A RESPONSABILIDADE CIVIL E PENAL DOS ENVOLVIDOS EM SEQUESTROS DIGITAIS EM FACE DA LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS

Júlia Fernandes de Mendonça[*]

RESUMO: O artigo tem por objetivo fazer uma análise dos envolvidos em sequestros digitais sob a perspectiva penal e as infrações configuradas, bem como sob a perspectiva cível e as leis esparsas que compõem o arcabouço brasileiro sobre proteção de dados. Faz-se, de igual maneira, uma relação da nova Lei 13.709/2018 com o objeto do artigo. O estudo compreende, ainda, uma análise sobre a responsabilização civil que pode ser imputada a partir de tal lei. A técnica utilizada nesta pesquisa é a de documentação indireta através de pesquisa bibliográfica e documental. Para tanto, foi necessária a utilização de documentos públicos tais como leis, pareceres jurídicos, informes estatísticos e informações disponíveis em sites, somando-se ainda pesquisa de bibliográfica de livros, artigos e periódicos.

PALAVRAS-CHAVE: Sequestro digital; Proteção de dados pessoais; Responsabilidade civil.

ABSTRACT: The article aims to make an analysis of those involved in digital hijacking from the criminal perspective and the configured infractions, as well as from the civil perspective and the sparse laws that make up the Brazilian data protection framework. A relation between the new Law 13.709 / 2018 and the object of the article is also made. The study also includes an analysis of civil liability that can be imputed from such law. The technique used in this research is that of indirect documentation through bibliographic and documentary research. Therefore, it was necessary to use public documents such as laws, legal opinions, statistical reports and information available on websites, in addition to a bibliographic search of books, articles and periodicals.

KEYWORDS: Digital hijacking; Protection of personal data; Civil responsibility.

[*] Graduanda pela Faculdade de Direito da Universidade Federal da Bahia (UFBA).

1 INTRODUÇÃO

Em uma sociedade na qual qualquer informação está a apenas um "clique" de distância, várias ações cotidianas migraram para o mundo virtual, tais como, fazer compras no supermercado, escrever uma agenda com as atividades diárias, resolver situações de trabalho, culminando, tudo isso, para um dia a dia no qual o compartilhamento e o consumo de dados é feito em tempo integral. Ocorre que, para tanto, expomos online diversas informações pessoais, endereços, números de cartões de crédito e até dados bancários.

Essa exponencial exposição torna os usuários, pessoas físicas e jurídicas, e seus respectivos dispositivos informáticos demasiadamente vulneráveis, ao passo que a toda a tecnologia e fornecimento de dados proporciona um ambiente atrativo para a prática de crimes. Variadas espécies destes foram criadas e outras ganharam uma nova roupagem dentro do mundo virtual, como, por exemplo, os sequestros digitais. Esses sequestros normalmente ocorrem por motivações diversas, seja para coagir o usuário de alguma forma ou, na sua configuração mais comum, para obter vantagem financeira ao ser estabelecido um tipo de "regaste" (normalmente pago em moeda virtual).

Em geral, os sequestradores invadem o dispositivo da vítima por meio de vírus de computador, coletando informações e criptografando dados para impedir o acesso à máquina, como ocorre nos ataques de *ransomware*. O estudo desse tema é de grande relevância, visto que esses *cibercriminosos* estão ampliando gradativamente seu rol de vítimas, incluindo também hospitais, tribunais, grandes empresas e arquitetando ataques de âmbito mundial. À vista disso, o entendimento acerca da figura dos sequestros digitais, bem como da responsabilização tanto cível, quanto penal, de forma detalhada, pode auxiliar na prevenção contra os mesmos, evitando que a impunidade prevaleça e mais vítimas sejam afetadas.

2 OS SEQUESTROS DIGITAIS: ALGUNS CASOS REAIS

Indivíduos com mesmas visões de mundo e opiniões semelhantes nunca puderam se organizar com tanta rapidez e destreza como conseguem atualmente por meio da internet e páginas online. Tal conjuntura, somada aos ânimos inflamados causados pela dicotomia político-ideológica brasileira e com a velocidade inerente à sociedade da informação (CASTELLS, 2009), ocasionam, cada vez mais, em diversos protestos e manifestações nos sítios de internet.

2.1 Caso do grupo do Facebook - "Mulheres contra Bolsonaro" e o roubo das informações

No segundo semestre de 2018, durante ápice das eleições presidenciais, uma mulher baiana resolveu tomar uma iniciativa após as questionáveis declarações do presidenciável à época, Jair Messias Bolsonaro. No dia 20 de agosto de 2018, a publicitária Ludmila Teixeira

criou um grupo denominado "Mulheres contra Bolsonaro", visando, conforme explicou em sua primeira ação no grupo[1], promover um debate político e social exclusivo para mulheres. Ocorre que, em apenas quinze dias, o grupo tomou gigantescas proporções, alcançando a marca de dois milhões de integrantes. Dessa forma, diante da magnitude alcançada em tão pouco tempo, outros grupos, de ideologias antagônicas, passaram a atacar a criadora e outras mulheres colaboradoras do projeto, que tiveram suas contas pessoais invadidas, incluindo e-mails e até aplicativos, como, por exemplo, o *WhatsApp*.

Em um dos seus relatos para o site de notícias "Catraca Livre"[2], ela desabafou: "[...] o que parecia uma grande oportunidade de aprofundarmos politicamente nossos anseios e medos do pleito eleitoral, virou um verdadeiro pesadelo em nossas vidas. Estão invadindo nossas contas pessoais na internet, hackeando desde o nosso WhatsApp ao Hotmail, o meu número pessoal de telefone foi resgatado em outra cidade que nunca nem coloquei os pés". Além de tudo isso, ela ainda precisou sair do aludido grupo, sob orientações do Facebook, passando a desativar sua conta. Conforme seu próprio relato, ela estava, sem dúvidas, com uma "mordaça virtual", se tornando mais uma vítima dos ataques furtivos dos sequestradores digitais.

Em nossa definição, o sequestro digital se resume na invasão de um dispositivo informático para obter senhas, documentos ou informações pessoais de seu dono, seja ele um usuário particular ou uma pessoa jurídica, tanto de direito público quanto privado. Essa prática consiste, em suma, na contaminação de um dispositivo informático por meio de um *malware*[3], que pode ser inserido de maneiras diversas, coletando informações da máquina e podendo, inclusive, criptografar seus dados. Dessa forma, os sequestradores passam a ter o controle de todo o conteúdo do dispositivo, impossibilitando o acesso do usuário.

