SOCIEDADE HIPERCONECTADA

E OS DESAFIOS DE UMA NAVEGAÇÃO SEGURA

Angela Dias Mendes*[1]
e Lourival José Passos Moreira*[2]

Atualmente as sociedades tornam-se cada vez mais digitalizadas e as pessoas conectadas de diversas formas. No atual estágio de desenvolvimento tecnológico, não é mais possível renunciar ao uso de ferramentas digitais tendo em vista a migração de processos no âmbito do trabalho, do consumo, dos serviços etc.

Mecanismos e processos físicos e analógicos estão sendo substituídos por digitais, forçando a execução das mais diversas ações na rede que vão desde uma simples compra virtual até o cumprimento de obrigações legais, como é o caso da Declaração Anual do Imposto de Renda de Pessoa Física. Aliás, a pandemia do coronavírus acelerou a migração virtual de inúmeras transações, serviços e do exercício laboral (*home office*), tendo em vista a necessidade do distanciamento social para a contenção do vírus.

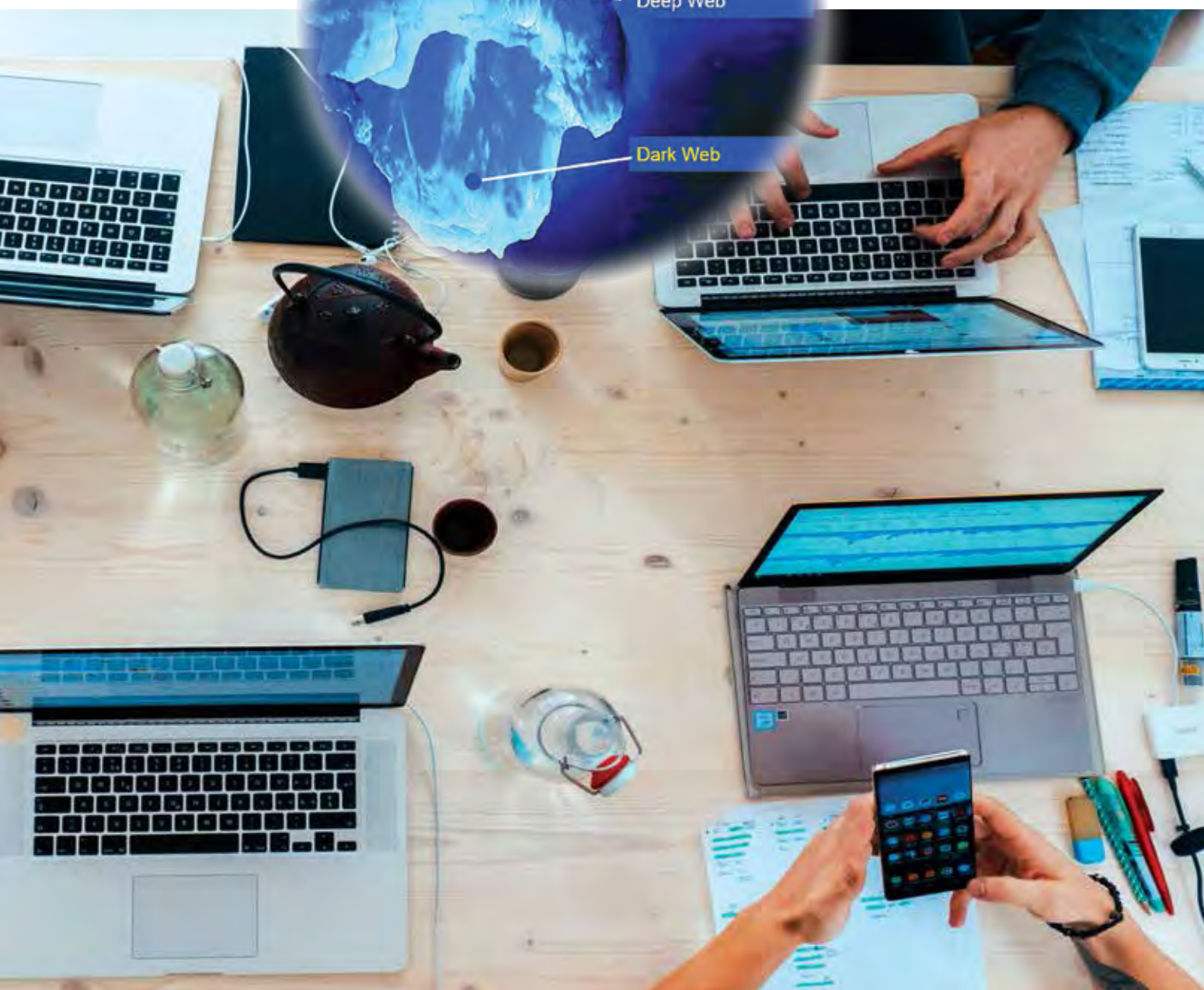
Na sociedade tecnológica hiperconectada, observa-se que conceder informações pessoais é condição *sine qua non* imposta pelos provedores de serviços e de produtos para que o usuário possa efetivar sua transação ou consumo, uma vez que o meio digital é o único disponível para acessar o objeto desejado.

