INTRODUÇÃO AO DIREITO DIGITAL

AN INTRODUCTION TO DIGITAL LAW

JOSÉ EDUARDO DE SOUZA PIMENTEL
Promotor de Justiça do Estado de São Paulo
Mestre em Direito das Relações Sociais pela PUC/SP
Especialista em Gestão e Governança de Tecnologia da Informação pelo SENAC/SP

RESUMO

O Direito Digital representa a evolução do próprio Direito, abrangendo todos os seus ramos. Trata, especialmente, de dilemas da denominada "Sociedade da Informação" e das novas formas de criminalidade surgidas da evolução tecnológica e da expansão da internet. O artigo aborda questões relacionadas a tais temas e indica como vêm sendo tratadas em normas internacionais e brasileiras.

Palavras-chave: Direito Digital. Crimes cibernéticos. Dados pessoais. GDPR.

ABSTRACT

Digital Law represents an evolution of the law itself, covering all its ramifications. It deals, in particular, with the dilemmas of the "Information Society" and the new forms of crime related to technological evolution and the expansion of the internet. The article addresses the issues related to the themes and indicates how the international and Brazilian regulations treat them.

Keywords: Digital Law. Cybercrimes. Personal data. GDPR.

SUMÁRIO

1 INTRODUÇÃO

O Direito Digital vem sendo considerado uma nova disciplina jurídica. Sua idade é estimada em duas décadas. Costuma-se dizer que a Portaria Interministerial 147, de 31 de maio de 1995, editada pelos ministros da Comunicação e da Ciência e Tecnologia, que regulou o uso de meios da rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à Internet, foi o primeiro diploma legal desse ramo (ARAÚJO, 2017, p. 17).

A pesquisa do Prof. João Marcello de Araújo Jr., apresentada no Congresso de Würzburg (Alemanha), em outubro de 1992, demonstrou, entretanto, que, pelo menos desde 1976, a Câmara dos Deputados e o Senado tramitaram projetos de lei que tratavam de informática. São exemplos: o projeto de lei nº 3.279, de 1976, do Deputado Siqueira Campos, que dispunha "sobre a programação viciada de computador"(arquivado em 1979); o projeto de lei nº 96, de 1977, do Senador Nélson Carneiro, que dispunha "sobre a proteção das informações computadorizadas" (arquivado em 1980); projeto de lei nº 579, de 1991, do Deputado Sólon Borges dos Reis, que dispunha "sobre o crime de interferência nos sistemas de informática (destruição); entre outros (REIS, 1997, p. 50).

O Direito Digital nasceu da necessidade de se regularem as questões surgidas com a evolução da tecnologia e a expansão da internet, elementos responsáveis por profundas mudanças comportamentais e sociais, bem como para fazer frente aos novos dilemas da denominada "Sociedade da Informação".

Em obras mais antigas também encontramos alusão ao "Direito Informático" como "o conjunto de normas, princípios e instruções que regulam as relações jurídicas emergentes da atividade informática" (ALTMARK, 1987 apud REIS, 1997, p. 14).

A doutrina tem assinalado um aspecto interessante desse ramo do Direito: afirma que o Direito Digital não tem objeto próprio. Seria um Direito com um "modus operandi diferente, sendo, na verdade, a extensão de diversos ramos da ciência jurídica, que cria novos instrumentos para atender a anseios e ao aperfeiçoamento dos institutos jurídicos em vigor" (ARAÚJO, 2017, p. 24).

De acordo com Patrícia Peck Pinheiro, o Direito Digital é a evolução do próprio Direito e abrange "todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas" (2008, p. 29).

2 INTERNET E VIDA DIGITAL

2.1 Sociedade da Informação

Segundo Alvin Toffler (apud PINHEIRO, 2008, p. 6), três ondas caracterizam a evolução da humanidade.

A primeira onda representa a era agrícola, fundada na propriedade da terra como instrumento de riqueza e poder.

A segunda onda coincide com a denominada revolução industrial, com seu

ápice no tempo da Segunda Grande Guerra. Nesta, a riqueza consiste na combinação da propriedade, do trabalho e do capital.

A terceira onda é a da informação. Suas primeiras manifestações se deram ainda antes do apogeu da segunda onda, com o surgimento de grandes invenções no campo das comunicações, de que são exemplos o telefone, o cinema, o rádio e a TV (sec. XX). Caracteriza-a o volume crescente de informação trafegada, a serviço de um "modelo de produção em grande escala, de massificação, centralização de poder e estandardização ditada pela Era Industrial" (TOFFLER, 1999, p. 230).

Com a implementação da tecnologia digital e criação da internet, consolida-se a terceira onda, pela inclusão de dois novos elementos: a velocidade de transmissão de informações e a descentralização de suas fontes.

Relembre-se que a Internet tem sua origem na rede de computadores conhecida como ARPANET, do Departamento de Defesa dos Estados Unidos, criada com fins militares. Em plena guerra fria, os EUA temiam um ataque soviético sobre seu sistema de comunicações e desenvolveram o conceito de rede de computadores de várias rotas e sem um centro estabelecido. Na década de 70, universidades e instituições se conectaram à ARPANET. Em 1975 já existiam cerca de 100 sites publicados.

A rede mundial cresceu. Estima-se que, só no Brasil, haja mais de 120 milhões de pessoas conectadas. É o quarto lugar no *ranking* de usuários.

No cenário do crescimento exponencial do uso de computadores e dispositivos interconectados, multiplicam-se os conflitos que o Direito deve dirimir e os casos de crimes praticados pela rede e com uso de tecnologia.

A internet não tem dono. É um instrumento de comunicação, de abrangência planetária, cujo acesso vem sendo mundialmente compreendido como direito fundamental. Registra-se tramitar no Senado Federal proposta de emenda à Constituição (nº 6/2011), para incluir "entre os direitos sociais consagrados no art. 6º da Constituição Federal o direito ao acesso à Rede Mundial de Computadores (Internet)".

A vida conectada pressupõe transparência, colaboração, conhecimento compartilhado e poder de mobilização. Reclama novos comportamentos e o exercício do que se pode chamar de cidadania digital, fonte de direitos e deveres de indivíduos, governo e empresas.

2.2 Desafios

Diversos temas interessam ao Direito Digital.

Inicialmente podemos lembrar os direitos autorais, objeto de especial proteção na Constituição Federal, que assegura aos autores "o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível a seus herdeiros pelo tempo que a lei fixar" (art. 5º, inciso XXVII).

Direitos do autor são, nos termos da Lei 9.610/98, bens móveis. Ocorre que, com o fenômeno das novas tecnologias, dá-se a desmaterialização da obra de seu suporte físico (MP3, e-book, streaming, etc.) e a possibilidade efetiva de que esta seja replicada pela Internet à revelia de seu titular e se torne permanente.

O Direito Digital busca a melhor solução para proteger o direito dos autores.

Outro elemento relevante para o Direito Digital é o e-mail como instrumento de comunicação e ferramenta de trabalho, bem como a sua possibilidade de ser monitorado pela empresa.

Há tempo, ensina Araújo, os e-mails são instrumento de declaração de vontade e geram efeitos jurídicos, podendo-se, até mesmo, classificá-los em espécies: "e-mail oferta", o "e-mail contrato", o "e-mail notificação", entre outros (2017, p. 34).