As formas de invasão podem variar de acordo com a finalidade e o perfil da vítima, consistindo, usualmente, em ataques personalizados. O *malware* mais comum é denominado *ransomware*[4] e costuma ser o personagem principal nos ataques de grandes proporções dos sequestradores. Esse tipo de contaminação geralmente ocorre por meio de *sites* já infectados que se aproveitam das falhas de segurança do dispositivo, realizando *downloads* sem que o usuário perceba, os chamados *download drive-by*. A partir daí o *malware* faz uma varredura de todo o conteúdo da máquina, desabilitando qualquer possibilidade de contenção ou reversão do ataque. Dessa forma, os arquivos, planilhas, sites visitados, senhas e imagens são criptografados, bloqueando o seu acesso e, consequentemente, para conseguir acessar de novo

[1] VIGNÁ, Júlia. Criado por baiana, grupo de mulheres contra Bolsonaro no Facebook sofre ataque cibernético. *Correio da Bahia*. Disponível em: https://www.correio24horas.com.br/noticia/nid/criado-por-baiana-grupo-mulheres-contra-bolsonaro-no-facebook-sofre-ataque-cibernetico/. Acesso em: 23 jul. 2019.
[2] CRIADORA do grupo contra Bolsonaro: 'Sou uma sequestrada digital". Op. cit.
[3] REGAN, Joseph. *Programa malicioso ou software malicioso, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita*. Disponível em: https://www.avg.com/pt/signal/what-is-malware/. Acesso em: 23 jul. 2019.
[4] *TIPO de software nocivo que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido*. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 23 jul. 2019.

seus dados, as vítimas são compelidas a pagar uma quantia, por meio de criptomoedas[5]. Essa configuração é a mais comum nos sequestros digitais, consistindo na usurpação dos dados pessoais informáticos das vítimas, para obter vantagem financeira.

No entanto, apesar de recorrente, tal modelo não é o único. Conforme exposto no caso do grupo do Facebook, é possível verificar que as invasões tiveram uma motivação ideológica, objetivando não apenas afetar a individualidade da criadora do grupo, mas também atacar toda uma coletividade que compartilhava daquela visão sobre o cenário político à época. O citado ataque foi, na sua essência, alegórico, visando demonstrar "discordância" dos ideais apresentados.

2.2 Extorsão e invasão de dispositivo informático em outras situações

Diante da constante inserção da tecnologia no dia a dia, vários âmbitos da realidade humana foram virtualizados, inclusive, os crimes. Essa modernização dos delitos expõe, cada vez mais, a vulnerabilidade dos sistemas e dispositivos informáticos, culminando, como ocorreram nos últimos anos, em ataques de proporções gigantescas, com gravíssimas violações perpetradas pelos *cibercriminosos*, incluindo sequestros e extorsões digitais que atingiram todo o globo.

Em meados de 2017, ocorreu um dos maiores casos de sequestro de dados já registrado. Iniciando seu ataque pela Espanha e Reino Unido, o *ransomware* denominado "*Wannacry*", aproveitou-se de uma falha no sistema operacional *Windows* para se infiltrar e sequestrar dados em redes de todo o mundo, afetando mais de 150 países e fazendo aproximadamente 200.000 vítimas[6]. O principal fator motivador de tamanho dano sucedeu-se devido ao atraso existente entre os avanços conquistados contra as ameaças digitais e a efetiva implantação nos sistemas de segurança.

A supracitada morosidade se tornou ainda mais evidente, ao passo que a referida praga virtual paralisou mais de 16 hospitais no Reino Unido[7], atingiu a empresa de veículos francesa chamada *Renault*[8], bem como a multinacional de telecomunicações Telefônica S/A. Durante o ataque, o qual foi direcionado principalmente à pessoas jurídicas, as vítimas tiveram seus arquivos criptografados, ficando impossibilitadas de acessá-los, e chegando a ter que paralisar as suas produções[9] até o pagamento da quantia solicitada. A ideia dos sequestradores é que os valores cobrados pelos "resgates" sejam relativamente baixos, para que a empresa prefira pagar

[5] *CRIPTOMOEDAS nada mais do que moedas virtuais, utilizadas para a realização de pagamentos em transações comerciais.* Disponível em https://www.politize.com.br/criptomoedas-o-que-sao-e-como-funcionam/. Acesso em 29 abr. 2020.
[6] CEBRIÁN. Belén Domínguez. Cibertaque: o vírus WannaCry e a ameaça de uma nova onda de infecções. *El País*. Disponível em: https://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html. Acesso em: 12 ago. 2019.
[7]CIBERATAQUE paralisa 16 hospitais do Reino Unido. *El País*. Disponível em: https://brasil.elpais.com/brasil/2017/05/12/internacional/1494602389_458942.html. Acesso em 13 jul. 2019.
[8] ATAQUE afeta quase cem países, de Renault na França a bancos russos. *El País*. Disponível em: https://brasil.elpais.com/brasil/2017/05/13/internacional/1494668788_755982.html. Acesso em 13 jul. 2019.
[9] Ibidem.

o valor estipulado, ao optar por tomar maiores providências. Tal objetivo é fortalecido diante da possibilidade de publicização do ataque e do consequente receio da vinculação da empresa à um status de "insegura", dessa forma, a grande maioria tende a buscar ocultar essas situações dos seus clientes.

No Brasil, diversas pessoas foram afetadas por esse gigantesco ataque. Dentre os casos mais gravosos, o Tribunal de Justiça de São Paulo (TJ-SP) admitiu que foi infectado[10] e procedeu com o envio de *e-mails* aos seus funcionários para determinar o desligamento de suas máquinas, como forma de precaução. Além disso, há relatos[11] que empresas como a Vivo e a Petrobrás também procederam com medidas de segurança semelhantes.

Outro nicho de usuários que também sofreu com sequestros digitais foram os que utilizam dispositivos móveis. No início de 2016, foram registrados diversos casos de infecções por *ransomware* na plataforma *Android*, sendo o principal deles denominado "*Simplelocker*"[12]. Por meio de arquivos que simulam jogos e aplicativos reais e já conhecidos, esse *malware* imita ícones e os nomeia com nomes populares, tais como: "*Adobe Flash Player*" ou "*Video Player*". Dessa forma, a vítima acaba acreditando que se trata do verdadeiro aplicativo e faz o *download* pela "loja virtual" do *Android*, a *Google Store*. A partir daí, o *Simplelocker* se alastra pelo sistema, dificultando o acesso a arquivos e impedindo a utilização da "interface do usuário". Assim, para que a vítima possa retomar o acesso regular dos seus tablets, celulares e dispositivos móveis em geral, ela deve, como de praxe, pagar uma quantia determinada.

Há, ainda, uma outra forma de invasão que o Brasil é líder[13] na quantidade de usuários afetados, o *phishing.* Trata-se de uma fraude eletrônica pela qual dados da vítima são roubados, mediante um sítio ou *e-mail* com informações falsas. O método mais comum é o envio de um *e-mail*, copiando o estilo de comunicação de uma empresa real e confiável, no qual contém *links* que redirecionam para um sítio fraudulento, induzindo o usuário a informar dados e senhas de cartões, bancos e outras credenciais de acesso importantes. Já existem, ainda, registros de *phishing* ainda mais sofisticados[14] que, também via *e-mail*, convidam a vítima a entrar em um sistema de buscas de vagas de emprego, solicitando a instalação de um aplicativo. Entretanto, o que ocorre é o redirecionamento do usuário para um servidor na nuvem, o qual realiza o *download* automático de um instalador semelhante a um arquivo do *Word*, espalhando no dispositivo o trojan bancário denominado Gozi[15].

[10] D'URSO, Luiz Flávio Filizzola; D'Urso, Luiz Augusto Filizzola. Ataque cibernético mundial é a comprovação da insegurança na internet. *Conjur*. Disponível em: https://www.conjur.com.br/2017-mai-17/ataque-cibernetico-mundial-comprova-inseguranca-internet. Acesso em: 01 ago. 2019.
[11] Op. cit. Acesso em: 01 ago. 2019.
[12] BREWSTER, Tom. Simplocker Android malware locks up mobile data and demands a ransom. *The Guardian*. Disponível em: https://www.theguardian.com/technology/2014/jun/05/simplocker-android-ransomware-malware-virus. Acesso em: 01 ago. 2019.
[13] ROHR, Altieres. Brasil é o país com mais usuários atacados por phishing. *G1*. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/05/20/brasil-e-o-pais-com-mais-usuarios-atacados-por-phishing.ghtml. Acesso em: 01 ago. 2019.
[14] RODRIGUES, Renato. Brasil é o País com mais usuários atacados por phishing. *Kaspersky Daily*. Disponível em: https://www.kaspersky.com.br/blog/brasil-ataques-phishing/11826/. Acesso em: 25 jul. 2019.
[15] MALWARE utilizado em roubos financeiros. Disponível em: https://www.enigmasoftware.com/pt/gozitrojan-remocao/. Acesso em: 01 ago. 2019.

Evidente, portanto, estarmos vivenciando uma crescente e diversificada criação de mecanismos para invasão de dispositivos informáticos, sendo necessário que se direcione cada vez mais atenção para o estudo da temática.

3 OS SEQUESTROS DIGITAIS E AS CONSEQUÊNCIAS JURÍDICAS ENGENDRADAS: A ESFERA PENAL

A já citada velocidade que é inerente ao âmbito digital, junto a crescente diversificação das formas de atuação dos *cibercriminosos*, acarreta uma carência de tipificação para os crimes cibernéticos (2016, p.83). Ao longo do tempo, devido a tal contexto fático, foram ocorrendo tentativas de subsumir as condutas dos casos concretos em tipos penais preexistentes. Muitos promotores, por exemplo, nos casos de cópia indevida de dados ou informações, procediam com o oferecimento da denúncia em face do crime de furto (Art. 155, CP). Ocorre que esses tipos de analogia, chamadas por Damásio de Jesus e José Antônio Milagre de "enquadramentos forçosos" (2016, p.83), acabam gerando diversas discussões na doutrina sob a perspectiva da analogia "*in malan partem"* e sob o princípio da reserva legal, sem chegar a um consenso efetivo.

3.1 Infrações penais configuradas

A Lei nº 12.737/2012 que ficou conhecida como "Lei Carolina Dieckmann" e a consequente tipificação do delito de invasão de dispositivo informático, foi importantíssimo para, finalmente, possibilitar um melhor "encaixe" aos crimes relacionados a roubo de dados. O artigo 154 – A do supracitado texto normativo tipifica o ato de invadir dispositivo informático alheio, que esteja conectado ou não à rede de computadores, quando ocorre uma violação indevida de algum mecanismo de segurança, com o objetivo de "obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou instalar vulnerabilidades para obter vantagem ilícita", prevendo, como pena, a detenção, de 3 (três) meses a 1 (um) ano, bem como multa.

Tal tipificação objetivou, em suma, a proteção da intimidade, privacidade e da segurança da informação de indivíduos e empresas, que abrangem também seus respectivos dispositivos informáticos. Damásio de Jesus e José Antônio Milagre, de maneira objetiva, definem o bem tutelado por esse tipo penal, como sendo a "liberdade individual de manter íntegros os dados dispostos em preceito informático", objetivando também manter ilesos os próprios dispositivos, protegidos por mecanismos de segurança de acessos não autorizados que tem por finalidade "a) obter dados (objeto da alteração); b) alterar dados; c) destruir dados; d) instalar vulnerabilidade para obter vantagem ilícita vantagem ilícita" (2016, p.88).

O sequestro digital, objeto do presente artigo, enquadrar-se-ia nesse delito no que concerne aos ataques que não envolvem vantagem financeira, como o caso do grupo "mulheres contra Bolsonaro", ora discutido. Isso porque, a invasão do dispositivo e das contas de *Hotmail*

e *Facebook* das colaboradoras do grupo, com o objetivo de obter informações, já configuraria o delito.

A referida tipificação também foi extremamente importante para o enquadramento dos casos de "*Ransomware as a Service",* ou também conhecido como *"RAAS*". O "*RAAS*" consiste em um modelo de negócio criado por grupos de *hackers* que possibilita a compra e desenvolvimento de um *malware* personalizado, tendo como foco uma vítima específica. Essa comercialização acontece por meio da *darknet*[16] e vem ocorrendo com mais frequência desde 2016, sendo seu público alvo principalmente governos, empresas privadas, ativistas ou até mesmo terroristas. Os cibercriminosos criam "*kits*" que, por meio do método de "tentativa e erro", são adequados aos interesses do contratante. Desse modo, o referido artigo foi extremamente preciso em seu §1º[17], na medida em que incriminou a prática de produzir, oferecer, distribuir e vender a terceiros, programas ou dispositivos de computador que possibilitem a prática da invasão de dispositivo de forma terceirizada.

No entanto, o principal método utilizado na prática dos sequestros, conforme já explicitado, envolve a intenção de obter vantagem financeira, sendo cobrado um tipo de "resgate" para autorizar novamente o acesso aos dados. Tal conduta, quando nesses moldes, se subsume ao crime de extorsão, presente no art. 158 do Código Penal. Isso porque, o delito engloba todas as características de um ataque de sequestro digital mais comum, como, por exemplo, os realizados por meio dos já mencionados *ransomwares*, tendo em vista que consiste basicamente no "constrangimento de alguém", pessoa física ou jurídica, mediante "grave ameaça", bloqueando seu acesso aos dados digitais, visando obter vantagem ilícita, qual seja, o "resgate" pago por *criptomoedas*. Sendo assim, o delito do artigo 154-A do Código Penal se torna o que Nelson Hungria chama de "soldado de reserva", deixando de ser aplicado pela existência de norma penal principal mais gravosa (p. 147 *apud* BITENCOURT, 2012, p. 284).

Por fim, importa salientar que o delito de extorsão é considerado pacificamente pela doutrina como crime formal, portanto, mesmo que o resgate solicitado pelos sequestradores não seja efetivamente pago, o crime já se consumou.

3.2 Posicionamentos doutrinários e jurisprudenciais

Existem inquietações na doutrina acerca da aplicação de alguns tipos penais informáticos no caso concreto. O principal debate gira em torno do delito tipificado pelo artigo 154-A que, apesar de estabelecer uma finalidade de agir por meio do dolo específico de "obter, adulterar ou destruir dados ou informações do titular do dispositivo" ou "instalar vulnerabilidades para obter vantagem ilícita", a doutrina, em sua maioria, entende se tratar de

[16] É o termo usado para classificar partes da internet que estão escondidas e podem ser de difícil acesso sem a utilização de um software especial.
[17] Art. 154 – A, § 1º da Lei 12.737 – "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".

um crime formal, ou seja, apenas o ato de "invadir" o dispositivo já consumaria o delito, configurando todas as outras consequências como um mero exaurimento.

Nesse ínterim, Márcio André Lopes (2012) é taxativo ao discorrer sobre o assunto, asseverando tratar-se de um crime formal que se consuma apenas com a invasão, não se exigindo a ocorrência do resultado naturalístico. Para ele, em verdade, a adulteração ou destruição de dados do titular do dispositivo ou a instalação de vulnerabilidades não precisam efetivamente acontecer para que o crime esteja consumado. De igual maneira, Damásio de Jesus e José Antônio Milagre asseveram que o crime é formal, não importando que finalidade descrita no tipo seja atingida para a consumação (2016, p.93). Para eles, é suficiente apenas a ocorrência da invasão, não importando o resultado. Outrossim, Marcelo Crespo (2015) também coaduna com esse entendimento, concluindo que o crime se consuma mesmo sem a efetiva obtenção, adulteração ou destruição de dados À vista disso, vale destacar que baseando-se nessa parte da doutrina, o caso prático do *Facebook* discutido anteriormente, se enquadraria nesse tipo penal. Isso porque, o crime se consumaria no momento da invasão do dispositivo das colaboradoras do grupo.

Por outro lado, concordando com a parte doutrinária minoritária, Túlio Vianna e Felipe Machado afirmam tratar-se de crime material, visto que só seria consumado com a efetiva leitura, escrita ou execução dos dados do sistema computacional (2013, p.120).

Por fim, para a análise da aplicação ou não desse tipo no caso concreto, vale destacar o julgamento do REsp 1461946, citado por Daiane Fanti Tangerino[18], de relatoria do Ministro do STJ, Sebastião Reis Júnior, publicado em 29 de abril de 2016. A conduta do réu consistiu na posse de um aparato computacional, conhecido como "chupa-cabra", utilizado na captura de dados bancários dos clientes constantes em cartões magnéticos e confecção de outros cartões, nos quais eram inseridos os dados obtidos ilicitamente.

Ocorre que o Ministro Relator julgou que "a conduta atribuída ao réu não constitui delito informático, mas sim crime patrimonial". Em verdade, para ele, houve cometimento de furto qualificado, em continuidade delitiva, com a subtração reiterada de numerário em contas bancárias por meio de cartões magnéticos fraudados (cartões clonados) e não crime informático, nos seguintes termos: "Ora, é de conhecimento notório que a norma em questão, conhecida popularmente como "Lei Carolina Dieckmann", possui o claro e especifico intuito de tipificar e reprimir aqueles delitos ditos informáticos. Entretanto, tem-se que a conduta imputada ao réu constitui, flagrantemente, crime de cunho patrimonial" (excerto do acórdão proferido pelo Tribunal Regional Federal da 5ª Região na Apelação Criminal n. 6.810/PE – 2007.83.08.001065-4) (grifos nossos). Conclui-se, em verdade, que, nessa situação, o delito do art.154-A do CP, foi apenas um crime "meio" para a consumação do delito de furto, sendo, portanto, por este absorvido.

[18] TANGERINO, Daiane Fanti. Invasão de dispositivo informático (art. 154-A, CP) e o STJ. Disponível em: https://canalcienciascriminais.com.br/invasao-de-dispositivo-informatico/. Acesso em: 30 ago. 2019.

4 A RESPONSABILIDADE CIVIL DOS SEQUESTRADORES DIGITAIS COM BASE NO CÓDIGO CIVIL PÁTRIO, NO CDC E NO MARCO CIVIL DA INTERNET

Diante do atual contexto da sociedade da informação, para que seja possível a operacionalização da tutela de proteção de dados dentro do ordenamento, sobretudo antes da Lei 13.709/18, é necessário estabelecer um diálogo entre as leis esparsas, ainda que elas guardem seu fundamento último na Constituição Federal (MARTINS, 2014, p.119). Dessa forma, se faz prudente uma análise conjunta e dialógica, por meio do "diálogo das fontes", combinando variadas leis do ordenamento brasileiro, de modo a formar um sistema coerente e passível de ser aplicado pelo operador do direito (MENDES, 2014, p.192). A aludida teoria, conforme ensinado por Claudia Lima Marques (2017), consiste, em termos simples, na aplicação simultânea, coerente e coordenada das múltiplas fontes legislativas, dentre elas, leis especiais e gerais com campos de aplicação convergentes, mas não iguais.

Nesse ínterim, a partir da compreensão da importância de uma análise conjunta do ordenamento para uma aplicação prática do direito a proteção de dados, principalmente no âmbito civilista, passamos a análise direcionada ao tema deste artigo.

4.1 A incidência do Código Civil de 2002

Como sabido, o Código Civil (Lei 10.406/02) não foi concebido em um contexto com relações digitais tão delineadas, todavia, gerou subsídios primários e gerais para a verificação da responsabilidade dos delitos informáticos, especialmente no que concerne ao âmbito da responsabilidade civil e contratos. Em seu texto legal, foi ensinado que os direitos da personalidade são irrenunciáveis, não sendo admitida qualquer limitação voluntária sobre o exercício desses direitos (Art. 11, CC), exceto nos casos previstos em lei.

Dentre os direitos da personalidade elencados, foi incluído em seu artigo 21, a inviolabilidade da vida privada da pessoa natural, asseverando, inclusive, que o juiz poderá, a requerimento do interessado, adotar as "as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". Deste modo, o Código Civil contribuiu para delinear os caminhos para uma posterior tutela da proteção de dados pessoais no Brasil, visto que "a vida privada" assinalada como inviolável em 2002, guarda grandes relações com o que é partilhado na internet e dispositivos informáticos na atualidade (MENDES, 2014). Além disso, ao direcionar ao judiciário a responsabilidade para conceder as "providências necessárias" nos casos de violação à privacidade, o código abriu um leque primordial para a responsabilização dos que agem de forma a ferir tal direito (MENDES, 2014, p.114). Portanto, o Código Civil estabeleceu as linhas gerais para possibilitar a tutela da privacidade de dados *online*, o que repercute diretamente no tema aqui debatido, sequestros digitais.

4.2 O Código de Defesa do Consumidor

O Código de Defesa do Consumidor (Lei 8.078 de 1990) foi uma das primeiras leis brasileiras que tratou expressamente de alguns aspectos da proteção de dados pessoais, inclusive, versando sobre novas tecnologias de processamento de dados. Trata-se de uma norma destinada à proteção da parte hipossuficiente da relação contratual, com relevante conteúdo principiológico contra os abusos praticados pelos fornecedores de um produto ou serviço (PASSOS, 2017, p.84).

Em seu artigo 43, o CDC inovou ao regulamentar os bancos de dados e cadastros dos consumidores, exigindo o atendimento a parâmetros norteadores legais. Essa imposição de paradigmas basilares visa ajustar o desequilíbrio entres as partes e resguardar a intimidade e privacidade do consumidor, que não possui recursos para se empoderar em face à dinâmica agressiva do mercado. O citado código foi preciso e vanguardista ao lidar com as novas formas de tecnologia e tratamento de dados, inseridos no contexto da sociedade da informação. Ora, diante da modernização e informatização das relações, só é possível concretizar o dever de proteção ao consumidor, mediante o reconhecimento do direito básico à proteção de dados pessoais (MENDES, 2014, p.202).

Sendo assim, interessante se faz destacar um dos primeiros julgados da jurisprudência brasileira que avançou na discussão acerca da privacidade à proteção de dados pessoais, a Apelação tombada sob o nº 0195078-74.2010.8.26.0100, julgado pelo Tribunal de Justiça de São Paulo. Esse acórdão discutiu a responsabilidade civil da Google em relação a indevida divulgação de uma imagem da residência e dos dados pessoais de um indivíduo, pelo serviço *Google Maps*. A empresa foi condenada, em primeira instância, ao pagamento de indenização por danos morais. No Tribunal, foi confirmado o dever de indenizar, porém, o montante foi reduzido.

O acórdão destrinchou a ideia da responsabilidade do fornecedor e a sua relação com a proteção de dados: "(...) não convence a alegação da ré de que não tem condições técnicas de evitar que tais informações, removidas em obediência à liminar, sejam inseridas em seu mapas por um usuário qualquer ou pela criação de um outro 'site' que tenha tais informações". Concluiu-se, ainda, que nesse caso não havia terceiros envolvidos, sendo, portanto, de responsabilidade única do *Google Maps* a obrigação de possuir sistemas de proteção à privacidade e intimidade do indivíduo, com base no "risco da atividade". Portanto, ou a empresa deve criar mecanismos de proteção aos clientes ou continua a correr o risco de responder por eventuais danos que seu serviço vier a causar.

Destarte, infere-se que foi imposta uma obrigação de indenizar à empresa não só por conta de uma utilização arbitrária dos dados do consumidor, mas, principalmente, devido a omissão da mesma em estabelecer sistemas de proteção da privacidade adequados (MENDES, 2014, p.160). Nesse julgado, o princípio do "risco da atividade" (Art. 927, § único, CC), o qual consiste na responsabilização do causador do dano, independente de culpa, quando a atividade desenvolvida incorre em risco para os direitos de outrem foi inserido em um contexto das novas tecnologias e formas de tratamento de dados.

Somado ao citado princípio, a responsabilidade objetiva do fornecedor (Art. 14, CDC) e o direito básico de reparação de danos (Art. 6º, inciso VI, CDC), levam a consolidar uma

obrigação do fornecedor em manter os dados pessoais dos usuários seguros, tomando as medidas necessárias para tal objetivo. Isso porque, principalmente no âmbito digital, o estabelecimento de uma "segurança" exige um demasiado cuidado, devido a estruturação da internet estar sempre suscetível a diversas formas de ataque, o que podemos relacionar diretamente com o objeto do presente artigo. Nessa senda, interessante se faz levantar a seguinte situação hipotética: Determinada empresa "X" possui um banco de dados pessoais dos seus usuários e acaba sofrendo um ataque de *ransomware*, tendo todo o seu conteúdo sequestrado. Caso tais dados sejam publicizados, deletados ou utilizados de forma a causar dano aos usuários, poderiam esses exigir alguma reparação frente à empresa "X"?.

Para Laura Schertel Mendes (2014) a resposta seria "sim", visto que, em geral, as ameaças de segurança aos sistemas de informação não são imprevisíveis ou inevitáveis e decorrem, usualmente, da utilização de sistemas de segurança antiquados ou fora dos padrões recomendados. Dessa maneira, a concretização de um ataque de *ransomware* estaria severamente ligado a alguma deficiência no sistema de segurança da empresa, havendo nexo de causalidade direto entre a atividade da empresa fornecedora com o dano causado ao consumidor. Conclui-se, portanto, que o dever de indenizar seria plenamente viável nos casos de sequestro digitais

Por fim, vale ressaltar a existência do instituto do *recall* (Art. 10, §1º e §2º, CDC), que estabelece a obrigação de comunicação imediata da autoridade competente e dos consumidores quando ocorre um incidente de segurança que possa acarretar em riscos. Retomando a hipótese outrora suscitada, ao sofrer o aludido ataque, a empresa "X" deveria informar imediatamente aos seus clientes sobre o ocorrido, bem como à respetiva autoridade competente. Nesse sentido, arremata-se o entendimento de que os fornecedores que lidam com banco de dados pessoais no âmbito digital, devem se preocupar ainda mais com a seguridade dos seus sistemas de proteção, diante da velocidade na qual a tecnologia evolui, tomando todas as precauções necessárias frente os novos riscos e ameaças.

4.3 O Marco Civil da Internet

O Marco Civil da Internet foi uma reivindicação da sociedade civil que exigiu o estabelecimento de direitos dos usuários de *internet*, antes de qualquer criminalização de condutas *online*. Para tanto, contou com um amplo debate colaborativo, pioneiro em âmbito mundial, que ficou disponível para consulta pública entre novembro de 2009 e junho de 2010, recebendo mais de mil contribuições[19]. Dessa forma, a Lei 12.965/14, trouxe consigo respostas legislativas que contribuíram para o fortalecimento do Estado Democrático de Direito e, principalmente, para o reconhecimento de direitos e sua extensão para a *internet* (FORTES, 2018, p.120).

[19] RONCOLATO, Murilo. Regulamentação do Marco Civil recebeu 1;2 mil contribuições. *Estadão*. Disponível em: https://link.estadao.com.br/noticias/geral,regulamentacao-do-marco-civil-recebeu-12-mil-contribuicoes,10000029384. Acesso em 15 ago. 2019.

Dentre os principais pontos tratados, podemos verificar uma importante mudança na concepção do espaço da *online*, deixando de considerá-lo como um mero ambiente de entretenimento, para reconhecê-lo como uma arena de desenvolvimento da personalidade do indivíduo e o exercício pleno da cidadania (PASSOS, 2017, p.91). Outrossim, esse texto legal tem seu alicerce em um tripé axiológico, pautado na neutralidade, privacidade e liberdade de expressão (MARTINS, 2017, p.111). Além disso, em seu artigo 7º, foram elencados diversos direitos e garantias dos usuários para nortear as formas de utilização da *web,* dentre eles, a inviolabilidade da intimidade e da vida privada e a inviolabilidade e sigilo de suas comunicações privadas armazenadas, estabelecendo hipóteses de responsabilização civil em casos de violação.

Restringindo-se ao objeto desse artigo, a Lei 12.965/14 foi importante no sentido de impor aos provedores de Internet ou serviços o dever de registrar os *logs*[20] das atividades de seus usuários, tendo em vista que, na grande maioria dos crimes digitais, para que seja possível a apuração da autoria do delito, é necessária a contribuição de terceiros que fornecem e administram as aplicações as quais serviram de ambiente para o crime.

Os provedores de *internet* são, em regra, os que possibilitam o acesso do usuário à rede, atribuindo-lhe um endereço de IP (*Internet Protocol*) em uma determinada faixa de data e horário, visando a sua identificação. Além disso, ao interagir com serviços na *internet*, como *blogs, e-mails* e redes sociais, o usuário tem seus dados registrados por essas aplicações (fornecedores dos serviços), criando o que se chama de "registro de acesso a aplicações na internet" (JESUS; MILAGRE, 2016, p.170). Assim, os provedores de serviços passam a armazenar dados que ajudam na identificação da autoria de delitos informáticos, conforme explicam Damásio de Jesus e José Antônio Milagre (2016): "Obtendo-se os dados de acesso às aplicações daquele que utilizou o serviço para más finalidades, pode-se, através do IP que será fornecido, descobrir qual o provedor de acesso associado", dessa forma, pode "oficiá-lo, para que apresente os dados físicos (nome, endereço, RG, dentre outros) da pessoa responsável pela conta de internet a qual estava atribuído o referido IP, na exata data e hora da atividade maliciosa".

Diante disso, o Brasil alcançou uma mudança significativa no combate aos crimes digitais, principalmente levando em consideração o estabelecido nos artigos 13º e 15º do Marco Civil, os quais regulamentaram o registro dos dados dos usuários, possibilitando seu acesso pela via judicial. No citado artigo 13º, tal lei estabeleceu que devem ser mantidos os registros de conexão, em ambiente controlado e de segurança, pelo administrador de sistema autônomo, durante o prazo de 1 (um) ano. Tal determinação transmitiu a tais operadores uma maior responsabilidade no que tange não só o tratamento, mas também à necessidade de armazenamento e manutenção dos dados dos seus consumidores. Interessante se faz destacar também o disposto no seu §1º, o qual estabelece que a referida responsabilidade pela manutenção de registros de conexão não pode ser transmitida a terceiros, solidificando ainda mais o compromisso do administrador. Ressalte-se, de igual maneira, o disposto no §5º, o qual

[20] É uma expressão utilizada para descrever o processo de registro de eventos relevantes num sistema computacional.

preleciona que, em qualquer hipótese, a disponibilização ao requerente dos registros deverá ser precedida de autorização judicial.

Outrossim, o mencionado artigo 15º, igualmente reforça o conceito de manutenção dos registros de acesso à internet, fazendo um recorte no que concerne aos provedores que exercem a atividade de forma organizada e profissionalmente, nos seguintes termos: "o provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet" estabelecendo, ainda, a incumbência de fazê-lo sob "sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento". Enfatize-se que tal determinação se torna mais abrangente ao passo que seu § 1º estabelece que até os provedores de aplicações de internet não abarcados pelo *caput* podem ser obrigados a guardar registros de acesso às suas aplicações, mediante ordem judicial. Diante das considerações feitas, verifica-se que a Lei 12.965/2014 foi essencial na regulamentação e organização de recursos que possibilitam a captação de informações identificadoras da autoria de crimes digitais -inclusive sequestros -, viabilizando a punição dos seus responsáveis.

5 A NOVA LEI DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E A RESPONSABILIDADE DOS SEQUESTRADORES DIGITAIS

Após análise de algumas normas que interpretadas de forma conjunta fazem parte do arcabouço da proteção de dados pessoais no Brasil, é possível verificar, ainda, a existência de algumas lacunas a serem supridas pelo ordenamento brasileiro. Conforme outrora exemplificado, país já dispunha de diversas leis esparsas que influenciavam direta e indiretamente na proteção à privacidade de dados pessoais, contudo, a falta de uniformização gerava imprecisões e, por conseguinte, insegurança jurídica. Nesse ínterim, a criação da Lei nº 13.709/2018 foi extremamente necessária para sistematizar as ideias discutidas nas normas preexistentes, bem como para trazer inovações e diretrizes visando uma melhor efetividade do controle de dados.

5.1 Principais inovações normativas

Uma das características mais marcantes da Lei Geral de Proteção de Dados (LGPD), é o fato de ser uma norma enciclopédica, ou seja, que possui um caráter educativo e autoexplicativo, ao elucidar conceitos como "dados pessoais" (Art. 50, inciso I, LGPD) e "tratamento" (Art. 50, inciso X, LGPD). Outra marcante particularidade diz respeito ao estabelecimento de princípios que buscam guiar a interpretação legislativa acerca dos dados pessoais, tais como, o princípio da finalidade, da adequação, da necessidade, do livre acesso aos dados por parte dos titulares, da qualidade dos dados, da transparência e da não discriminação (Art. 6º, LGPD).