Por outro lado, a ingerência sobre os dados pessoais,

em muitos casos, decorre da mudança comportamental do usuário que, motivado pelo fascínio das redes sociais, publica por vontade própria fotos, vídeos, imagens e informações da sua vida privada.

A privacidade é um direito que compõe o núcleo principiológico da Dignidade Humana previsto no artigo 12 da Declaração Universal dos Direitos do Homem: *ninguém será sujeito a interferências na vida privada, na sua família, no seu lar ou na sua correspondência*. No Brasil, ele encontra abrigo no art. 5º, inc. X, da Constituição Federal de 1988, a saber: *são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação*. A possibilidade de exigir reparação pelo dano sofrido em virtude da violação da vida privada é outro elemento fundamental desse direito. Porém, em que pese a proteção legal, resultado de um processo histórico de reconhecimento dos direitos da pessoa, não faltam, nas redes sociais, imagens e situações da vida privada, postadas pelo próprio titular, que expõem sua intimidade.

A proteção da privacidade inclui, também, a responsabilidade com os dados de terceiros. Aqui nos referimos, especialmente, à proteção de dados pessoais sensíveis por sistemas de segurança da informação. Neste sentido, as recorrentes notícias de vazamentos de dados nos últimos anos vem chamando a atenção em todo o mundo.



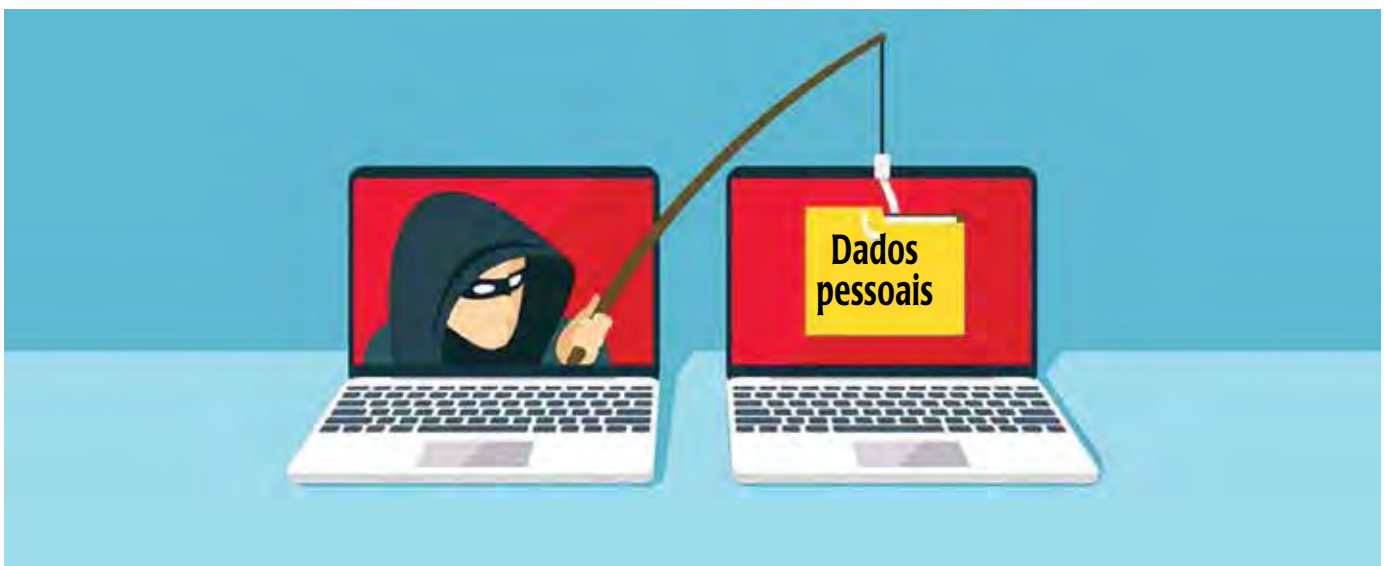
Embora incidentes de segurança e vazamentos não sejam temas novos na área de Segurança Cibernética, o volume de dados pessoais vazados atualmente traz preocupações relevantes. Uma consulta simples na internet pode revelar diversas notícias de sites como *Linkedin* (165 milhões), *Twitter* (300 milhões), *Microsoft* (250 milhões) e, mais recentemente, no Brasil, 223 milhões de pessoas foram vítimas do vazamento de fotos e documentos pessoais por fonte ainda não identificada e mais de 100 mil contas de clientes das operadoras brasileiras de telefonia móvel Claro, Oi, TIM e Vivo foram expostas.

