos abrir nossos olhos para os perigos de expor nossas vidas a essas novidades e, principalmente, que tipos de fragilidade desses avanços podem ser utilizados por criminosos.

Dedicamo-nos a alertar sobre as consequências criminais da ubiquidade contemporânea em automóveis e habitações, destacando as principais tecnologias ubíquas e suas possíveis implicações criminais, face à popularidade, aceitação e, principalmente, falta de precaução dos usuários dessa tecnologia.

3.3.1. Dos crimes em automóveis

Convém ressaltar que o setor automobilístico é o principal investidor no ramo da ubiquidade computacional. A acirrada disputa entre as montadoras e uma clientela cada vez mais plural e mais ligada à tecnologia são fundamentais para o investimento pesado em sistemas que proporcionem conforto, luxo, comodidade e facilidades para a condução de um veículo.

Assim, o ambiente é perfeito para a integração de sistemas sempre mais complexos, que auxiliem o motorista nas mais variadas funções. Hoje em dia já existem tecnologias que auxiliam o condutor a estacionar seu carro, a ajustar a temperatura de forma automática, e até a acionar automaticamente o limpador de para-brisa.

Verifica-se que é possível desabilitar o sistema de frenagem de um carro; controlar o computador de bordo para ocasionar acidentes; aumentar ou diminuir a temperatura do ar e travar as portas e janelas para provocar um homicídio; controlar o funcionamento da central eletrônica e do motor de um carro e roubar dados sigilosos registrados no sistema de entretenimento a bordo. Controlar os carros, de maneira que as ações dos motoristas possam ser totalmente ignoradas: os pedais, rodas e botões não responderem.

Os especialistas em segurança já estão prognosticando que o futuro do roubo de carros será lucrativo para *hackers,* que poderão vender seus serviços para ladrões, fornecendo localização GPS do carro, destrancando e dando a partida imediatamente no veículo[97].

97 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.

O nível de sofisticação dos sistemas, como já revelado, é grande. Isso implica linhas e mais linhas de código. Para que se tenha uma ideia, já há uma estimativa em 1.400.000 (um milhão e quatrocentas mil) linhas de código de programação, em um único veículo[98].E a maior parte desses sistemas implementados nos automóveis conecta com a internet, com a tecnologia *bluetooth* e, às vezes, com servidores internos das próprias montadoras. É o caso que vemos de forma mais popular com a General Motors e o seu On Star[99].

É importante frisar que o consumidor é carente de quaisquer observações específicas sobre essas tecnologias, ao passo que cada pessoa, ao comprar um automóvel, recebe um manual de instruções completo de cada funcionalidade, e é instruído de noções básicas de uso do veículo; porém, verifica-se que a parte tecnológica do carro só é demonstrada em seu acesso, e nunca em seu conteúdo, isso implica dizer que o proprietário do veículo apenas aprende como conectar seus aparelhos tecnológicos ao seu automóvel, ou como acionar os serviços da montadora para utilizar determinadas funções, mas não sabe como o sistema trabalha para gerar as funcionalidades vendidas como "o futuro que chegou em seu automóvel".

E o fundamento para isso esbarra em diversos fatores, dentre os quais dois se destacam: o primeiro diz respeito ao comportamento educacional do brasileiro de não se importar com a forma como a tecnologia funciona; e o segundo ponto consiste na ausência de uma regulação específica para esse tipo de consumo, o que permite que o uso da tecnologia seja legítimo em face de um "termo de uso" que poucos consumidores leem[100].

A prova disso é que 97% da população não leem o termo de uso e concordam com ele. O consumidor brasileiro segue cedendo seus dados, sem óbices legais, a empresas que exploram isso sob o véu da comodidade, praticidade, conforto, e até mesmo segurança. Tudo isso colabora para um ambiente de redução das preocupações dos motoristas em relação ao seu próprio veículo, e esse é o ambiente que mais merece alerta, por ser perfeito para a ação de criminosos[101].

3.3.2. Coleta de informação

Um dos primeiros problemas que acontece a partir da modernização dos carros, atualmente, consiste na coleta de informações. Esse, inclusive, não é

98 GOODMAN, Marc. **Future Crimes: tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso** São Paulo :HSM Editora, 2015.

99 ROMERO, Luiz. Não li e concordo. Super Abril, 2017. Disponível em:< https://super.abril.com.br/tecn ologia/nao-li-e-concordo/>. Acesso em: 12 out 2018.

100 ROMERO, Luiz. Não li e concordo. Super Abril, 2017. Disponível em:< https://super.abril.com.br/tecn ologia/nao-li-e-concordo/>. Acesso em: 12 out 2018.

101 ROMERO, Luiz. Não li e concordo. **Super Abril, 2017.** Disponível em:< https://super.abril.com.br/tecn ologia/nao-li-e-concordo/>. Acesso em: 12 out 2018.

problema exclusivo dos automóveis e suas novas funcionalidades, mas de toda a forma como a tecnologia vem adentrando nas relações humanas.

A era 2.0 da *web*[102] trouxe uma massificação das relações humanas como produtoras de conteúdos informativos diversos; A chegada da era 3.0[103] faz com que essa coleta também se dê pelos mecanismos que os seres humanos usam, conforme os avanços da computação ubíqua.

Dessa maneira, os seres humanos massificam as informações sobre si, em um grande banco de dados organizado pelos coletores de informações. E aqui é que temos o problema em questão: A coleta de informação dos carros.

Inicialmente, convém mencionar que o conceito de "consumidor médio" de um automóvel é de um sujeito que conduza seu carro com frequência, em seu dia a dia. Assim, apenas com o monitoramento do sistema de GPS do veículo, a pessoa teria informações cruciais, como o local da casa do condutor, os locais para os quais frequentemente ele se encaminha (como o seu trabalho, escola, faculdade, mercado, entre outros), e com que frequência ele se desloca para esses locais.

Isso também implica dizer que (e apenas com o monitoramento do GPS) dá pra perceber toda a rotina que a pessoa tem, a frequência com que se ausenta de de sua residência e o tempo que passa longe. Além disso, com esses dados, é possível calcular também o tempo médio em que a pessoa está fora de onde mora, a velocidade com a qual dirige o seu carro e a que distância está do seu lar.

Apenas usando essas informações, é possível arquitetar um furto dos bens em sua residência, invadindo a propriedade da pessoa em um horário no qual saiba que ela estará fora – deixando sua residência vulnerável.

Também é possível saber o itinerário da potencial vítima, e buscar um momento propício pra realização de um sequestro ou homicídio. E estamos, aqui, falando de apenas um dado fornecido de bom grado pelo consumidor, que comprou seu carro moderno e confortável, e vê como vantagem a cessão de informações dessa estirpe.

Outras funcionalidades do carro também podem ser utilizadas em *big data*, e expor o condutor a situações de perigo. O controle de voz, por exemplo, pode revelar planejamentos que gerem violações de privacidade, utilizáveis como barganha para extorsões, ao exigir, mediante chantagem, que a pessoa entregue uma determinada e exorbitante quantia, sob pena de revelar conteúdo de áudio com informação constrangedora. Saber o que é conversado também pode ir além e ser utilizado para crimes perante terceiros, de forte

102 Amoro, Danilo. O que é web 2.0? **TecMundo, 2008.**Disponível em:<https://www.tecmundo.com.br/web/183-o-que-e-web-2-0-.htm>. Acesso em 22 de dez de 2018.

103 **Internet Innovation**. Disponível em:<https://www.internetinnovation.com.br/blog/entenda-o-conceito-da-web-3-0/ >Acesso em: 22 de dez de 2018.

envolvimento com o "alvo" da interceptação sonora. É o caso, por exemplo, de descobrir quem é a pessoa amada, ou seus filhos, por meio de conversa realizada em uma carona; a mesma carona que, em informação cruzada com o GPS, pode informar também o local onde essa terceira pessoa amada mora. Daí, um sequestro mediante ligação a quem esteja conduzindo, para que esse arque com a quantia da soltura de sua pessoa amada, teria todas as ferramentas para ser executado.

E o que mais impacta é a ausência de qualquer tipo de previsibilidade desses delitos. Não só, "convenientemente", por parte das montadoras – que não fazem o menor esforço pra conscientizar seus consumidores dos perigos e usos de informações coletadas pelo seu "computador sobre 4 rodas" – quanto por parte de seus consumidores, que saem agradecidos, satisfeitos, impressionados e, principalmente, sem a menor preocupação com a coleta ou o uso dos seus dados pessoais.

Assim, a vulnerabilidade dos usuários de carros, principalmente dos motoristas, aumenta massivamente, ao passo que as formas de defesa dos ataques cibernéticos sequer esboçam uma reação ou, em alguns casos, uma criação.

3.3.3. Controle remoto

Uma outra questão importante de se destacar é a possibilidade de o carro ser dirigido de forma remota, por outra pessoa que não o condutor, mesmo ele estando dentro do carro. Ao ser ligado, o sistema elétrico do carro é acionado, dando a partida em todas as funções tecnológicas que o veículo tiver. Iniciam-se, então, o navegador GPS, a direção elétrica, o computador de bordo, entre outras tantas funções que se encontram até mesmo nos carros mais populares.

Contudo, não há um rigor na segurança dos sistemas. Pelo contrário, eles são feitos de forma simples, para que o condutor tenha pleno uso sem senhas, sem reconhecimentos faciais ou biométricos, controles de voz etc.

Dessa forma, um carro torna-se um computador móvel, com forte estrutura funcional, grandes setores computacionais cruciais para seu funcionamento e um sistema de segurança da computação frágil.

Um *hacker* que adentre em um carro, poderia controlar remotamente e conduzir o veículo para situações de perigo, como quedas em alturas, batidas em alta velocidade, ou até mesmo o deslocamento do carro para um local ermo, de difícil acesso, propício para crimes de sangue, ou sequestro.

Outra situação preocupante é a dificuldade de encontrar os rastros digitais que certas condutas consequentes desse controle remoto pode causar. Um automóvel que seja remotamente trancado, e conduzido lentamente à submersão,

implica não só o delito de homicídio doloso, como o prejuízo dos mecanismos de provas, uma vez que os sistemas operacionais serão degradados a ponto de tornar-se quase impossível a perícia dos equipamentos eletrônicos.

Isso significa dizer que estamos diante de diversas hipóteses do crime perfeito, onde assassinatos passarão por acidentes, e os prestadores da conduta delituosa serão acobertados pelo manto da impunidade, graças à vulnerabilidade de sistemas e usuários desatentos a pontos tão cruciais de suas vidas.

3.3.4. Mudança de Código

Outra preocupação diz respeito ao código que os carros hoje carregam. Conforme visto anteriormente, mais de um milhão de linhas de código estão presentes nos veículos mais modernos.

Os sistemas dos automóveis possuem em suas linhas de códigos de programação diversas informações. Há códigos para fazer o carro virar automaticamente à direita, outros à esquerda; há linhas de código para identificar a temperatura do carro e, quando atingir determinado marco no termômetro, acionar o ar condicionado, entre tantas outras programações que tornam o automóvel mais confortável para o usuário.

O problema aqui consiste na vulnerabilidade do sistema, aliada à desatenção de um usuário cada vez mais dependente dessas inovações tecnológicas. Um *hacker* pode adentrar no sistema do automóvel e, ao invés de buscar controlá-lo remotamente ou utilizar-se das informações coletadas pelo veículo, simplesmente alterar algum marco fundamental da linha de código.

Suponhamos que um determinado automóvel, com função de estacionamento automático, tenha suas milhões de linhas de código e, em algumas delas, o sistema identifique e programa que faz o volante girar e o carro ganhe aceleração a uma velocidade baixa, permitindo acionar o "modo de estacionamento automático". Aqui, um *hacker* mal intencionado poderia apenas adentrar nos sistemas operacionais do carro uma única vez e alterar o marco da velocidade de supostos 10km/h para 100km/h. O acréscimo de um único numeral (no exemplo, o zero à direita) no marco base do código de estacionamento automático pode causar uma verdadeira catástrofe, com riscos seríssimos de lesões à integridade física, psicológica e até mesmo de responsabilização penal à pessoa errada, pois difícil será provar a culpabilidade de o *hacker* ter alterado uma linha de código, quando há um condutor dentro do veículo.

Nesse ponto, destaque merece o papel das montadoras. Elas poderão ser – e muito provavelmente serão - responsabilizadas pela deficiência técnica apresentada em seus veículos, em caso da incidência desses crimes.

3.4. Dos Crimes cometidos em/por habitações

Como já dizia Edward Coke, "a casa de um homem é seu castelo"[104], e nada traz mais a sensação de segurança, do que o doce lar do cidadão.

Com esse pensamento, cada vez mais frequentemente, as *smarthouses* ou *smarthomes,* estão na mira da computação ubíqua. Isto se dá porque é em sua casa que o indivíduo se sente mais seguro, mais confortável e, consequentemente, mais vulnerável.

Em sua casa, ambiente de total relaxamento após uma dura rotina, quanto menos esforço o habitante fizer, mais ele se sentirá confortável. E é com base nesse sentimento que temos avanços tecnológicos: Temos cobertores inteligentes que regulam temperatura, realizam arrumação automática da cama[105]; temos também geladeiras que permitem identificar o item que falta e fazer mercado dentro de sua casa ou até programá-la para fazer isso automaticamente[106]; temos banheiras e ar condicionados que se ajustam a partir de acionamento remoto da água – e regulamentação de sua temperatura – ou regulação do clima, através da sua proximidade dos cômodos, dentre tantas outras coisas.

E um indivíduo relaxado também é um indivíduo vulnerável. Nos tempos de hoje, nenhum "castelo" está imune aos ataques cibernéticos. Poucos, aliás, possuem sequer algum tipo de preparo ou repreensão a esses ataques.

Na conferência de segurança DEFCON, uma dupla de *hackers* comprovou que um termostato inteligente pode ser hackeado instalando um *ransomware* nele. Ou seja, *hackers* podem, a distância, controlar a temperatura dentro de uma casa ou qualquer ambiente que tenha esse equipamento e, por exemplo, exigir dinheiro das vítimas[107].

Neste item, analisamos algumas das muitas possibilidades de ataque que uma casa pode sofrer, ensejando consequências criminais.

3.4.1. Coleta de informação habitacional

Assim como nos automóveis, as *smart houses* também são fontes de captação de informações fundamentais à rotina de uma pessoa e, consequentemente, perigosas se mantidas ao alcance de criminosos.

---

104 Pensador. Disponível em:< https://www.pensador.com/frase/MTE3NDA/>. Acesso em: 20 out 2018.

105 Como funciona o cobertor inteligente controlado pelo celular de quem está em cada metade da cama **G1,2017.** Disponível em: <https://g1.globo.com/tecnologia/noticia/como-funciona-o-cobertor-inteligente-controlado-pelo-celular-de-quem-esta-em-cada-metade-da-cama.ghtml>. Acesso em:20 out 2018.

106 RASMUSSEM, Bruna. Geladeira inteligente da Samsung faz compras e até twitta **Tecmundo,2011**. Disponível em: https://www.tecmundo.com.br/ifa-2011/13000-geladeira-inteligente-da-samsung-faz-compras-e-ate-twitta.htm >. Acesso em: 30 de nov. 2018.

107 JUNQUEIRA, Daniel. **Gizmodo, 2016**.Hackers invadem termostato para nos lembrar que a internet das coisas ainda é insegura. Disponível em:< https://gizmodo.uol.com.br/seguranca-internet-coisas-hacker/>. Acesso em 12 de jul.2018.

Uma das mais primazes envolve a rotina do habitante da *Smart house*: o tempo que essa pessoa se dedica a afazeres em sua casa, a frequência dos seus afazeres domésticos – e, em alguns casos, e até mesmo o local exato da casa em que a pessoa se encontra. Tais informações, se vazadas, podem ensejar não apenas emboscadas ou crimes direto ao indivíduo, mas sim que ele se encontra distante de bens que podem ser preciosos – portanto, alvos de crimes.

Não bastasse isso, o *Big Data* também atinge os eletrodomésticos. Portanto, o uso das câmeras de aparelhos como geladeira e televisão, bem como a frequência do uso de ambos; os produtos normalmente consumidos e armazenados, e também aqueles que estão presentes e ausentes em sua geladeira; a frequência e temperatura em que o ar condicionado é mantido; as informações circulatórias e respiratórias do indivíduo que dorme em uma cama inteligente, ou seja, os exemplos não param.

Então, vê-se que um indivíduo mal intencionado, com posse dessas informações, pode saber detalhes do cotidiano do proprietário que habita aquele lar e a partir dessas informações, realizar furtos ou filmagens em momentos íntimos ou trajes mais confortáveis – ou até mesmo despido, possuindo, assim, material para uma extorsão mediante chantagem.

As informações são preciosas e, de fato, quando bem utilizadas, geram avanços inegáveis ao modo de viver dos seres humanos. Contudo, não existem informações que não sejam importantes; e como o *Big Data* abre um verdadeiro "ciberuniverso de informações cruzáveis", não há também como esconder os riscos que uma coleta irresponsável, ou vulnerável, pode causar na vida de um indivíduo.

Os sistemas de segurança desses produtos de alta tecnologia dependem bastante do usuário, pois a produção em massa exige uma senha padrão, de baixa dificuldade de memorização, até para que sejam realizados testes e desenvolvimentos dos eletrodomésticos e aparelhos para o lar.

Somadas, essas forças são pratos cheios para *hackers* invadirem facilmente a casa de alguma pessoa, e adquirirem todas essas informações para fins criminosos. Sabemos que o limite para isso varia de acordo com a criatividade do criminoso, mas não é difícil imaginar a quantidade de delitos que podem ser tentados ou consumados em posse de informações tão pessoais, precisas, cruciais e rotineiras.

3.4.2. Mudança de código habitacional

Como digo em tópico anterior, as inovações tecnológicas que ocorrem em automóveis consistem em inserção de milhões de linhas de código, para que o *software* (denominação atribuída a um programa de computador) responsável

pela função funcione perfeitamente. Nas *Smart houses* não é diferente, para cada função que permita a um organismo computadorizado captar informações do ambiente e gerir automaticamente tarefas, necessita-se de linhas e mais linhas de códigos de origem.

Dessa forma, seguindo os exemplos, são linhas e linhas de código que fazem a sua banheira captar a temperatura da água, atribuir-lhe em tabela comparada as escalas de temperatura, e estabelecer potências de pré-aquecimento para que se regulem àquilo apontado pelo acionador remoto – que pode ser um *smartphone* ou aparelho específico para tal fim. Após essa função, a água é acionada automaticamente pela banheira, em potência que permita uma climatização da água considerada agradável – e previamente determinada, seja por modificação do consumidor, ou seja, pelo padrão da fabricante – para que o indivíduo tome seu banho tranquilo e relaxado assim que chegar em sua casa.

Então, um *hacker* pode perfeitamente mudar esse código-fonte, fazendo com que os marcos utilizados pelo sistema operacional dos eletrodomésticos sejam alterados. Voltando ao exemplo da banheira, o código-fonte poderia ser alterado, fazendo com que seu marco inicial de temperatura não seja igual a 0ºC, mas sim 50ºC. Dessa forma, ao acionar remotamente o relaxante banho na banheira a 25ºC1, o sistema acrescenta esses 20ºC em cima dos 50ºC do marco zero, o que gera um banho de temperatura em 75ºC, e a potencialidade de queimaduras graves ao banhista desavisado, que habitualmente cumpre sua rotina tomando banho com esse artifício tecnológico.

4. POSSÍVEIS SOLUÇÕES.

ESTA PARTE DO TEXTO APRESENTA PROPOSIÇÃO DE MEDIDAS QUE PREVINAM E ATENUEM A RECORRÊNCIA DOS CRIMES CIBERNÉTICOS, DENTRO DA NOVA REALIDADE QUE NOS CIRCUNDA, COM O SURGIMENTO E EVOLUÇÃO DA UBIQUIDADE COMPUTACIONAL.

4.1. TECNOLOGIA *HASH*

Uma das possíveis soluções pode advir da tecnologia *Hash* e sua criptografia avançada, central para o uso da tecnologia *Blockchain*. Para que saibamos como funciona essa tecnologia em termos práticos, vejamos o seguinte exemplo, muito utilizado em plataformas de compartilhamento massivo de dados, chamadas de *torrents*.

Torrent é uma maneira de transferência de arquivos pela internet, que funciona de forma muito peculiar. Dentre as várias características que a destacam,

uma das que mais chamam a atenção é a maneira pela qual os dados alcançam o destinatário final.

A grosso modo, a integridade do dado é garantida através de um truque: Ao gerar um arquivo original, os *softwares* de *torrent* elaboram uma sequência única, diferenciada, de códigos de computação comprimidos em letras e números, para que sejam atribuídos aos conteúdos que estejam sendo compartilhados através dessa maneira.

Assim, antes de começar a baixar os arquivos, pastas, ou demais dados disponibilizados por *torrent,* os clientes fazem com que o programa que iniciará esse processo "converse" com o computador, pedindo as mesmas sequências de letras e números do arquivo original. Caso o conteúdo a ser baixado passe por esse "check in", a transferência será iniciada; caso seja reprovado, o arquivo é considerado alterado e não deverá ser baixado. Essa sequência é conhecida como "Hash info"; e pode ser facilmente verificada em indexadores de *torrent*. O uso dessa técnica é conhecida no mundo da informática como *hash* ou *hashsum*[108].

A função Hash é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções *Hash* são conhecidas por resumirem o dado. A principal aplicação dessas funções é a comparação de dados grandes ou secretos[109]. Dessa forma, as funções *Hash* são largamente utilizadas para buscar elementos em bases de dados, verificar a integridade de arquivos baixados ou armazenar e transmitir senhas de usuários.

Temos, então, que a tecnologia *Hash* apresenta-se como possibilidade de minimização dos impactos que esse sistema pode causar, por diminuir muito a simplicidade da transferência de dados, o que facilita a percepção de dados alterados.

Com essa tecnologia sendo alcançada nessas plataformas, carros e casas passam a enviar dados criptografados, e resistentes a ataques brutos, o que dificultaria a ação de criminosos, já que o próprio sistema dessa tecnologia é desfavorável a ataques cibernéticos. Também convém frisar que o alcance desses dados já é visto em tecnologias que vão além dos terminais computacionais, o que nos traz a percepção de que bastaria um olhar para as plataformas automobilísticas e habitacionais, para que de pronto chegassem aos confortos dos lares e veículos.

---

108 PISA, Pedro. O que é Hash? **Techtudo,2012.** Disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html>. Acesso em: 12 jul.2018.

109 PEREIRA, Ana Paula. O que é hash?**Tecmundo, 2009**. Disponível em:<https://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm>. Acesso em: 11 jul. 2018.

4.2. *WI-FI MESH*

A rede Mesh também é um Sistema que se mostra alternativo ao atual, buscando melhorias de segurança.

A rede *mesh* sem fio consiste em pontos de rádio – chamados de "nós" - organizados em uma topologia em malha – e daí advém o nome "*mesh*". As redes *mesh* são compostas de clientes, roteadores e portais mesh, que distribuem o sinal de *Wi-Fi* de forma uniforme e sólida em torno do ambiente desejado, seja um escritório, ou até mesmo uma casa. Em redes *mesh*, os roteadores se conectam entre si e enviam o sinal *Wi-Fi* de um para outro, bem como, para a área que os rodeia. Basicamente, é como um cobertor de retalhos que cobre todo o espaço[110].

Funciona de forma diferente do *Wi-Fi* comum que, quando ausente essa tecnologia *mesh*, concentra o sinal emitido ao roteador central - geralmente conectado à via telefônica. Quando esse sinal é enviado, parte de sua "potência" se perde, fazendo com que o próximo receptor tenha menos força que o receptor primário.

Na tecnologia *mesh* a descentralização da transmissão do sinal de *Wi-Fi* que, dessa forma, transforma todos os roteadores em independentes, permitindo que as rotas de envio de sinal sejam aquelas nas quais os dados sejam melhor transferidos, e não a rota que leve ao roteador central – para que esse efetue a conexão com a rede mundial de computadores. Esses pontos intermediários são chamados de "saltos" ou "*hops*" da rede. Cada salto introduzirá certo nível de atraso e, por isso, o ideal é que o número de saltos seja minimizado. O que o usuário da rede *mesh* consegue é transformar esses pontos intermediários em dispositivos de qualidade tão boa quanto o roteador primário, e que funcionem em conexão direta entre si, encontrando o ponto mais direto entre eles[111].

Quando você tem roteadores *mesh* suficientes, se por algum motivo um deles apresentar defeito e desconectar da rede mundial de computadores, o sinal pode encontrar o seu caminho, graças aos nós alternativos à descentralização e à busca constante de melhores rotas. Se o seu telefone estiver conectado ao roteador *mesh* A e está tentando se comunicar com o receptor a cabo conectado ao roteador C, o roteador *mesh* B, que fica entre ambos, irá fornecer uma melhor comunicação[112].

---

110 Portal Netspot. Disponível em:<https://www.netspotapp.com/pt/what-is-mesh-networking.html>Acesso em: 10 agosto 2018.

111 Ibidem

112 NERI, Neto. Conheça a tecnologia WiFi Mesh, que promete resolver problemas de sinal em internet sem fio. **Adrenaline uol,2017**. Disponível em:https://adrenaline.uol.com.br/2017/08/27/51032/conheca-a-tecnologia-wifi-mesh-que-promete-resolver-problemas-de-sinal-em-internet-sem-fio/. Aceso em: 10 agosto 2018.

Assim, da mesma maneira que funciona a internet, temos agora a descentralização como norteadora dos roteadores. Isso equivale a afirmar que a emissão de sinal agora passa a ser descentralizada, onde cada usuário é receptor e transmissor de sinais alheios.

E de que forma a tecnologia *mesh* torna a conexão mais segura? É importante termos a consciência de que um *cyberataque* em regra congestiona a conexão. É natural que a entrada de novos dispositivos – em especial os maliciosos – tenda a sobrecarregar os canais de transmissão de dados.

Quando isso ocorre na tecnologia *Wi-Fi* comum, a única rota presente é aquela sobrecarregada por algum dispositivo ou programa malicioso; assim, mesmo com a conexão mais lenta, os sistemas operacionais buscam manter-se conectados e utilizar essa rota para transmissão de dados. Isso expõe o aparelho utilizado como terminal de conexão com a *internet*, que abre os canais de comunicação para enviar e receber dados e, dessa forma, permite a entrada de algo que possa gerar malefícios ao usuário.

Na tecnologia *mesh*, isso funciona um pouco diferente. A informação transmitida, então, passa a buscar as melhores rotas. E, ao encontrar um caminho com o peso da ação de um criminoso cibernético, ao invés de buscar manter-se naquela trajetória e abrir o sistema aos programas maliciosos utilizados por eles, as informações simplesmente buscarão uma rota mais limpa, rápida, o que amplia a segurança do usuário.

4.3. LI-FI

Outra alternativa que dificultaria a ação dos criminosos cibernéticos é a popularização da tecnologia *Li-Fi*. Capaz de ser até 250 vezes mais rápida que a tecnologia Wi-Fi, a Li-Fi tem seu funcionamento com algumas características que a tornam um pouco mais segura. O *Li-Fi* funciona de formar similar ao conhecido Wi-Fi, mas usando as ondas de luz em lâmpadas especiais feitas em LED, em um sistema que recebe sinais de comunicação ao ligar e desligar essas lâmpadas em um período de nano segundos.

Apesar de as luzes precisarem ficar ligadas para transmitir os dados, elas podem ser reguladas a um ponto invisível para os olhos; contudo, essa medida diminui o seu alcance. Também importa mencionar que cada lâmpada é capaz de oferecer conectividade para até quatro computadores[113].

Enquanto o *Wi-Fi* requer circuitos de rádio, antenas e receptores mais complexos, a *Li-Fi* utiliza métodos de modulação semelhantes aos raios infraver-

113 DÂMASO, Lívia. Entenda o que é Li-Fi, Internet à luz que pode substituir o Wi-Fi. **Techutudo,2014**. Disponível em :<https://www.techtudo.com.br/noticias/noticia/2014/09/entenda-o-que-e-li-fi-internet-luz-que-pode-substituir-o-wi-fi.html>. Acesso em:10 agosto 2018.

melhos, tais como os controles remotos. As lâmpadas de LED agem como semicondutores e a saída óptica pode ser modulada em velocidades altas capazes de serem detectadas em dispositivos fotodetectores, e convertidas de volta para a corrente elétrica[114]. Por isso, a tecnologia *Li-Fi* é extremamente veloz, além de ser mais segura.

Como se nota, a utilização da luz como plataforma de transmissão de dados é um sistema eficiente de segurança, na medida em que exige que os invasores estejam ao alcance das luzes ou seja, o *hacker* teria que estar dentro do domicílio, ou do carro, para adentrar nesse sistema e invadir as informações do usuário; ou, em trabalho ainda maior, teria que invadir o código-fonte, ou os cabos das provedoras de internet.

Contudo, o *Li-Fi* tem suas desvantagens. O usuário precisaria estar com a luz ligada – ainda que em baixa frequência – para utilizar seus aparelhos domésticos. E mais, as possibilidades de um emissor de *Li-Fi* transgredir os cômodos da casa são baixas, já que as frequências de luz não atravessam paredes.

4.4. EDUCAÇÃO DIGITAL

O avanço tecnológico e a explosão da internet trouxeram um mundo de possibilidades diante de nossos olhos; surgem, a todo momento, muitas ferramentas que tornam o nosso cotidiano mais prático. Contudo, assim como em outras áreas, a tecnologia trouxe ameaças, muitas pessoas utilizam as facilidades geradas pela internet para cometerem crimes. Temos o direito de usufruir dos benefícios oferecidos pela internet com segurança e tranquilidade, porém, devemos fazer o uso consciente da rede de maneira sadia. A conscientização do uso responsável da rede é o caminho para redução de crimes virtuais.

Anualmente é celebrado o Dia da Internet Segura (Safer *Internet Day)*, uma ação mundial onde Instituições, empresas, agentes e usuários da *web,* em centenas de países, promovem ações nas redes, escolas, universidades, Ong's para conscientização e estimulação das boas práticas de navegação, uso ético, seguro e responsável da *Web*[115]. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil criou guias para utilização da internet segura e promove ações que disseminam e incentivam a leitura desses materiais, que são disponibilizados no seu site[116]. O compartilhamento de materiais educativos e promoções de ações

114 DÂMASO, Lívia. Entenda o que é Li-Fi, Internet à luz que pode substituir o Wi-Fi. **Techutudo,2014.** Disponível em :<https://www.techtudo.com.br/noticias/noticia/2014/09/entenda-o-que-e-li-fi-internet-luz-que-pode-substituir-o-wi-fi.html>. Acesso em:10 agosto 2018.

115 **SAFERNET ORG**. Disponível em:<http://www.safernet.org.br/site/sid2018/o-que-e>. Acesso em: 04 dezembro 2018.

116 **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**. Disponível em: <https://www.cert.br/>. Acesso em: 04dezembro 2018.

deve ser realizado continuamente, pois é um modo eficaz de auxiliar a sociedade a edificar um ambiente digital mais protegido contra os criminosos.

O Comitê Gestor de Internet no Brasil (CGI.BR) idealizou o Portal Internet Segura que reúne materiais para conscientização sobre segurança e uso responsável da Internet no país, com foco em diferentes públicos: crianças, adolescentes, pais, responsáveis e educadores[117].

Segundo Daniel Ackerman, coordenador do Departamento de Propriedade Intelectual da Justiça dos Estados Unidos, desenvolver um trabalho de educação digital com a população pode ser um dos caminhos para diminuir o número de crimes cibernéticos[118].Ou seja, através da educação, juntamente com a cooperação de cada cidadão com uso consciente e responsável podemos prevenir e reduzir os ataques virtuais. A prevenção é a melhor forma de evitar esses atos criminosos, e é possível, através da educação e do conhecimento.

5. CONCLUSÃO

Passamos por um momento de transição no comportamento da sociedade, em adaptação às mudanças tecnológicas. Também é notório que essas mudanças buscam cada vez mais a comodidade dos usuários, que veem com ótimos olhos a chegada da tecnologia como elemento facilitador em suas vidas.

Contudo, também vemos que a despreocupação perante a chegada da tecnologia traz imensas vulnerabilidades, em especial a falta de educação digital e ausência de medidas simples de segurança – como uma simples troca de senha. Assim, os sistemas que saem vulneráveis de suas fábricas continuam com segurança fragilizada em seu uso e, dessa forma, facilmente atacados por *hackers*.

É claro que a vulnerabilidade dos sistemas possui nas fabricantes uma parcela da responsabilidade. Contudo, atribuir-lhes a culpabilidade pelos crimes citados é o caminho? Deveríamos obrigar as empresas a excluir tecnologias frágeis – como o *bluetooth* – em um mercado cada vez mais competitivo e com consumidores cada vez mais necessitados das benesses que essas conexões podem causar? Por outro lado, vale a pena expor esses mesmos consumidores a uma vulnerabilidade tão perigosa? Ou devemos arrumar meios que obriguem as fabricantes a fiscalizarem constantemente cada linha de código dos seus produtos comercializados, dentre bilhões, ou até trilhões, a serem supervisionadas por minuto?

Constata-se que a solução seria a atualização dos critérios de segurança das redes como um todo, aliada a uma educação digital mais forte. Não apenas

117 **Portal Internet Segura.** Disponível em:<https://internetsegura.br/sobre/. Acesso em: 04 dezembro 2018.

118 **FIESP**. Disponível em:< http://www.fiesp.com.br/noticias/tecnologia-digital-se-transforma-rapidamente-e-dificulta-a-prevencao-de-crimes-ciberneticos/>. Acesso em: 04 dezembro 2018.

creditar os fabricantes – seja qual for a tecnologia – mas também os usuários. Compreender que os avanços tecnológicos também trazem perigos, e que precisam de vigilância constante.

De tudo isso, dois pontos merecem especial destaque. O primeiro deles é que os interesses do consumidor devem ser vistos além do que os próprios consumidores veem. Não é porque as tecnologias hoje são amplamente utilizadas, que devemos mantê-las em suas fragilidades essenciais para não perder espaço no mercado - afinal, tal pensamento não permitiria avanço tecnológico algum.

Devemos ter, a princípio, um avanço tecnológico que permita as mesmas comodidades, porém por caminhos que sejam mais seguros. Esses, sim, serão os caminhos que dificultarão a ação de criminosos.

O segundo ponto consiste em entendermos que os consumidores necessitam de uma compreensão do quanto às tecnologias que usam. Quem hoje adquire um automóvel, nem cogita as informações que serão coletadas e os perigos que passa por não atualizar o sistema ou não trocar a sua senha; há consumidores que buscam no dicionário o significado da palavra "*backup*", algo crucial para a segurança digital em microssistemas – imagine os macrossistemas que abrangem um veículo automotor.

Aqui, as próprias fabricantes colaboram para essa "ignorância digital", pois quanto menos o consumidor souber dos perigos que corre, mais encantado e motivado a consumir ele estará. Isto implica, nos ditames do sistema capitalista, que dificilmente o livre mercado buscará a modificação desse panorama, restando a intervenção estatal como alternativa a isso.

Em outras palavras: é preciso uma legislação urgente, de autoridades atuantes que saibam o quanto a população está sujeita a verdadeiras atrocidades no que diz respeito ao uso das tecnologias. Ao passo que essa mesma legislação também deve ser redigida cautelosamente, pois a dinâmica da evolução computacional poderá rapidamente trazer novas tecnologias que se esquivem das letras da lei, e mantenham os perigos aos usuários. Diante disso, torna-se imprescindível o dinamismo entre as novas condutas em meio virtual e as normas jurídicas, objetivando a segurança jurídica e social.

Contudo, tal panorama beira a utopia. É notório que, na realidade brasileira, o conhecimento da tecnologia, informação e ciência computacional interessa a poucos, sendo difícil vermos surgir da política alguém com força para mudar essa realidade.

Por fim, ressalta-se que o exaurimento da temática nesse momento é impossível, visto que é um tema em constante metamorfose e com distintas ramificações, que vão além das apresentadas neste artigo.

REFERÊNCIAS

ABOWD, G.D. *Classroom 2000: **An experiment with the instrumentation of a living educational environment.*** IBM Systems Journal, v. 38, 1999.

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out.2001. Disponível em: <https://jus.com.br/artigos/2250>. Acesso em: 01 set. 2018.

ARAUJO, Regina Borges. Computação Ubíqua, Princípios, Tecnologias e Desafios - XXI Simpósio Brasileiro de Redes de Computadores. 2003. http://twiki.im.ufba.br/pub/MAT570/LivroseArtigos/045_AraujoRB.pdf. Acesso em 12 de maio 2018.

ARAÚJO, R. B. (2003). Computação Ubíqua: Princípios, Tecnologias e Desafios. In: XXI Simpósio Brasileiro de Redes de Computadores. (Org.). 1 ed. Natal – RN: SBRC2003, p.45 – 115.

AREIAS, Mariana. Dependência de tecnologia: conheça a doença do futuro. **Metrópoles, 2017.** Disponível em:<https://www.metropoles.com/vida-e-estilo/bem-estar/saude-bem-estar/dependencia-de-tecnologia-conheca-a-doenca-do-futuro>. Acesso em: 15 outubro 2018.

BRADICICH, Tom. **HP**, 2017. *IoT Research Study*. Disponível em: <https://community. hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.U9exjfldXtt>. Acesso em: 10 jul. 2018.

BARRETO Junior, Irineu. Atualidade do Conceito de Sociedade da Informação para a Pesquisa Jurídica. *In*: PAESANI, Liliana Minardi (Coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

BARROS, Tiago. Lâmpadas inteligentes são hackeadas para furto de senhas de Wi-Fi**. Techtudo**, 2014.Disponível em: <https://www.techtudo.com.br/noticias/noticia/2014/07/lampadas-inteligentes-sao-hackeadas-para-furto-de-senhas-de-wi-fi.html>. Acesso em :10 jul. 2018.

BRASIL.**CONSTITUIÇÃO FEDERAL**. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 28 jul. 2018.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 20 agosto 2018.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm >. Acesso em 20 de agosto 2018.

BRASIL. Lei nº 9.296, de 24 de Julho 1996. Disponível em:<http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em 20 de agosto 2018.

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Disponível em:< http://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em 20 de agosto 2018.

BRASIL. Lei nº 9.983. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm>. Acesso em: 20 de agosto 2018.

BRASIL. Lei nº 11.829, de 25 de Novembro 2008. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 20 de agosto 2018.

BRASIL. Lei nº 12.034, de 29 de setembro de 2009. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12034.htm>. Acesso em: 20 de agosto 2018.

BRASIL. Lei nº12.735, de 30 de novembro de 2012.Disponível em:http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 20 agosto 2018.

BRASIL. 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 >. Acesso em: 20 de agosto 2018.

BRASIL. 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 >. Acesso em 20 de agosto 2018.

BRASIL. Lei nº 10.764, de 12 de Novembro de 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/L10.764.htm. Acesso em: 20 de agosto 2018.

CAMARGO SANTOS, Coriolano Alberto de Almeida; FRAGA, Ewelyn Schoots. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico**. 2.ed.SãoPaulo.OAB/SP, 2010.Disponível em:< http://www.oabsp.org.br/comissoes2010/direito-eletronico-crimes-alta-tecnologia/livro-sobre-crimes-eletronicos/livro.pdf/download+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em 10 jul. 2018.p.09

CARVALHAL, Aline.8 coisas que você nunca acreditaria que *hackers* pudessem fazer**. Techtudo,2011.** Disponível em:<https://www.techtudo.com.br/noticias/noticia/2011/09/8-coisas-que-voce-nunca-acreditaria-que-hackers-podem-fazer.html >. Acesso em: 10 jul. 2018.

CRESPO, Marcelo Xavier de Freitas. ***Crimes Digitais***. São Paulo: Editora Saraiva, 2011.

DÂMASO, Lívia. Entenda o que é Li-Fi, Internet à luz que pode substituir o Wi-Fi. **Techutudo,2014**.

Disponível em :<https://www.techtudo.com.br/noticias/noticia/2014/09/entenda-o-que-e-li-fi-internet-luz-que-pode-substituir-o-wi-fi.html>. Acesso em:10 agosto 2018.

DEIVISON, Pinheiro Franco. *Investigação de Crimes Cibernéticos - A Carreira da Computação Forense*. *Revista da Sociedade Brasileira de Computação* - Horizontes, v. 5, 2012.

De longe, hackers 'invadem' e controlam carro com jornalista dentro. **G1**,2015. Disponível em: <http://g1.globo.com/carros/noticia/2015/07/de-longe-*hackers*-invadem-e-controlam-carro-com-jornalista-dentro.html >. Acesso em: 12 jul. 2018.

DIAS, Diego. *Quadrilha de hackers especializada no roubo de Jeeps é presa***. Quatro rodas**, 2016.

Disponível em: < https://quatrorodas.abril.com.br/noticias/quadrilha-de-*hackers*-especializada-no-roubo-de-jeeps-e-presa/>. Acesso em: 10 jul. 2018.

DREY, Ramiro Fetzner. TI especialistas,2015. Disponível em: <https://www.tiespecialistas.com.br/definicao-e-principios-da-computacao-ubiqua/> Acesso em 27 de jul. 2018

FERREIRA, Ivete Senise. *A criminalidade informática*. In Direito & internet: aspectos jurídicos relevantes. Bauru: Edipro, 2011.

GOODMAN, Marc. **Future Crimes: Tudo Está Conectado, Todos Somos Vulneráveis e o que Podemos Fazer Sobre isso.** São Paulo: Editora HSM ,2015.

*Vídeo: polícia flagra 'furto hacker' de carro sem as chaves***. G1,**2017**.** Disponível em:< https://g1.globo.com/carros/noticia/video-veja-como-e-o-furto-*hacker*-de-carro-sem-as-chaves.ghtml>. Acesso em: 12 jul. 2018.

Cibercriminosos monitoram sistemas de empresas terceirizadas para obter informações de seus alvos. Disponível em: <https://tecnologia.ig.com.br/2014-04-26/*hackers*-exploram-falhas--em-sistemas-de-ar-condicionado-e-maquinas-de-salgados.html. Acesso em: 12 jul.2018

GOMES, Luiz Flávio. Crimes informáticos. 10 dez. 2000. Disponível em:< http://www.ibccrim.org.br>. Acesso em: 14 jul. 2018.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim IBCCRIM, v. 8, 2000.

HERRTWICH, R. G. **Ubiquitous Computing in the Automotive Domain**. Proceedings of the Pervasive Computing – First International Conference, 2002.

JESUS, Damásio E. de**. Manual de Crimes Informáticos**. 1 ed. São Paulo: Saraiva, 2016.1 ed. p.50-52.

KAHL, Marcelo; FLORIANO, Diogo. **Computação ubíqua, tecnologia sem limites**. Vale do Itajaí SC,2012. Disponível em:<http://www.ceavi.udesc.br/arquivos/id_submenu/387/diogo_floriano_marcelo_kahl_computacao_ubiqua.pdf>. Acesso em: 10 de maio 2018.

LEME, José Antônio. Conheça os benefícios da indústria 4.0. **Estadão, 2018**.

Disponível em:<https://jornaldocarro. estadao.com.br/carros/conheca-os-beneficios-da-industria-4-0/ >. Acesso em 07 agosto 2018

LIMA, Paulo Marco Ferreira. **Crimes de Computador e Segurança Computacional**. São Paulo: Editora Atlas, 2011.

LOUREIRO, Antônio AF et al. Comunicação ao Sem Fio e Computação ao Móvel: Tecnologias, Desafios e Oportunidades. Disponível em: <https://homepages.dcc.ufmg.br/~loureiro/cm/docs/jai03.pdf>-. Acesso em 24 de jun. 2018.

LÓSSIO, Claudio Joel Brito; SANTOS, Coriolano Aurélio Almeida Camargo. Breve comentário sobre a internet das coisas a luz do direito penal brasileiro. **E DE DIREITO**, p. 15, 2018.Disponível em:< http://www.portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/issue/download/274/42#page=16 >. Acesso em: 26 ago.2018.

MALACARNE, Juliana. *Hacker invade babá eletrônica de menino de 1 ano*. **Revista Crescer**, 2016. Disponível em: <https://revistacrescer.globo.com/Bebes/Seguranca/noticia/2016/01/*hacker*-invade-baba-eletronica-de-menino-de-1-ano.html>. Acesso em: 10 jul. 2018.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova – A investigação criminal em busca da verdade**. Curitiba: Juruá Editora, 2012.

MOREIRA, Rene. *Hackers* atacam sistema de Santa Casa de Pirajuí (SP) e exigem bitcoins. **O Estadão,**2018. Disponível em:< https://sao-paulo.estadao.com.br/noticias/geral,*hackers*-atacam-sistema-de-santa-casa-de-pirajui-sp-e-exigem-bitcoins,70002426223>. Acesso em: 10 agosto 2018.

WEISER, Mark. **The computer of 21st century. Scientific American,** jan. 1991. < Disponível em: http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>. Acesso em: 12 de maio de 2018

Wi-Fi Alliance. Disponível em <https://en.wikipedia.org/wiki/Wi-Fi_Alliance>. Acesso em 15 de jul. 2018.

PEDROSO, Fernando de Almeida. Direito Penal - Parte Geral: Estrutura do Crime. LEUD: São Paulo, 1993.

PEREIRA, Ana Paula. O que é hash?**Tecmundo, 2009**. Disponível em:<https://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm>. Acesso em: 11 jul. 2018

PINHEIRO, Emeline Piva. *Crimes virtuais: uma análise da criminalidade informática e da resposta estatal*. Santa Catarina: UFSC, 2006, p.14. Disponível em: <http://www.egov.ufsc.br/portal/ sites/default/files/anexos/29397-29415-1-PB.pdf>. Acesso em: 16 jan. 2017.

PINHEIRO, Mauro; SPITZ, Rejane**. O design de interação em ambientes de ubiqüidade computacional**. In: Congresso Internacional de Design da Informação. 2007. Disponível em:<http://www.academia.edu/801383/O_design_de_intera%C3%A7%C3%A3o_em_ambientes_de_ubiq%C3%BCidade_computacional >. Acesso em: 05 de maio 2018.

PINHEIRO, Patrícia Peck. *Direito Digital*. São Paulo: Editora Saraiva, 2013.

PIOVESAN, S, D. et al. **Modelagem de um Framework para M-Learning**. In: *XXI Simpósio Brasileiro de Informática na Educação*, Paraíba, Brasil, 2010. PERTMED - Sistema de TeleMedicina Móvel, disponibilizando a informação onde ela é necessária. Disponível em:<http://pertmed.wkit.com.br/pertmed/doku.php>. Acesso em 12 de maio 2018.

PISA, Pedro. O que é Hash? **Techtudo,2012.** Disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-hash.html>. Acesso em: 12 jul.2018.

ROCHA, C. L., Costa, C. A., Righi, R. R. ***Um modelo para monitoramento de sinais vitais do coração baseado em ciência da situação e computação ubíqua***. VII Simpósio Brasileiro de Computação Ubíqua e Pervasiva, Pernambuco, 2015.

ROMERO, Luiz. Não li e concordo. **Super Abril, 2017.** Disponível em:< https://super.abril.com.br/tecn ologia/nao-li-e-concordo/>. Acesso em: 12 out 2018.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002.

ROSA, Nathalie. *Família descobre que estava sendo observada por uma babá eletrônica***. Canaltech,** 2018.Disponível em: <https://canaltech.com.br/*hacker*/familia-descobre-que-estava-sendo-observada-por-uma-baba-eletronica-115350/ >. Acesso em: 10 jul. 2018.

ROUSSOS, George. Ubiquitous Computing for Electronic Business. In: ROUSSOS, G. (Ed.). *Ubiquitous and Pervasive Commerce*: New Frontiers for Electronic Business. Springer, 2006.

SALMI, Deborah. *Ransomware ataca computador do hotel e sistema de cartão chave*. **Avast**, 2017.Disponível em:< https://blog.avast.com/ransomware-attacks-hotel-computer-and-keycard-system>. Acesso em: 10 de jul. 2018.

SANTAELLA, Lucia. **Comunicação Ubíqua - Repercussões na Cultura e na Educação.** São Paulo: Paulus, 2013.

SANTANA, Reinaldo Costa. Computação móvel, histórico da evolução. **São Paulo**, 2008. Disponível em:<http://grenoble.ime.usp.br/~gold/cursos/2008/movel/mono/Historico-ComputacaoMovel.pdf>. Acesso em 03 de jul. 2018.

SILVA, Débora. Computação ubíqua: a informática no cotidiano das pessoas. Disponível em:<https://www.estudopratico.com.br/computacao-ubiqua-a-informatica-no-cotidiano-das-pessoas>. Acesso em: 01 de jul. 2018.

SILVA, Everton et al. Computação Ubíqua–Definição e Exemplos. **Revista de Empreendedorismo, Inovação e Tecnologia**, v. 2, n. 1, p. 23-32, 2015. Disponível em:< https://seer.imed.edu.br/index.php/revistasi/article/view/926 >. Acesso em: 20 de abril de 2018.

SOUZA, Lisandro Carmona de. Rifles de precisão: a Internet das Coisas Controlada por *Hackers*. **Avast, 2015**.Disponível em:https://blog.avast.com/pt-br/2015/08/09/rifles-de-precisao-a-internet-das-coisas-controlada-por-*hackers*/. Acesso em: 25 jul. 2018.

VENTURA, Felipe. Cama inteligente monitora seu sono para ajustar o colchão e sugerir novos hábitos. Gizmodo, 2016.Disponível em:< https://gizmodo.uol.com.br/cama-inteligente-ces-2016/>. Acesso em: 27 de jul. 2018.