O autor recomenda a atenção do empregador em relação às mensagens enviadas por seus colaboradores, pois um e-mail equivocado pode gerar responsabilidade civil da empresa, de natureza objetiva, a teor da Súmula nº 341 do STF ("É presumida a culpa do patrão ou comitente pelo ato culposo do empregado ou preposto"). Sugere, quanto a esse cuidado, a instituição de uma política de segurança da informação à qual devem aderir os empregados.

O teletrabalho é outro tema que interessa ao Direito Digital. Com efeito, a evolução das relações de trabalho permeadas pelo avanço da tecnologia da informação alterou a legislação trabalhista, tornando praticamente equivalente a circunstância de o trabalhador se encontrar fisicamente na empresa ou na sua própria casa para fazer jus às benesses legais.

A recente Lei 13.467, de 13 de julho de 2017, alterou a Consolidação das Leis do Trabalho (CLT), que agora define, no art. 75-B, o teletrabalho como "a prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo".

Dada a possibilidade técnica de que os teletrabalhadores sofram vigilância dos períodos de conexão (controle de *login* e *logout*), inclusive pausas, podem ter direito à proteção da jornada, incluindo horas extras, nos termos do que dispõem o art. 7° da CF e o art. 6°, parágrafo único, da CLT.

O Direito Digital se ocupa, igualmente, das transações bancárias, do *internet banking*, do *home broker* e de pagamentos realizados com moedas virtuais, como o *bitcoin*.

Embora os bancos brasileiros tenham atingido um elevado grau de maturidade e sofisticação tecnológica, seus sistemas não estão imunes a erros e vulnerabilidades. Oferecendo tais serviços, sujeitam-se ao Código de Defesa do Consumidor, de sorte que só se eximem de responsabilidade se provarem a culpa exclusiva do consumidor ou de terceiro.

No STJ também se fixou o entendimento segundo o qual as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiro no âmbito das operações bancárias (Súmula 479).

A responsabilidade civil no âmbito do Direito Digital vem sofrendo mudanças para que possa fazer frente aos atos ilícitos realizados no meio eletrônico, mormente quando caracterizados pelo anonimato.

Segundo Araújo, a tendência é a prevalência, nesse ramo, da teoria do risco com a responsabilização objetiva, como forma de punir aqueles que, mesmo sem culpa, foram vetores na transmissão de conteúdos inadequados ou criminosos (2017,

p. 55 e 56).

Os crimes digitais são objeto de preocupação à parte. O Brasil foi, em 2017, conforme relatório da Norton Cyber Security, o segundo país com maior incidência de crimes da espécie, com 62 milhões de vítimas e prejuízo estimado em US$ 22 bilhões. Supõem-se que o aumento de crimes cibernéticos se relacione à popularidade dos *smartphones*, que estão nas mãos de 236 milhões de brasileiros (UOL, 2018).

2.3 Desafios+

A Constituição Federal protege a privacidade, ao estabelecer, no art. 5.º, inciso X, que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

A Carta Política também declara livre a manifestação do pensamento. Repudia, entretanto, o anonimato (art. 5°, IV), salvo no que diz respeito ao denominado "sigilo de fontes" (art. 5°, XIV), também previsto na na Lei de Imprensa como instrumento necessário do exercício profissional.

A privacidade, porém, não é um direito absoluto. Quando se apresenta em conflito com outros direitos de dignidade constitucional, como a segurança pública, pode e tem sido afastada por ordem judicial para fins de investigação criminal. Faz-se a ponderação dos valores em jogo, e, se houver motivo idôneo e grave que a justifique, a intervenção no direito individual é legítima. Essa ponderação é o que se denomina princípio da proporcionalidade.

As tecnologias disponíveis, porém, têm sido empregadas para o anonimato e se apresentam, muitas vezes, como escudos para práticas ilícitas, ocultando a identidade dos agentes e se estabelecendo como entraves à investigação criminal.

A privacidade também tem sido desafiada por empresas que oferecem serviços gratuitos, como o Facebook, enquanto coletam dados de seus usuários sobre seus relacionamentos, ocupação, preferências, perfis de consumo, etc.

2.3.1 Darknet e navegação anônima

Nos anos 90, a Marinha dos EUA se dedicou à concepção de um software que permitisse a navegação anônima na Internet. A ferramenta serviria a pessoas submetidas a regimes totalitários.

O projeto deu origem à construção do "Tor", browser gratuito, multiplataforma e preferido para ocultar identidade e localização de seus usuários[1].

A privacidade da navegação é garantida por um processo conhecido como *onion routing*, que encripta os dados e os transmite através de séries de servidores. Desse modo, o host não identifica de qual IP partiu a requisição.

Estima-se que 2 milhões de pessoas/dia utilizem o Tor e que parte disso acesse alguns dos 5.000 sites ocultos.

Muitos desses sites vendem drogas, armas e serviços ilegais e podem ser

1 Para saber mais, ver HIGA (2018).

facilmente encontrados em pesquisa feita diretamente no browser, numa experiência parecida com o Google (EMCDA, 2017).

2.3.2 Criptografia

No ano de 2017, o FBI tentou, sem sucesso, acessar 7.775 dispositivos eletrônicos protegidos por criptografia (THE WASHINGTON POST, 2018) . Para o diretor da instituição, Christopher Wray, este é um grave problema de segurança pública.

Os Estados Unidos cogitam exigir que fabricantes criem soluções que permitam o acesso de autoridades ao conteúdo de aparelhos encriptados. A isso se opõem as corporações de tecnologia como a Apple, argumentando que tais soluções (*backdoors*) criam vulnerabilidades que serão, futuramente, exploradas por hackers em prejuízo de seus consumidores.

Investigando o atirador de San Bernardino, Syed Farook, o FBI contratou hackers profissionais para desbloquear o iPhone 5Cs (rodando o iOS 9) apreendido em poder do criminoso. A agência pretendia estabelecer a relação do atirador e de sua esposa com grupos externos.

Sabe-se que, no caso específico do iPhone, a senha de desbloqueio fica armazenada no próprio dispositivo. Após dez tentativas de senhas erradas, o aparelho deleta seu conteúdo. Segundo o Washington Post, os hackers do FBI encontraram ao menos uma falha no iOS e os investigadores teriam obtido os arquivos armazenados. Não se sabe de que modo o conteúdo foi acessado.

2.3.3 Criptomoedas

Cada vez mais gente está usando criptomoedas (especialmente *bitcoins*), dinheiro virtual de pouca rastreabilidade, que circula mundialmente e sem depender do sistema bancário. O site coinmap.org estima que mais de 80 estabelecimentos de São Paulo (Capital) já o aceitem[2].

Em Buenos Aires, esse número é bem maior: quando se restringiu a compra de moeda estrangeira na Argentina, parte da população foi buscar proteção contra a inflação na moeda digital e, hoje, há muita dessa espécie sustentando negócios no país vizinho.

Em novembro de 2017, um desenvolvedor do Google publicou uma lista com 1.000 sites que mineravam criptomoedas. Dentre eles estava o Portal do Cidadão, mantido pelo Governo do Estado de São Paulo (no endereço <www.cidadao.sp.gov.br>).

Assim, quando o usuário acessava o serviço, um código malicioso escrito em JavaScript sequestrava parte do poder da CPU do visitante e a utilizava para criar dinheiro digital em determinada conta (RKbAaJRO6...Qti8a), mantida no site Coinhive. A mágica era possível porque a oferta da capacidade computacional para manter a rede que controla as transações virtuais é remunerada.

Enquanto o assunto era debatido no Twitter pelo pessoal de TI, um desen-

2 Dados de 14 abr. 2018 (nota do autor).

volvedor de Caxias do Sul teve a ideia de notificar a Coinhive e a conta teria sido bloqueada.

O Governo do Estado emitiu nota falando de uma “falha pontual já superada” e o *script* foi removido da página.

2.3.4 O caso Cambridge Analytica

Em 2014, pesquisadores do Centro de Psicometria da Universidade de Cambridge solicitaram que usuários do Facebook baixassem um *app* e respondessem a um questionário para fins acadêmicos sobre suas personalidades. 270 mil pessoas atenderam à pesquisa.

Na época, o Facebook permitia que *apps* extraíssem informações de perfis do usuário (extensíveis às de seus amigos) e, desse modo, o professor Aleksandr Kogan, responsável pela pesquisa, obteve os dados brutos de mais de 50 milhões de pessoas.

Kogan passou a trabalhar para a Cambridge Analytica e entregou os dados coletados à empresa.

Oficialmente, a Cambridge Analytica é uma empresa britânica de publicidade estratégica, que trabalha com *big data* (massa de dados) para traçar perfis de personalidade de consumidores e eleitores para, em seguida, dirigir-lhes o tipo de propaganda mais propícia a influenciá-los segundo esses perfis.

Os perfis são traçados segundo o modelo teórico das ciências comportamentais conhecido como O.C.E.A.N., que reflete as características de indivíduos, considerados os parâmetros Openess (abertura para novas experiências); Conscientiousness (nível de consciência e preocupação com organização e eficiência); Extroversion (nível de sociabilidade e positividade); Agreeableness (amabilidade e empatia); e Neuroticism (intensidade emocional com que a pessoa reage diante das informações).

Soube-se, recentemente, a partir de uma notável reportagem investigativa levada a efeito pela TV Channel4, que a Cambridge Analytica analisou clandestinamente informações de 87 milhões de perfis do Facebook (SILVA, 2018) e as utilizou para influir em eleições de países democráticos.

A matéria revela o diretor da empresa Chris Wiley arrependido de seu papel destruidor dos pilares da democracia. Ele descreve como capturava as preferências dos usuários das redes sociais e de que forma as utilizava, em escala maciça, para difundir informações relevantes no curso do processo eleitoral (CHANNEL 4, 2018).

Usando câmeras ocultas, repórteres se passaram por integrantes de um partido político do Sri Lanka e obtiveram confissões de executivos da empresa de sua responsabilidade por vitórias eleitorais diversas. A técnica, segundo eles, não se baseava em fatos, mas nas emoções humanas, esperança e medo. As informações vão para a Internet de modo sutil e se expandem sem que pareçam propaganda.

A Lei nº 13.488, de 6 de Outubro de 2017, alterando regras eleitorais, permitiu, expressamente, o denominado impulsionamento de conteúdo no Facebook, ao acrescentar à Lei nº 9.504 (Lei das Eleições), de 30 de setembro de 1997, o art. 57

– C, assim redigido:

> É vedada a veiculação de qualquer tipo de propaganda eleitoral paga na internet, excetuado o impulsionamento de conteúdos, desde que identificado de forma inequívoca como tal e contratado exclusivamente por partidos, coligações e candidatos e seus representantes.

A autorização legislativa permite que campanhas políticas sejam direcionadas a segmentos específicos de eleitores (FOLHA DE SÃO PAULO, 2017), tornando bastante valiosas quaisquer informações que permitam discriminá-los segundo suas crenças ou preferências.

3 CRIME DIGITAL

Na década de 80 surgem os primeiros estudos de fôlego sobre a dimensão dos crimes praticados com o uso do computador. O computador havia se tornado um equipamento pessoal e acessível.

A *American Bar Association* publica em junho de 1984 estudo com a estimativa de que se perdiam até 5 bilhões de dólares por ano nos EUA em razão dos *computer crimes* (GEMIGNANI, 1986 apud REIS, 1997, p. 18).

Michael Gemignani adverte, em artigo publicado em 1986 na Revista *Abacus, Computers and the Law*:

> If you have ideas on how to define, detect and – most importantly – prevent computer crimes, perhaps you should share them with your legislators, your employer, and appropriate professional societies. If computer crime is not the most serious criminal threat in the nation now, there is little question that someday it will be. The time to prevent the crimes of the future is today (apud REIS, 1997, p. 18).

O computador estava sendo usado para violar não somente os bens jurídicos já tutelados pelas leis penais (como o patrimônio, a fé pública e a intimidade) como também outros valores imateriais, ainda não completamente protegidos pelo Direito.

De fato, o material informático – composto por sistemas e dados eletrônicos – se mostra frágil e precioso.

Delineia-se, assim, um “bem jurídico informático” (FROSSINI, 1990 apud LIMA, 2011, p. 5) que reclama, em consequência, uma proteção legislativa própria. São exemplos dos novos bens jurídicos que advém da informática os dados eletrônicos, o sigilo e a segurança da informação (LIMA, 2011, p. 6).

A penalização de condutas praticadas mediante o uso de computadores ou que visem a sistemas e banco de dados informatizados constitui os denominados “crimes de informática”, “cibercrimes”, “delitos computacionais”, “crimes eletrônicos”, “crimes telemáticos”, “crimes digitais”, “crimes virtuais”, entre outras denominações.

Lima dá preferência à designação “crime de computador” por entender que a “máquina computadorizada” é a ferramenta básica para a produção do delito, de sorte que o nome definiria com exatidão o objeto do estudo (2011, p. 8).

Marcelo Crespo (2015), a seu turno, se insurge contra as denominações “virtual” e “cibernético” para os delitos praticados no meio digital. Argumenta que virtual é algo que não existe na realidade e que cibernético é termo que caiu em desuso e está associado à comparação do funcionamento do cérebro com os computadores.

Desse modo, a doutrina pátria vem preferindo o designativo “crimes digitais” para se referir às condutas típicas penais praticadas por meio de computadores e dispositivos análogos e/ou contra sistemas informatizados e dados (delitos de risco informático).

Particularmente aprecio a expressão “crime cibernético” pela sua equivalência com os cibercrime, objeto da versão em língua portuguesa da Convenção de Budapeste (2001), de boa literatura internacional e de área especializada do FBI. O Projeto de Lei do Senado n° 236, de 2012, Novo Código Penal, em tramitação, optou por essa denominação e reúne os delitos da espécie em única seção.

De se ver que, muito antes de estabelecer as regras gerais para o uso da Internet no Brasil, o legislador se ocupou da tipificação de crimes informáticos, do que são exemplos: Lei 9.609/98, art. 12; Código de Defesa do Consumidor, arts. 72 e 73; Lei 9.296/96, Art. 1º, § 1º e art. 10; Código Penal, Art. 153, § 1º-A, Art. 313-A, Art. 313-B, Art. 325, § 1º; Lei 8.137/90 (Sonegação Fiscal), Art. 2º, inc. V; Lei 9.504/97 (Eleitoral), Art. 72, I, II e III; e Estatuto da Criança e do Adolescente, art. 241-A.

De acordo com a doutrina, os crimes digitais se classificam em próprios (ou puros) e impróprios (ou mistos). Crimes digitais próprios ou puros compreendem as condutas contra os sistemas informáticos e os dados. São também denominados delitos de *risco informático*. Crimes digitais impróprios ou mistos são as condutas contra bens jurídicos tradicionais (vida, liberdade, patrimônio, honra) praticadas com o uso de dispositivos informatizados, pela internet ou mediante troca e armazenamento de arquivos eletrônicos.

4 NORMATIZAÇÃO INTERNACIONAL

4.1 Convenção de Budapeste

A Convenção de Budapeste, acordada em 2001, é uma tentativa de promover a cooperação entre Estados e a iniciativa privada para o combate da cibercriminalidade – consistente em atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados – e garantir a proteção dos interesses legítimos ligados ao uso e desenvolvimento da tecnologia da informação.

É, atualmente, o mais amplo instrumento jurídico para fazer frente às fraudes praticadas por computador, às violações de direitos autorais, à pornografia infantil etc e promover a cooperação internacional indispensável ao trato da matéria, dado o caráter transnacional e dinâmico dos cibercrimes.

Declara como seu escopo a garantia do “equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano”, tal como garantidos por outros tratados internacionais.

A Convenção de Budapeste é composta de quatro capítulos (Terminologia, Medidas a tomar a nível Nacional, Cooperação Internacional e Disposições Finais).

No Capítulo I (Terminologia) se definem “sistema informático”, “dados informáticos”, “fornecedor de serviço” e “dados de tráfego”.

O Capítulo II (Medidas a tomar a nível nacional) estabelece as providências que devem ser adotadas nos âmbitos dos direitos penal (Seção 1) e processual penal (Seção 2).

No âmbito penal, os Estados devem criminalizar as seguintes condutas: a) Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos; b) Acesso ilegítimo (art. 2º); c) Interceptação ilegítima (art. 3º); Interferência em dados (art. 4º); Interferência em sistemas (art. 5º); Uso abusivo de dispositivos (art. 6º); Infrações relacionadas com computadores; Falsidade informática (art. 7º); Burla informática (art. 8º); Infrações relacionadas com o conteúdo – Pornografia infantil (art. 9º); e Infrações relacionadas com a violação do direito do autor e dos direitos conexos – Violação do direito do autor (art. 10º).

A Convenção preconiza a responsabilização da pessoa jurídica, inclusive quando, por falta de fiscalização ou controle, o crime beneficiou o ente moral.

O documento também traz regras de processo. Estabelece que, na aplicação de tais regras, devem ser observadas as salvaguardas já estabelecidas na legislação nacional e garantir os direitos e liberdades fundamentais dos cidadãos objeto dos tratados internacionais.

Prevê a adoção de medidas legislativas para a conservação de dados informáticos armazenados, bem como a conservação e divulgação parcial de dados de tráfego. São previstas medidas para obrigar a pessoa que se encontre no território que comunique dados informáticos específicos. Da mesma forma um fornecedor de serviço que preste serviços no território da parte pode ser obrigado a comunicar os dados na sua posse ou sob seu controle relativos a seus assinantes.

A convenção também prevê a busca e apreensão de dados informáticos armazenados em suportes físicos e a possibilidade de realizar a cópia desses dados informáticos. Prevê a obtenção em tempo real dos dados relativos ao tráfego e a interceptação de dados no que diz respeito ao conteúdo.

A Convenção de Budapeste contempla, ainda, a cooperação internacional, estabelecendo princípios gerais a serem estabelecidos entre as partes.

Trata da extradição e de princípios gerais relativos ao auxílio mútuo, inclusive no que se refere às medidas cautelares.

Os signatários da Convenção também se obrigam a estabelecer uma rede 24x24, ininterrupta, para assegurar o apoio nas investigações das infrações penais nela previstas.

De se observar, em acréscimo, que todos os crimes previstos na convenção são dolosos.

Para tornar mais abrangente a cooperação entre os países, a convenção traz previsões relativas à assistência, extradição e cooperação mútuas mesmo para os casos em que não há acordos de reciprocidade.

Deve-se destacar a preocupação contida no texto de que se respeitem os

direitos humanos fundamentais das liberdades civis tais como direito à privacidade, à intimidade, à liberdade de expressão e o de acesso público ao conhecimento e à Internet.

O Brasil não é signatário da Convenção de Budapeste.

4.2 GDPR – Regulamentação Geral de Proteção de Dados

No dia 25 de maio de 2018, entra em vigor o GDPR (*General Data Protection Regulation*), promulgado pela União Europeia em 2016.

Trata-se de norma cogente, de observância obrigatória a todas as empresas que detêm ou manipulam dados pessoais dos cidadãos europeus, onde quer que estejam sediadas.

Os dados são o principal ativo de boa parte das organizações e movem a economia digital. Cogita-se hoje de que dados usados indevidamente teriam possibilitado a manipulação de milhões de pessoas e influído no Brexit e na eleição de Trump. Protegê-los de forma consistente é fundamental para a preservação do Estado Democrático de Direito e das liberdades públicas.

O período de *vacatio* de dois anos foi estabelecido para que as empresas pudessem se adaptar às novas regras, antes negligenciadas por grande parte das organizações.

O GDPR funda-se no consentimento. O titular do dado pessoal deve permitir que este seja coletado e pode, a qualquer tempo, revogar a concessão. Os serviços de coleta de dados devem informar claramente que o fazem.

Em apertada síntese, o GDPR: a) define dado pessoal como sendo qualquer dado, incluindo genéticos ou biométricos, que seja capaz de identificar uma pessoa; b) cria órgãos de controle em cada país da C.E. responsáveis pela recepção de denúncias e reclamações relacionadas à matéria do GDPR, bem como sua investigação; c) exige que as organizações possuam responsável (pessoa, departamento ou empresa diversa) pela gestão dos dados pessoais e transparência no que se refere à implementação das normas da GDPR; d) determina a comunicação aos órgãos de controle locais (e, em certas condições, ao titular) sobre a violação de dados pessoais, em até 72 horas; e) estabelece direitos aos cidadãos (de serem excluídos de cadastros de organizações; de se opor ao uso dos dados pessoais; de retificar dados pessoais; de portabilidade do registro de uma organização para a outra; à transparência, relativa à conservação e processamento de seus dados; e de privacidade, em relação aos dados dos menores de 13 anos, cujo armazenamento depende da autorização de seus pais).

Pelo GDPR, só se admite a transferência internacional de dados se o país receptor dispuser de norma com o mesmo nível de proteção da regulamentação europeia.

No Brasil, o assunto é tratado pelo Marco Civil da Internet, de forma menos abrangente.

Os projetos de lei nº 4060/2012 e 5276/2016, em trâmite na Câmara dos Deputados, dispõem sobre o tratamento de dados pessoais e poderão, se melhorados,

beneficiar as *startups nacionais*, colocando-as em condições de competir nos negócios que envolvem portabilidade de dados com congêneres de países com regras locais compatíveis com o GDPR, como a vizinha Argentina.

A violação à norma europeia implica em multas de €$ 20 milhões ou 4% do faturamento da corporação.

5 NORMATIZAÇÃO NACIONAL

5.1 Lei nº 12.735/12: "Lei Azeredo"

A denominada "Lei Azeredo" nasceu do projeto de lei nº 84, de 1999, do Deputado Luiz Piauhylino, para dispor "sobre os crimes cometidos na área de informática, suas penalidades e outras providências".

O projeto continha, inicialmente, 18 artigos.

Nos dois primeiros, estabeleciam-se os princípios: "o acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede"; dispunha ser livre "a estruturação e o funcionamento das redes de computadores e seus serviços", salvo disposições legais específicas.

O texto original punia com detenção o dano a dado ou programa de computador (art. 8º); o acesso indevido ou não autorizado a computador ou rede de computadores (art. 9º); a alteração de senha ou mecanismo de acesso a programa de computador ou dados (art. 10); a obtenção indevida ou não autorizada de dado ou instrução de computador (art. 11); a violação de segredo armazenado em computador, meio magnético, de natureza magnética, ótica ou similar (art. 12); e a veiculação de pornografia através da rede de computadores, sem indicar, de forma destacada, sua inadequação para criança ou adolescente (art. 14). Previa pena de reclusão, de 1 a 4 anos, para um único delito, o de criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos (art. 13), com pena aumentada, de 2 a 6 anos (art. 13, parágrafo único, inc. I a VII), se praticado contra o interesse dos entes federativos e da administração; com considerável prejuízo à vítima; com o intuito de lucro ou vantagem de qualquer espécie; com abuso de confiança; por motivo fútil; ou com a utilização de qualquer outro meio fraudulento.

Os crimes em questão tinham suas penas aumentadas de um sexto à metade se praticados no exercício da atividade profissional ou funcional (art. 15).

Em novembro de 2003, o projeto foi aprovado pela Câmara, nos moldes do Substitutivo da Comissão de Segurança Pública e Combate ao Crime Organizado, Violência e Narcotráfico. Recebeu Emenda de Plenário e a redação final ficou a cargo do Deputado José Ivo Sartori.

A nova versão do texto propunha a alteração do Código Penal, acrescendo-lhe seção ao Capítulo VI do Título I para tratar "dos crimes contra a inviolabilidade dos sistemas informatizados.

Pelo art. 154-A se puniria com detenção, de 3 meses a 1 ano, o acesso indevido ou sem autorização, a meio eletrônico ou sistema informatizado; e pelo art. 154-B tipificava-se a conduta de manter ou fornecer, indevidamente e sem autorização, dado ou informação obtida em meio eletrônico ou sistema informatizado, fato também sancionado com detenção, de 6 meses a 1 ano.

O projeto equiparava à coisa o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado e a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado, ao acrescentar o § 2º ao art. 163 do CP.

O § 3º do art. 163, que seria adicionado, puniria como dano qualificado a inserção ou difusão de vírus; se o "dado ou informação" (código malicioso) não tivesse potencial de propagação ou alastramento, a persecução estaria subordinada à representação.

O substitutivo previu a punição com reclusão da pornografia (fotografar, publicar ou divulgar) envolvendo criança e adolescente, com pena aumentada se o fato era praticado pela rede de computadores ou meio de alta propagação (art. 218-A).

Foram tipificados, também, o atentado contra a segurança de serviço de utilizada pública (art. 265) e a interrupção ou perturbação de serviço telegráfico ou telefônico (art. 266).

O cartão de crédito seria equiparado a documento, para punir a sua falsificação pelo art. 298 e se criava o crime de "falsificação de telefone celular ou meio de acesso a sistema eletrônico", pela inserção do art. 298-A no Código Penal.

No Senado, o projeto se arrastou por quase cinco anos. Foi reformulado e retornou à Câmara em 2008, na forma de substitutivo.

O acesso não autorizado à rede de computadores, dispositivo de comunicação ou sistema informatizado seria punido com reclusão, de um a três anos e multa. A obtenção, transferência ou fornecimento não autorizado de dado ou informação também se sujeitaria à pena de reclusão. Ambos os crimes demandariam representação para a persecução penal.

O substitutivo previa a incriminação da divulgação ou utilização indevida de informações e dados pessoais, punindo-a com detenção, e o dano de dado eletrônico alheio.

Previa, com pena de reclusão, a inserção ou difusão de código malicioso (vírus), com pena aumentada se a conduta fosse seguida de dano ou mesmo se o agente se valesse de nome falso ou identidade de terceiros para sua consumação.

O Senado também delineou, pelo substitutivo, o estelionato eletrônico no qual o artifício seria a difusão do código malicioso com intuito de facilitar o permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado.

O crime de atentado contra segurança de serviço utilidade pública, previsto no art. 265 do CP, passou a abranger o serviço de informação ou telecomunicação e, no crime do art. 266, seria punida, também, a interrupção ou perturbação do serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, redes de computadores ou sistema informatizado.

A falsificação de dado eletrônico e documento público foi equiparado pela nova redação que seria dada ao art. 297 do CP.

O substitutivo do Senado também previa alteração do Decreto-lei nº 1001, dia 21 de outubro de 1969, Código Penal Militar, para inserção dos tipos penais equivalentes.

O projeto definia dispositivo de comunicação, sistema informatizado, rede de computadores, código malicioso, dados informáticos e dados de tráfego, considerando-os expressamente protegidos para os fins penais.

O provedor de internet seria obrigado a manter, pelo prazo de três anos, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada e fornecê-los à autoridade investigatória mediante requisição judicial.

A lei também determinava que o provedor preservasse, imediatamente, após requisição judicial, outras informações necessárias para investigação e que respondesse, penal e civilmente, pela sua confidencialidade.

O provedor também seria obrigado a informar, de maneira sigilosa, à autoridade competente, sobre indícios da prática de crime de ação pública incondicionada perpetrado no âmbito da rede sob sua responsabilidade.

O desatendimento às requisições judiciais implicaria em multas de até R$100.000,00, aplicada em dobro em caso de reincidência.

Em maio de 2011, o Deputado Eduardo Azeredo, integrante de Comissão de Ciência e Tecnologia, Comunicação e Informática, foi designado o relator do projeto. Ele defendeu a aprovação, com adequações, baseando-se em dados de incidentes reportados ao CERT e evolução do crime digital (SENADO FEDERAL, 1999).

No entanto, o projeto de lei ainda tinha muitos pontos polêmicos, como as obrigações impostas aos provedores de acesso ou mesmo a redação de determinados dispositivos (como o que acrescentava o art. 285-B ao Código Penal)[3], que puniria com até 3 anos de reclusão aquele que baixasse música sem autorização de seu titular. Temia-se que a lei pudesse restringir a privacidade ou mesmo a liberdade no uso da internet (CARPANEZ, 2008).

Por isso, a "Lei Azeredo" acabou sendo desidratada: dos seus 23 artigos, 17 foram removidos pela Câmara dos Deputados. Das 13 condutas que seriam criminalizadas, sobrariam a falsificação do cartão de crédito, pela sua equiparação com o documento particular (art. 2º) e a ampliação do conceito de "favor ao inimigo", crime militar próprio, para considerar como traição também o fornecimento indevido de dado eletrônico (art. 3º).

Tais dispositivos, entretanto, foram vetados pela Presidente da República, o primeiro em razão da existência de tipo penal equivalente que derivaria da Lei "Carolina Dieckmann" e o segundo por se entender que "a amplitude do conceito de dado eletrônico como elemento de ação militar torna[ria] o tipo penal demasiado abrangente".

A lei afinal aprovada incluiu um novo dispositivo na Lei de Combate ao Ra-

3 Art. 285 – B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível.

cismo (7.716/89), obrigando que mensagens com conteúdo racista sejam retiradas do ar imediatamente (art. 5º), como já ocorre atualmente em outros meios de comunicação, como radiofônico, televisivo ou impresso, e previu a criação das delegacias especializadas no combate a crimes cibernéticos na Polícia Federal e nas Polícias Civis (art. 4º).

5.2 Lei nº 12.737/12: "Lei Carolina Dieckmann"

No início do ano de 2012, a atriz Carolina Dieckmann teve seu computador pessoal acessado por *hackers*, depois de haver clicado em link de e-mail, que instalou em seu computador pessoal um programa invasivo. O procedimento malicioso é conhecido como "*phishing*".

Através do programa instalado, os infratores tiveram acesso ao conteúdo da máquina da atriz e obtiveram cerca de 60 arquivos nela armazenados. Dentre esses arquivos se encontravam fotos íntimas de Carolina.

A partir de obtenção das fotos, os agentes – moradores de Minas Gerais e do interior de São Paulo – passaram a exigir 10 mil reais como condição para não as divulgar.

A vítima tentou surpreender os chantagistas, mas não obteve sucesso e as fotos foram, efetivamente, divulgadas na Internet.

A Polícia foi acionada e a investigação ficou a cargo da Delegacia de Repressão aos Crimes de Informática (DRCI) da Polícia Civil do Rio de Janeiro. Houve sucesso na identificação dos autores através do IP e a obtenção de prova material da prática do ilícito no cumprimento de mandado de busca domiciliar na casa dos suspeitos.

O fato fomentou a tramitação, em tempo recorde, do projeto de lei 35/2012, pois a atriz emprestou seu prestígio à causa, gerando o debate conclusivo sobre a necessidade de se tipificarem delitos informáticos. A curiosidade fica por conta de que o projeto acabou atropelando a reforma do Código Penal, que dedicaria um título aos delitos da espécie.

O projeto foi uma alternativa ágil e simplista à demanda social. Tipificaram-se condutas criminosas sem enfrentar as controvertidas questões sobre direitos e deveres na Internet, que a "Lei Azeredo" se propunha a dirimir.

A Lei nº 12.737/12, que dispõe, segundo sua rubrica e o art. 1º, sobre a tipificação criminal dos delitos informáticos, é a única lei dos crimes digitais próprios.

Pela Lei em questão se criminaliza a criação e disseminação de vírus computacional, os ataques tipo *Denial of Service* (DoS), o chamado *hacking* (invasão a sistemas) e a falsificação de cartões de crédito e débito.

Ela introduziu ao Código Penal o art. 154-A, que descreve a invasão de dispositivo informático, apenando-o com detenção, de 3 meses a 1 ano e multa. O § 1º do mesmo dispositivo prevê a mesma sanção para quem lida com dispositivo ou programa de computador (vírus) que propiciem a invasão. As penas são aumentadas se da invasão resulta prejuízo econômico (§ 2º).

Caso a invasão resulte na obtenção de conteúdo de comunicações eletrôni-

cas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, a pena será de reclusão, de até 2 anos (§ 3º), com aumento de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos mesmos dados (§ 4º).

Se a conduta vitimar determinadas autoridades, nova causa de aumento de pena, de um terço à metade, deve incidir (§ 5º).

A ação penal é pública, condicionada à representação, à exceção dos crimes praticados contra a Administração (art. 154-B).

A Lei também introduziu §§ ao art. 266, para que seja punida a interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade pública e, ao inserir o parágrafo único no art. 298 do Código Penal, equiparou, sob a rubrica de "Falsificação de cartão", o cartão de crédito ou débito ao documento particular, para o fim de incriminar a sua falsificação.

A lei tem recebido críticas porque teria criminalizado as atividades dos chamados "hackers do bem" (*ethical hacker*), profissionais bastante valorizados no mercado, que, com conhecimento e ferramentas apropriadas, invadem sistemas em busca de vulnerabilidades.

Critica-se, também, a exigência legal de violação do "mecanismo de segurança", supondo-se que esse requisito pode frustrar a responsabilização penal de quem cometeu o crime se aproveitando da desatenção da vítima. Parte da doutrina também observa que a conduta nuclear "invadir" não permite a punição de quem acessa indevidamente sistemas informatizados.

Por fim, a quebra de sigilo de dados telemáticos para a obtenção de prova do crime da Lei em estudo encontra óbice na própria lei de interceptações, que não permite a quebra do sigilo de dados telemáticos para condutas sujeitas a penas de detenção, como é o caso.

5.3 Lei nº 12.965/14 – "Marco Civil da Internet"

O Marco Civil da Internet (Lei nº 12.965/14) deriva de projeto nascido em 2009, forjado por intenso debate público. Surgiu como um contraponto ao projeto de lei de cibercrimes, conhecido como "Lei Azeredo", por alguns alcunhado de "AI-5 digital".

O MCI oferece uma base legal ao Poder Judiciário para dirimir questões sobre deveres de provedores de conexão e de acesso aplicações na internet, inclusive quando confrontadas com os direitos dos usuários. Tais controvérsias eram decididas com base no Código Civil e no Código de Defesa do Consumidor[4], os quais, não raramente, produziam soluções insatisfatórias.

O MCI é considerado a "Constituição da internet" (MINISTÉRIO PÚBLICO FEDERAL, 2016, p. 149). Traz uma "carta de princípios", direitos e deveres dos usuários da Internet, dos portais e sites, das prestadoras de serviço e do Estado. Os

4 O CDC dedica a Seção VI do Capítulo 5 (art. 43 a 45) à disciplina do banco de dados e cadastro dos consumidores.

principais pontos da lei dizem respeito à liberdade e à privacidade.

O texto afinal aprovado conta com 32 artigos, divididos em cinco capítulos: Disposições preliminares; Dos direitos e garantias dos usuários; Da provisão de conexão e aplicações da Internet; Da atuação do poder público; e Disposições Finais. Proclama: "O acesso à Internet é essencial ao exercício da cidadania [...]".

Barreto e Brasil (2016) ressaltam que o Marco Civil, embora vise, primordialmente, à tutela dos direitos civis na internet, tem larga aplicação no Direito Penal e Processual Penal, uma vez que estabelece conceitos fundamentais e disciplina a obtenção de provas concernentes à materialidade e à autoria delitiva. Nesse campo, ressaltam também a sua importância para a definição da terminologia que permite a padronização de ofícios, petições, representações, mandados judiciais etc.

Pelo MCI se estabelecem: o princípio da neutralidade da rede, o princípio da reserva jurisdicional, o princípio da não-responsabilidade de provedores de conexão à Internet e regras para *data centers* instalados fora do território nacional.

Pelo princípio da neutralidade de rede se impede que provedores discriminem a velocidade de conexão segundo o conteúdo acessado pelo usuário.

O princípio da reserva jurisdicional estabelece que a obtenção de dados relativos aos registros de conexão e de acesso a aplicações de Internet está subordinada à ordem judicial específica e fundamentada para o fim de investigação criminal.

A lei em análise estabelece que os provedores de conexão à Internet não serão responsabilizados civilmente por danos decorrentes de conteúdo gerado por terceiros (art. 18), salvo se, após ordem judicial específica, não tomarem as providências para tornar indisponível o conteúdo glosado.

A ideia subjacente é a de que não cabe ao provedor censurar previamente o que seus usuários publicam. No entanto, uma vez notificados da ilicitude do conteúdo, devem tomar medidas para retirar do ar esse material, sob pena de responsabilização civil e criminal.

Esse mecanismo tem recebido críticas. Membros do MP e das Polícias ponderaram à CPI da Pedofilia, no Senado, que a regra poderia servir de escudo a provedores que, diante de flagrante conteúdo criminoso (como a divulgação de pornografia infantil), esperariam a ordem judicial para suprimir a publicação (TELE.SÍNTESE, 2010).

Como regra, provedores são proibidos de guardar os registros de acesso a aplicações de internet. O art. 15, entretanto, determina que a empresa conserve essas informações pelo prazo de seis meses.

5.4 Projeto de Lei nº 236/12

Tramita no Senado o projeto de lei nº 236/2012, que se destina à edição de um novo Código Penal.

O texto foi elaborado por uma Comissão de Juristas nomeada em 2011, que é presidida pelo Ministro do STJ Gilson Langaro Dipp.

Durante 7 meses de trabalho da Comissão, foram realizadas audiências públicas e recepcionadas quase três mil proposições de diversos setores da sociedade

brasileira.

Segundo os objetivos declarados, a Comissão intentou modernizar o Código Penal, descriminalizando condutas e prevendo outras figuras típicas; unificar a legislação penal esparsa; tornar proporcionais as penas dos diversos crimes, de acordo com a gravidade relativa; e buscar alternativas à prisão.

No trabalho de sistematização, esforçou-se para que fossem criados tipos compreensivos, que oferecessem proteção a "diversas projeções do mesmo bem jurídico", de acordo com o que se lê na exposição de motivos (Segunda Parte). Cita-se como exemplo a unificação das seis figuras do estelionato.

O desafio mais evidente, entretanto, é o da adoção do princípio da "reserva de código", segundo o qual toda matéria criminal deveria estar contida na mesma lei.

A Comissão, entretanto, reputou haver um "patrimônio imaterial" a ser preservado, qual seja, o indicativo numérico de determinadas condutas e preservou o art. 121 para o homicídio, o 155 para o furto, o 157 para o roubo e o 171 para o estelionato. Essa opção impediu que os Crimes contra a Humanidade ou contra Interesses Metaindividuais antecedessem o Título relativo aos Crimes contra a pessoa, que inaugura a Parte Especial.

Desse modo, o texto foi dividido em: PARTE GERAL: Título I – Da aplicação da lei penal; Título II – Do crime; Título III – Das penas; Título IV - Individualização das penas; Título V – Medidas de segurança; Título VI - Ação penal; Título VII – Barganha e da colaboração com a Justiça; Título VIII - Extinção da punibilidade; PARTE ESPECIAL: Título I – Crimes contra a pessoa; Título II – Crimes contra o patrimônio; Título III – Crimes contra a propriedade imaterial; Título IV – Crimes contra a dignidade sexual; Título V – Crimes contra a incolumidade pública; Título VI – Crimes cibernéticos; Título VII – Crimes contra a saúde pública; Título VIII – Crimes contra a paz pública; Título IX – Crimes contra a fé pública; Título X – Crimes contra a Administração Pública; Título XI – Crimes eleitorais; Título XII – Crimes contra as finanças públicas; Título XIII – Crimes contra a ordem econômico-financeira; Título XIV – Crimes contra interesses metaindividuais; Título XV – Crimes relativos a estrangeiros; Título XVI – Crimes contra os direitos humanos; e Título XVII – Dos crimes de guerra; e DISPOSIÇÕES FINAIS.

O Título VI – Dos Crimes Cibernéticos compreende os artigos 208 a 211. Trata, na verdade, de dois únicos delitos, o de "Acesso indevido" (art. 209) e o de "Sabotagem informática" (art. 210).

Os crimes ficaram assim definidos:

> Acesso indevido
> Art. 209. Acessar, indevidamente ou sem autorização, por qualquer meio, sistema informático protegido, expondo os dados informáticos a risco de divulgação ou de utilização indevida.
> Pena - prisão, de seis meses a um ano, ou multa.
> § 1º Na mesma pena incorre que, sem autorização ou indevidamente, produz, mantém, vende, obtém, importa, ou por qualquer outra forma distribui códigos de acesso, dados informáticos ou programas, destinados a produzir a ação descrita no caput deste artigo.
> Causa de aumento de pena

> § 2º Aumenta-se a pena de um sexto a um terço se o acesso resulta prejuízo econômico.
> § 3º Se do acesso resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo acessado:
> Pena - prisão, de um a dois anos.
> Causa de aumento de pena
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver a divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas, se o fato não constituir crime mais grave.
> § 5º Se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos:
> Pena - prisão, de dois a quatro anos.
> Ação penal
> § 6º Somente se procede mediante representação, salvo nas hipóteses dos §§ 1º e 5º.
> Sabotagem informática
> Art. 210. Interferir de qualquer forma, indevidamente ou sem autorização, na funcionalidade de sistema informático ou de comunicação de dados informáticos, causando-lhe entrave, impedimento, interrupção ou perturbação grave, ainda que parcial:
> Pena - prisão, de um a dois anos.
> § 1º Na mesma pena incorre quem, sem autorização ou indevidamente, produz, mantém, vende, obtém, importa ou por qualquer outra forma distribui códigos de acesso, dados informáticos ou programas, destinados a produzir a ação descrita no caput.
> § 2º Se o crime é cometido contra a Administração Pública Direta ou Indireta, qualquer um dos Poderes da União, Estado, Distrito Federal ou Município, ou contra empresa concessionária ou permissionária de serviços públicos:
> Pena - prisão, de dois a quatro anos.

Pelo dispositivo que inaugura o título se definem “sistema informático”, “dados informáticos”, “provedor de serviços” e “dados de tráfego”. Notem-se que os mesmos elementos (e somente eles) foram objeto de definição também na Convenção de Budapeste (art. 1º).

O art. 211 traz uma disposição comum, estabelecendo que os crimes em questão são de ação privada, exceto se a vítima foi Administração Pública, direta ou indireta, Poderes da União, Estado, Distrito Federal ou Município ou empresa concessionária ou permissionária de serviços públicos. O dispositivo parece colidir com a previsão do § 6º do art. 209, que condiciona a persecução penal à representação.

Coube ao Desembargador Marco Antônio Marques da Silva, do Tribunal de Justiça do Estado de São Paulo, justificar o texto proposto. O jurista explicou que, com relação aos crimes cibernéticos próprios, aqueles “relacionados diretamente com o sistema informático”, protegem-se a confidencialidade dos dados informáticos, a integridade do documento eletrônico e a disponibilidade do sistema informático, daí porque se optou por criminalizar, de forma autônoma, condutas ilícitas contra esses bens jurídicos. Para o eminente autor, os tipos penais protegem o novo bem jurídico: o sistema informatizado.

Marques da Silva afirma que se pretendeu harmonizar a terminologia com a Convenção de Budapeste e que a redação do novo Código introduz núcleos do tipo

utilizados em informática, tais como “acessar”, “divulgar”, “capturar”, “processar”, “armazenar”, “transmitir”, entre outros.

Com relação aos crimes cibernéticos impróprios, explica que “o bem da vida a ser preservado será o correspondente a cada uma das condutas ilícitas cometidas”. Anota, entretanto, que, a circunstância de o crime ser praticado mediante a “utilização de sistema informático” será valorada como qualificadora, agravante específica ou causa de aumento, em delitos contra a honra, o patrimônio, a fé pública, a segurança nacional, entre outros.

Até o final de março de 2018, havia 83 emendas de parlamentares para inserção de dispositivos e outras adequações.

6 AÇÕES DO MINISTÉRIO PÚBLICO

6.1 Comissão de Proteção dos Dados Pessoais do MPDFT

O Ministério Público do Distrito Federal e Territórios editou, em 20 de novembro de 2017, a Portaria Normativa nº 512/2017, instituindo, no seu âmbito, a Comissão de Proteção dos Dados Pessoais (MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS, 2017).

Entre as justificativas para a edição do ato estão a entrada em vigor do Regulamento Geral de Proteção de Dados Pessoais da União Europeia (GDRP), “com impacto mundial, inclusive no Brasil” e a inexistência, entre nós, de uma “Autoridade de Proteção dos Dados Pessoais Nacional”.

No vácuo dessa autoridade, a Procuradoria-Geral de Justiça ousou conferir poder à comissão para receber comunicações sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares dos dados (*data breach notification*), inspirada, certamente, na novel normatização europeia. O site do MPDFT já possui área própria para o registro da ocorrência e instrui sobre a remessa de documentos físicos relativos ao evento.

Também compete à comissão promover políticas de proteção dos dados pessoais, inclusive entre a população, e influir para a definição de uma Política Nacional de Proteção dos Dados Pessoais e Privacidade.

Aparentemente extrapolando os limites do ato normativo, a Comissão anuncia, na página institucional, competir-lhe “propor ações judiciais visando à aplicação das sanções previstas no artigo 12, da Lei nº 12.965/14 - Marco Civil da Internet, em conjunto com o promotor natural” (pilar sancionador) e “instaurar procedimento preparatório, inquérito civil público e procedimento administrativo, em conjunto com o promotor natural” (pilar investigativo).

Há notícia de que a referida Comissão instaurou Inquérito Civil Público sobre o vazamento do cadastro de clientes da Netshoes e que está colhendo informações sobre descontos dados em farmácias mediante a informação do CPF do consumidor, suspeitando de que esse procedimento estaria gerando um banco de dados sobre as condições de saúde específicas da pessoa (FEITOSA JR., 2018).

No dia 20 de março de 2018, o órgão instaurou um inquérito civil para apu-

rar se a *Cambridge Analytica* capturou dados de usuários brasileiros no Facebook (LUCA, 2018).

6.2 Termo de cooperação MPSP e Microsoft

No dia 27 de fevereiro de 2018, o Ministério Público do Estado de São Paulo e a Microsoft celebraram um acordo de cooperação para combater e prevenir crimes cibernéticos.

O termo, com vigência inicial de cinco anos, prevê a capacitação de promotores na Unidade de Crimes Digitais (CDU) da empresa, disponibilização pela Microsoft de ferramentas de investigação e mitigação de delitos informáticos e fornecimento de relatórios de *malwares* e vulnerabilidades.

O termo de cooperação também contempla ações conjuntas para a educação da população em tema de prevenção dos crimes praticados com o uso do computador.

7 CONCLUSÕES

O Direito Digital abrange todas as áreas do Direito, de maneira transversal, e congrega novos elementos para dirimir os conflitos surgidos com a tecnologia, especialmente a Internet, e regular as relações da denominada “sociedade da informação”.

No campo do Direito Penal, o computador e a Internet têm sido cada vez mais usados para a prática de crimes. Surge o “bem jurídico informático” e a necessidade de se preverem novos tipos penais.

No âmbito internacional encontram-se normas destinadas à contenção dos crimes cibernéticos e a disciplinar o manejo de dados pessoais, com vista à proteção da privacidade.

Internamente, tipificam-se crimes digitais e proclama-se o Marco Civil da Internet, fundado nos princípios da liberdade, privacidade e neutralidade da rede. Este último instrumento é de fundamental importância para a investigação e obtenção de prova destinada à persecução criminal.

REFERÊNCIAS

ARAÚJO, Marcelo Barreto de. **Comércio eletrônico; Marco Civil da Internet; Direito Digital**. Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviço e Turismo, 2017.

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

MINISTÉRIO PÚBLICO FEDERAL. **Roteiro de atuação: crimes cibernéticos.** Brasília: MPF, 2016.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. **Portaria PGJ – 0512**. 2017. Disponível em: <http://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pessoais/Portaria_PGJ_n2017_0512.pdf>. Acesso em: 30 mar. 2018.

CARPANEZ, Juliana. **Entenda a polêmica sobre o impacto da lei de crimes cibernéticos.** 2008. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL-651929-6174,00-ENTENDA+A+POLEMICA+SOBRE+O+IMPACTO+DA+LEI+DE+-CRIMES+CIBERNETICOS.html>. Acesso em: 30 mar. 2018.

CHANNEL 4. **Data, Democracy and Dirty Tricks**. Disponível em: <https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose>. Acesso em: 7 abr. 2018.

CRESPO, Marcelo. **Crimes digitais: do que estamos falando**. 2015. Disponível em: <https://canalcienciascriminais.com.br/crimes-digitais-do-que-estamos-falando>. Acesso em: 25 mar. 2018.

FEITOSA JR., Alessandro. **Ministério Público investiga uso de dados de clientes por farmácias**. 2018. Disponível em: <http://gizmodo.uol.com.br/ministerio-publico-cpf-farmacia/>. Acesso em: 30 mar. 2018.

FOLHA DE SÃO PAULO. **Big data eleitoral que elegeu Trump tenta se firmar no Brasil.** 2017. Disponível em <http://www1.folha.uol.com.br/tv/poder/2017/12/1941024-big-data-eleitoral-que-elegeu-trump-tenta-se-firmar-no-brasil.shtml>. Acesso em: 7 abr. 2018.

EMCDA. **Drugs and the darknet: perspectives for enforcement, research and policy**. Lisbon, nov. 2017. Disponível em: <http://emcdda.europa.eu/publications/joint-publications/drugs-and-the-darknet>. Acesso em: 4 abr. 2018.

HIGA, Paulo. **Como entrar na deep web utilizando o Tor**. Disponível em: <https://tecnoblog.net/189897/como-acessar-deep-web-links>. Acesso em: 04 abr. 2018.

LIMA, Paulo Marco. **Crimes de computador e segurança computacional**. São Paulo: Atlas, 2011.

LUCA, Cristina de. **MP vai investigar se Cambridge Analytica coletou dados de brasileiros**. 2018. Disponível em: <https://porta23.blogosfera.uol.com.br/2018/03/21/mp-vai-investigar-se-cambridge-analytica-coletou-dados-de-brasileiros/>. Acesso em: 30 mar. 2018.

PINHEIRO, Patricia Peck. **Direito digital.** 2. ed. São Paulo: Saraiva, 2008.

REIS, Maria Helena Junqueira. **Computer crimes: a criminalidade na era dos computadores**. Belo Horizonte: Del Rey, 1996.

SENADO FEDERAL. **Projeto de Lei nº 84 de 1999**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=991858&filename=Tra-

mitacao-PL+84/1999>. Acesso em: 30 mar. 2018.

SILVA, Victor Hugo. **O caso Cambridge Analytica é ainda maior e atinge 87 milhões de pessoas**. Disponível em: <https://tecnoblog.net/238321/facebook-cambridge-analytica-87-milhoes/>. Acesso em: 7 abr. 2018.

TELE.SÍNTESE. **Promotores e Delegados criticam Marco Civil da Internet no Senado.** 2010. Disponível em: <http://www.telesintese.com.br/promotores-e-delegados-criticam-marco-civil-da-internet-no-senado/>. Acesso em: 13 abr. 2018.

TOFFLER, Alvin. **The third wave**. Nova Iorque: Betan Books, 1999.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. São Paulo, 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm>. Acesso em: 30 mar. 2018.

Submetido: 17/05/2018
Aprovado: 12/09/2018