Vazamentos de dados geralmente são resultantes de ataques cibernéticos, decorrentes de possíveis vulnerabilidades tecnológicas, procedimentais, comportamentais ou regulatórias, fatos que justificam o investimento em recursos tecnológicos de proteção, políticas institucionais consistentes para o estabelecimento de políticas e normas de uso seguro de sistemas de informação e comunicação, além de ações contínuas de prevenção e educação.

As consequências dos vazamentos vão desde o cometimento de golpes em desfavor de uma vítima individual, até o comprometimento de assuntos de Estado. As revelações trazidas a público em junho de 2013 pelo ex-contratado da Agência de Segurança Nacional dos Estados Unidos (NSA – *National Security Agency)* Edward Snowden trouxeram severas dificuldades diplomáticas ao governo norte-americano perante governos de países aliados, como Brasil e Alemanha. Outro personagem que chamou a atenção internacional pelo compartilhamento público de informações confidenciais foi Julian Assange, fundador em 2006 do site de denúncias *WikiLeaks*. O portal publicou diversas informações sensíveis dos Estados Unidos, como informações militares em 2007 e milhares de e-mails da candidata presidencial Hillary Clinton e do Comitê Nacional Democrata em 2016[1]. Os eventos associados a Assange e Snowden tornaram-se notáveis e demonstram a vulnerabilidade até dos sistemas de informação com alto grau de proteção à confidencialidade. É certo que não existe sistema totalmente seguro, mas o que se busca com as medidas de segurança é mitigar a possibilidade de ataque, invasão e vazamento de dados.

O ambiente de ameaças é bem amplo e está presente e disperso nas camadas denominadas web de superfície, onde o cidadão normalmente navega; na *deep web*, uma região de conexões fechadas, criptografadas e normalmente legítimas onde transações e aplicações com maior nível de segurança são realizadas, como *home banking*; e na região da internet denominada *dark web*, onde atividades ilegais e ilegítimas como terrorismo, tráfico de drogas e de pessoas, espionagem, compra e venda de dados, pornografia infantil, dentre outras violações e ilicitudes são cometidas livremente.

O repertório de ameaças também é amplo e diversificado, compreendendo furto de identidade, técnicas enganosas de engenharia social para captura de informações pessoais (*phishing*), interceptação de tráfego (*sniffing*), falsificação de e-mail (*spoofing*), desconfiguração de página (*defacement*), negação de serviço (DoS – *Denial of Service* ou DDoS – *Distributed Denial of Service*), sequestro de dados (*ransonware*) dentre outras formas de ataques ou golpes. Em geral, muitos destes ataques são executados a partir de programas maliciosos (*malwares*) injetados nos dispositivos



conectados à rede, como vírus, cavalo de troia (*trojan*) ou outro *malware*.