A LGPD também estabeleceu, de maneira expressa, em seu artigo 7º, os requisitos para possibilitar o tratamento de dados, reunindo ideias já trazidas, por exemplo, pelo CDC, e

acrescentando pontos relevantes ao delimitar que o aludido tratamento apenas poderá ser realizado mediante o fornecimento de consentimento pelo titular, nos casos de cumprimento de obrigação legal ou regulatória pelo controlador, ou ainda, por parte da administração pública, no que tange aos dados "necessários à execução de políticas públicas previstas em leis ou respaldadas em contratos, convênios ou instrumentos congêneres [...]" (grifos nossos). Além disso, também possibilitou o tratamento nos casos de realização de estudos por órgão de pesquisa, quando houver necessidade da execução de contrato ou de procedimentos ao relacionados seu objeto, bem como nos cenários relativos à tutela da saúde, vida ou incolumidade física de terceiros. Ainda, de igual maneira, viabilizou o citado tratamento quando for indispensável para "atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". Importa destacar que supracitado consentimento "realizado pelo titular" deve ser expresso, na forma escrita ou não, em cláusula destacada dos demais termos contratuais (Art. 8, §1º, LGPD). Ressalte-se também que o controlador dos dados está proibido de dar tratamento diverso daqueles informados inicialmente e, caso altere a finalidade do tratamento, deve requerer novo consentimento do titular (Art. 8º, §6º, LGPD).

Outro fator que merece ênfase é a relação do indivíduo com o tratamento dos seus dados pessoais. Os titulares agora tem direitos expressos para: a) confirmar a existência de tratamento do seus dados; b) corrigi-los quando estiverem incompletos ou inexatos; c) obterem informações sobre a possibilidade ou não de consentir com tal tratamento e tomar conhecimento das consequências da negativa; (Art.18, LGPD).

Em âmbito global, as relações internacionais do Brasil também foram impactadas pela Lei 13.109/18. Isso porque, no primeiro semestre de 2018 entrou em vigor uma nova regulamentação europeia, denominada "*General Data Protection*" (GDPR), a qual possui eficácia e aplicação extraterritorial. Nesse sentido, empresas nacionais que prestam ou oferecem serviços na região da União Europeia, devem se adaptar à nova regulamentação, sob risco de perderem os contratos outrora firmados. A GDPR também gerou óbice no que tange à transferência internacional de dados pessoais para países que não possuem um nível adequado de proteção. Dessa forma, ao estabelecer uma Lei Geral de Proteção de Dados, o Brasil passa a compor o rol de países interligados comercialmente à União Europeia, para os quais tais dados podem ser transferidos de forma segura, o que certamente ocasionará em fortes impactos econômicos e comerciais (MONTEIRO, 2014). Em breve, a LGPD também possibilitará a entrada do Brasil no rol de mais de cem países[21] adequados na proteção e uso de dados, possibilitando o processamento de informações oriundas o que irá, consequentemente, fomentar e avolumar os setores de tecnologia e de informação.

Nota-se, portanto, que o país está passando por uma mudança de paradigma extremamente relevante, implantando uma nova cultura de proteção de dados sistemática e elucidativa. Isso posto, resta evidente que as empresas devem buscar, cada vez mais, a

[21] BANISAR, David. *National Comprehensive Data Protection/Privacy Laws and Bills 2019*. Disponível em SSRN: https://ssrn.com/abstract=1951416. Acesso em: 21 ago. 2019

adaptação gradativa aos novos e necessários parâmetros trazidos pela a Lei 13.709/18 e suas eventuais influências no âmbito público e privado, *online* e *offline*.

5.2 A responsabilidade civil dos sequestradores digitais

Após uma análise geral sobre as principais inovações normativas da Lei 13.709/2018, passemos para um recorte dos avanços relacionados com o objeto do presente projeto. É fato que LGPD trouxe elementos significativos para uma maior segurança e sigilo dos dados pessoais, sendo um dos principais deles a determinação expressa que os agentes de tratamentos (Empresas) devem adotar medidas de segurança capazes de conter acessos não autorizados, eventos acidentais ou ilícitos de destruição, perda e alteração, além de garantir proteção frente a qualquer outra ocorrência de tratamento inadequado ou ilícito (Art.46). Essa ideia é complementada pelo artigo 49, o qual fixa que os sistemas de tratamento dos dados devem ser estruturados para atender aos requisitos de segurança, aos padrões de boas práticas e aos princípios gerais da LGPD. Ainda, a Lei também estabelece que inobservância do princípio da segurança (Art. 6º, VII) pode, em caso de dano ao titular, gerar responsabilidade civil e criminal solidária entre controlador e operador, além de impor o dever de reparar os danos (Art. 42).

Verifica-se, portanto, que a LGPD reforça a situação hipotética outrora posta em discussão no presente artigo, responsabilizando qualquer empresa que seja vítima de um sequestro digital e tenha os dados de seus usuários utilizados de forma indevida. Isso porque, conforme já debatido, a empresa deve manter seus mecanismos de proteção sempre atualizados, não sendo cabível a alegação de caso fortuito, já que trata-se do próprio "risco da atividade". É perceptível, ainda, o desenvolvimento das figuras do "controlador" e do "operador" de dados pessoais (Art.37), com a delimitação de suas atribuições nos artigos 41 e 39, respectivamente. O controlador tem como função principal indicar quem ficará encarregado pelo tratamento dos dados pessoais e pela transmissão das instruções para o "operador", bem como possui a obrigação de prestar esclarecimentos, adotar providências, e receber comunicações das autoridades competentes, além de orientar funcionários e contratados do "operador" acerca das práticas adequadas a serem adotadas. Tal fragmento da lei foi de relevante importância no que concerne à proteção contra sequestros digitais, porquanto a autoridade competente poderá solicitar ao controlador um relatório de impacto referente às operações de tratamento, possibilitando pôr em prática ações efetivas para a proteção de danos (Art. 38)

De igual maneira, ressalte-se que a LGPD determinou que o controlador deve comunicar à autoridade competente e ao titular, em prazo razoável, sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou danos aos seus titulares (Art.48). O referido artigo claramente dialoga com a figura do *recall*, já normatizada anteriormente pelo Código do Consumidor (Art.10 § 1º,2º) e aqui debatida. Evidente, portanto, que esse ponto abordado pela lei, faz notória diferença na contenção de danos após um *ciberataque* dos sequestrados digitais, visto que estipula a obrigação das vítimas serem informadas sobre o incidente de segurança, possibilitando a busca pelas providências cabíveis. Por fim, a Lei 13.709/18 também inova ao elencar sanções administrativas quando ocorrerem infrações às normas estabelecidas, no

entanto, tais penalidades não substituem a aplicação de outras - civis, penais ou administrativas-, já previstas em legislação específica.

Á vista das diversas elucidações aqui trazidas, conclui-se pela urgência e necessidade do desenvolvimento célere e crescente de mecanismos e figuras legais que permitam, cada vez mais, uma efetividade na proteção dos dados pessoais, tendo em vista que qualquer "falha" nesse aspecto possui grande potencial destrutivo, podendo atingir uma quantidade incontável de vítimas, sejam elas pessoas físicas ou jurídicas, já que todas passam a ter um status de vulnerabilidade ao armazenar suas informações em dispositivos informáticos.

6 CONSIDERAÇÕES FINAIS

O presente artigo teve como objetivo discutir o avanço da tecnologia e a sua forte influência no aparecimento de novos crimes ou novas configurações de antigos delitos. Os *cibercriminosos* se aproveitam da falta de discernimento dos usuários, da leniência das empresas na busca da atualização dos seus sistemas de segurança, bem como da dificuldade na normatização dos delitos, para realizarem seus ataques. Verificou-se que os mecanismos que possibilitam o anonimato, como o uso da *darknet*, associados a brechas informáticas, auxiliam na concretização dos mesmos. Dessa forma, a análise da responsabilização, tanto na esfera penal quanto cível, é extremamente necessária, ao passo que estabelece limites e contribui para uma melhor compreensão e prevenção das investidas realizadas. Para tanto, exige-se o estabelecimento de um diálogo das fontes utilizando-se de todo o arcabouço legislativo ora apresentado, sob ambas as aludidas esferas. Somado a isso, ao analisar a Lei 13.709/18 e suas novas diretrizes, é possível verificar um considerável avanço para a prevenção dos sequestros digitais, objeto do presente artigo, sendo possível o vislumbre de um futuro promissor para a tutela de dados.

Em contrapartida, verifica-se também a necessidade de uma colaboração cíclica de diversos agentes para que a prevenção seja efetiva. Nesse sentido: a) os usuários devem buscar se informar mais sobre os perigos online, analisando a veracidade de sítios e e-mails, sem fornecer dados de maneira aleatória; b) as empresas devem promover uma efetiva movimentação para atualizar e modernizar seus sistemas de segurança regularmente, a fim de gerar menos danos aos seus clientes e a elas próprias; c) o governo deve focar em uma efetiva tutela prática e legislativa para a proteção de dados, sempre atentos as mudanças exponenciais que o mundo virtual possibilita.

7 REFERÊNCIAS BIBLIOGRÁFICAS

ATAQUE afeta quase cem países, de Renault na França a bancos russos. *El País*. Disponível em: https://brasil.elpais.com/brasil/2017/05/13/internacional/1494668788_755982.html.

BANISAR, David. *National Comprehensive Data Protection/Privacy Laws and Bills 2019*. Disponível em SSRN: https://ssrn.com/abstract=1951416. Acesso em: 21 ago. 2019

BREWSTER, Tom. Simplocker Android malware locks up mobile data and demands a ransom. *The Guardian*. Disponível em: https://www.theguardian.com/technology/2014/jun/05/simplocker-android-ransomware-malware-virus. Acesso em: 21 ago. 2019

CAVALCANTE, Márcio André Lopes. Primeiros comentários à Lei n.° 12.737/2012, que tipifica a invasão de dispositivo informático. Disponível em: https://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html.

CEBRIÁN. Belén Domínguez. Cibertaque: o vírus WannaCry e a ameaça de uma nova onda de infecções. *El País*. Disponível em: https://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html.

CIBERATAQUE paralisa 16 hospitais do Reino Unido. *El País*. Disponível em: https://brasil.elpais.com/brasil/2017/05/12/internacional/1494602389_458942.html.

CRESPO, Marcelo. As Leis nº 12.735/2012 e 12.737/2012 e os crimes digitais: acertos e equívocos legislativos. Disponível em: https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/.

D'URSO, Luiz Flávio Filizzola;. Ataque cibernético mundial é a comprovação da insegurança na internet. *Conjur*. Disponível em: https://www.conjur.com.br/2017-mai-17/ataque-cibernetico-mundial-comprova-inseguranca-internet.

FORTES, Vinicius Borges. *Os direitos de privacidade e a Proteção de Dados Pessoais na Internet*. Rio de Janeiro: Editora Lumen Juris, 2018. p. 120.

JESUS, Damásio de Jesus; MILAGRE, José Antônio. *Manual de crimes cibernético*. São Paulo: Editora Saraiva, 2016. p. 81.

MALWARE utilizado em roubos financeiros. Disponível em: https://www.enigmasoftware.com/pt/gozitrojan-remocao/.

MARQUES, Claudia Lima. *Manual de Direito do Consumidor*. 8. ed. atual. [*S. l.*]: Revistas dos Tribunais, 2017. p. 506.

MARTINS, Guilherme Magalhães. *Contratos Eletrônicos de Consumo*. [*S. l.*]. Editora Atlas, 2014. p. 119.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor:* Linhas gerais de um novo direito fundamental. [*S. l.*]: Editora Saraiva, 2014. p. 192.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018.

PASSOS, B.R.S. *O direito à privacidade e a proteção aos dados pessoais na sociedade da informação:* uma abordagem acerca de um novo direito fundamental. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2017. p. 79-97.

REGAN, Joseph. *Programa malicioso ou software malicioso, é um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita*. Disponível em: https://www.avg.com/pt/signal/what-is-malware/. Acesso em: 23 jul. 2019.

RODRIGUES, Renato. Brasil é o País com mais usuários atacados por phishing. *Kaspersky Daily*. Disponível em: https://www.kaspersky.com.br/blog/brasil-ataques-phishing/11826/.

ROHR, Altieres. Brasil é o país com mais usuários atacados por phishing. *G1*. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/05/20/brasil-e-o-pais-com-mais-usuarios-atacados-por-phishing.ghtml.

RONCOLATO, Murilo. Regulamentação do Marco Civil recebeu 1;2 mil contribuições. *Estadão*. Disponível em: https://link.estadao.com.br/noticias/geral,regulamentacao-do-marco-civil-recebeu-12-mil-contribuicoes,10000029384.

TANGERINO, Daiane Fanti. Invasão de dispositivo informático (art. 154-A, CP) e o STJ. Disponível em: https://canalcienciascriminais.com.br/invasao-de-dispositivo-informatico/.

TIPO de software nocivo que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 23 jul. 2019.

VIANNA, Túlio; MACHADO, Felipe. *Crimes informáticos*: Conforme a Lei nº 12.737/2012. Belo Horizonte: Editora Fórum, 2013. p. 120.