Diante disso, uma navegação defensiva na internet pode começar conhecendo as principais características desses elementos, o que já reduziria bastante alguns deslizes decorrentes da falta de informação. Para não cansar o leitor, recomendamos a leitura da *Cartilha de Segurança para Internet* elaborada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil [2].

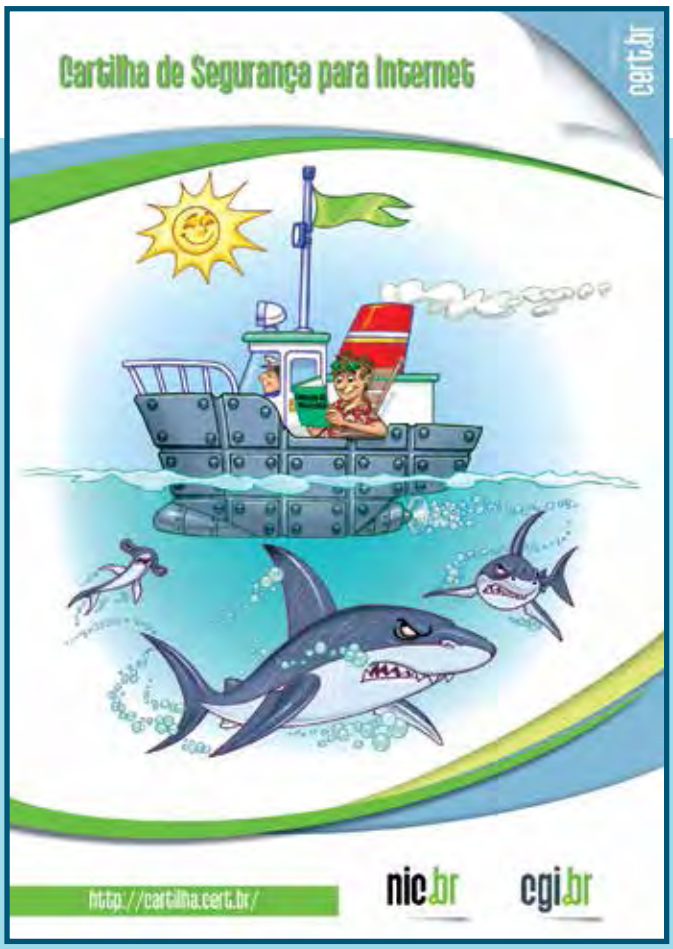
Na esteira da ordem jurídica internacional foi promulgada a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados-LGPD) que dispõe sobre o tratamento de dados pessoais da pessoa natural e jurídica e traz elementos normativos para proteção dos direitos fundamentais de liberdade e de privacidade no Brasil.

A LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), um órgão da Administração Pública, integrante da Presidência da República e responsável por zelar por seu cumprimento em todo território nacional. Outras funções da Autoridade essenciais à eficácia do instrumento são: elaborar as diretrizes nacionais da política de proteção de dados pessoais e privacidade, editar os normativos iniciais para alavancar as iniciativas de proteção e privacidade e propor as orientações gerais para o setor público e privado. Em um contexto crescente de ameaças cibernéticas que fragilizam a segurança da sociedade, o papel da ANPD torna-se ainda mais relevante.

Ao Estado cabe a definição de políticas públicas como coadjuvantes à regulação, sobretudo no campo educacional, para transformar o modo como o usuário lida com seus dados e com dados de terceiros que lhe são confiados. Normatizar é uma das formas com a qual o Estado se relaciona com as tecnologias e promove segurança jurídica. Contudo, educar o usuário é vital para suscitar uma nova cultura de proteção, sem a qual todos os investimentos em segurança cibernética podem ser infrutíferos.

*[1] *Advogada, Doutoranda PPGD/UNESA, Mestre em Direito, Integrante do Grupo de Interesse CTEMI do Clube Naval*

*[2] *Doutor em Política e Estratégia, Professor Mestre em Educação, Engenheiro Eletrônico e Integrante do Grupo de Interesse CTEMI do Clube Naval*



Notas

[1] Informações disponíveis nas seguintes páginas:

http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

ttps://www.bbc.com/portuguese/noticias/2013/11/131126_espionagem_resolucao_brasil_alemanha_mm

https://www.biography.com/activist/julian-assange

[2] A cartilha encontra-se disponível em https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf.