CARTILHA DE DIREITO DIGITAL

Comissão de Direito Digital

NITERÓI

Ano 2021

ORDEM DOS ADVOGADOS DO BRASIL

Seccional Rio de Janeiro

Subseção Niterói

Presidente
Claudio Vianna

Vice-Presidente
Elio Ferreira

Secretária-Geral
Enir Cezar

Secretária Adjunta
Helga Mansur

Diretor Tesoureiro
Ralph de Andrade

2021

Candida Diana Terra
organizadora

Colaboradores:
Bárbara Franco Gonçalves Pinto, Carla Maria Martellote Viola, Fernanda Couzzi Velasco, Fernando Galba, Iasmin Neiva, Isabella Pinto Barros de Andrade, Louana Costa, Marcelo Camargo, Marília Kairuz Baracat, Mona Freitas Obeica Meirelles, Rodrigo Borges Valadão, Tarcila Bairral, William Lima Rocha, Amanda Rodrigues Carvalho Gomes

CARTILHA DE DIREITO DIGITAL

COMISSÃO DE DIREITO DIGITAL

Niterói
2021

COMISSÃO DE DIREITO DIGITAL

Presidente

Candida Diana Terra

Secretários

William Lima Rocha
Fernanda Couzzi Velasco

EDIÇÃO
Amanda Rodrigues C. Gomes

ILUSTRAÇÃO DE CAPA
Andressa Lourenço

Índice Analítico

PREFÁCIO

Amanda Rodrigues Carvalho Gomes

A princípio, a cartilha elaborada pelos membros da Comissão de Direito Digital de Niterói tem o objetivo de buscar e compartilhar conhecimentos com os advogados. No entanto, os textos se tornaram vivos como o universo digital, transcendendo a simples disseminação de conteúdo, por instigarem o leitor a desenvolver o próprio pensamento crítico sobre os temas “mais em alta” da área em 2021.

A Lei Geral de Proteção de Dados, ou LGPD, trouxe notoriedade e importância para todo o Direito, pois a maioria das pessoas e empresas tem buscado se adequar aos padrões da norma e acabam esbarrando em outras Leis, Resoluções, Normas Internacionais e, até mesmo, na Constituição, como será elucidado pelos textos da cartilha, necessitando de profissionais do Direito para os nortearem.

Por essas razões, é imprescindível a adequação desses profissionais, não só dos advogados, mas também dos atuantes do setor público. Assustador? Fique calmo, não ache que é necessário um *background* técnico de tecnologia, até porque sempre haverá a possibilidade de consultas com especialistas da área, providência recomendada e que devemos buscar. É claro que é esperado o mínimo de conhecimento e é, por isso, que você está no lugar certo.

Resumindo, podemos dizer que aqui você encontrará desde significados básicos do Direito Digital, de responsabilidade civil e de violência de gêneros, chegando até o tratamento de dados no Poder Público, ao papel do *data protection officer*, a aplicação da LGPD e aos desafios de sua implementação.

Dessa forma, cabe ressaltar, mesmo correndo o risco da obviedade, que o Direito Digital é muito mais que a Lei Geral de Proteção de Dados, abrangendo todos os ramos do Direito. Podemos até mesmo dizer que quem não se adequa ao mundo digital quase não existe ou, em última análise, ficará “velho”, “obsoleto”, diria mesmo ultrapassado.

Pode parecer um pensamento um tanto dramático, mas é a verdade. O que não está na rede, conectado ou na nuvem é facilmente despercebido ou esquecido na atualidade. Portanto, esteja digital e faça parte desse universo.

Não podemos nos esquecer que o mundo digital nada mais é do que o reflexo das culturas sociais!

1. INTRODUÇÃO AO DIREITO DIGITAL

Marcelo Camargo

O QUE É O DIREITO DIGITAL?

Direito Digital ou Virtual é uma evolução de todos os ramos do Direito que interagem com a sociedade digital ou com o meio ambiente digital. Ele alberga os princípios e institutos do Direito existentes, bem como os inova em suas diversas áreas de atuação, tais como no Direito Internacional, no Direito da Propriedade Intelectual, no Direito Constitucional, nos Direitos Humanos, na Bioética, nas pesquisas científicas e genéticas, no Direito Civil, Penal, Administrativo, Tributário, Financeiro, Ambiental, Processual, Previdenciário, Trabalhista, Eleitoral, no Direito Médico, entre outros.

QUEM INTEGRA A SOCIEDADE DIGITAL?

A sociedade digital é um conceito que leva em conta as pessoas físicas ou jurídicas que são usuárias da internet, das tecnologias de informação, de transmissão de dados, e até mesmo as pessoas que não têm acesso à internet ou a tais tecnologias, pois seus dados são coletados e transmitidos pela rede, muitas vezes independentemente do seu próprio conhecimento a respeito.

NO QUE CONSISTE O MEIO AMBIENTE DIGITAL?

O meio ambiente digital decorre da criação humana, é um patrimônio imaterial, virtual, um conjunto de condições, leis, influências e interações que acontecem no ambiente digital, através de software e hardware conectados, e que acabam por gerar efeitos nas pessoas, nas relações sociais, na política, na economia e no meio ambiente físico, até mesmo no extraterrestre, uma vez que dados são coletados e transmitidos por artefatos espaciais.

O MEIO AMBIENTE DIGITAL SE CONTRAPÕE AO MUNDO FÍSICO?

Não, ele não é desconectado do mundo físico onde seus efeitos ocorrem, ao revés, ele faz parte do mundo real, o qual sofre direta ou indiretamente suas influências e efeitos.

O DIREITO DIGITAL ESTÁ LIMITADO À INTERNET?

Não, a internet é apenas mais um dos meios, dos recursos tecnológicos em que o ambiente digital acontece, uma das inúmeras inovações tecnológicas que precisam ser disciplinadas pelo Direito Digital. Ele deverá regrar também outras inovações tecnológicas que estejam por vir. Sua evolução é rápida e dinâmica, acompanha as novas tecnologias que surgem a todo momento, acompanha a evolução da sociedade digital.

O DIREITO DIGITAL É UM DIREITO INTERNACIONAL?

Sim, a globalização das sociedades, o compartilhamento de tecnologias tanto pelos países quanto pelas pessoas e empresas, a coleta e troca de informações que ocorrem a todo instante, com efeitos em todos os cantos do planeta, exigem também uma globalização do pensamento jurídico, para que seja possível delimitar critérios mínimos a serem observados pelos diversos países e pelas pessoas. Assim, cada vez mais estão a surgir Convenções e Tratados Internacionais a respeito.

QUAIS SÃO OS PRINCIPAIS DESAFIOS DO DIREITO DIGITAL?

Atingir o consenso sobre a liberdade de acesso à informação entre nações reais e virtuais, e entre pessoas, com culturas e costumes tão diversos, com visões distantes sobre o que é a “dignidade da pessoa humana” a ser preservada, sobre até onde vai a soberania de cada país, definir os limites territoriais e físicos que tantas consequências trazem na análise dos atos e negócios jurídicos, e inclusive na esfera penal e do Direito Internacional Público e Privado.

DEVE SER PRIORIZADA A CRIAÇÃO DE NORMAS ESPECÍFICAS OU A DE NOVOS PRINCÍPIOS DE RELACIONAMENTO PARA A SEGURANÇA DAS RELAÇÕES VIRTUAIS?

Deve ser priorizada a criação de novos princípios de relacionamento, contendo requisitos básicos e gerais, pois normas específicas perderiam rapidamente sua eficácia no espaço e no tempo em razão da constante e rápida evolução das tecnologias e consequentes alterações no mundo virtual e físico.

NO DIREITO DIGITAL, ONDE SE ENCONTRA O MAIOR NÚMERO DE REGRAS?

Existem diversos Tratados, Convenções, Legislações e Instruções Normativas envolvendo o Direito Digital, os *disclaimers* publicados pelos provedores continuam sendo as normas que mais frequentemente se aplicam aos participantes das relações digitais. O Direito Digital, pela sua natureza global e em constante evolução, tende à autorregulamentação, que obviamente deve atender ao disposto em diversos ordenamentos jurídicos.

COMO SE DÁ A PUBLICIDADE DAS REGRAS NO DIREITO DIGITAL?

No ordenamento brasileiro, ninguém pode alegar o desconhecimento da lei, mas como no Direito Digital ocorre uma autorregulamentação imensa, há o dever de se dar maior conhecimento público das regras. Por isso é muito importante que os provedores façam a publicação clara e com destaque dos *disclaimers*, políticas de privacidade, enfim, de todas as regras e procedimentos que devem ser observados pelo seu público. O Direito Digital se socorre frequentemente do *pacta sunt servanda*, pois muitas vezes as únicas regras estabelecidas são as contratuais.

O QUE PODERIA MITIGAR O PROBLEMA DA OBSOLESCÊNCIA DAS NORMAS DO DIREITO DIGITAL?

Em decorrência da constante evolução e modificação do mundo virtual e físico, quanto mais genérica for uma norma, mais flexível e duradoura ela será. Estabelecer princípios que possam ser interpretados conforme evolui a sociedade digital e as tecnologias, seria o ideal.

COMO SE RELACIONA O DIREITO COSTUMEIRO COM O DIREITO DIGITAL?

O Direito Digital, com frequência, trabalha junto com o Direito Codificado e com o Direito Costumeiro, pinçando do Direito Costumeiro as soluções para as lacunas jurídicas existentes.

COMO SE DÁ A APLICAÇÃO DA ANALOGIA E DA ARBITRAGEM NO DIREITO DIGITAL?

Ela se dá de modo muito intenso, considerando a necessidade de uma solução rápida para eventuais problemas, que em muitos casos não podem esperar que tais soluções emanem do Legislativo e do Judiciário. Como as tecnologias se tornam obsoletas de forma muita rápida, muitas discussões judiciais poderiam se tornar ineficazes com o tempo, resolvendo, no máximo, problemas referentes à responsabilidade civil.

COMO SE DÁ A APLICAÇÃO DA UNIFORMIDADE ORIUNDA DO DIREITO COSTUMEIRO NO DIREITO DIGITAL?

Se dá de forma intensa, e recomenda-se que, quando houver uma decisão sobre um determinado tema comum aos outros sites, estes implantem as recomendações das respectivas decisões.

A PUBLICAÇÃO DAS DECISÕES ARBITRAIS PODERIA MITIGAR O PROBLEMA DA OBSOLESCÊNCIA DA JURISPRUDÊNCIA E DA FALTA DE UNIFORMIZAÇÃO DAS DECISÕES ARBITRAIS?

Sim, a publicidade de tais decisões seria um excelente norteador, mas muitas empresas insistem em manter confidencialidade em suas arbitragens.

APLICA-SE A INVERSÃO DO ÔNUS DA PROVA NO DIREITO DIGITAL?

No Brasil, em razão do Código do Consumidor, já se aplica há algum tempo a inversão do ônus da prova em contendas que envolvem consumidores e o Direito Digital, inclusive sobre seus dados pessoais. A Lei Geral de Proteção de Dados - LGPD veio reforçar a aplicação da inversão do ônus da prova também.

QUAIS AS PRINCIPAIS CARACTERÍSTICAS DO DIREITO DIGITAL?

Pouca legislação, mutabilidade e dinamismo, pois se socorrem do Direito Costumeiro, do uso da analogia e da arbitragem.

2. CINCO DESAFIOS DA IMPLEMENTAÇÃO DA LGPD: NAS EMPRESAS E DEMAIS ORGANIZAÇÕES.

Marília Kairuz Baracat

1º DESAFIO - CULTURA DAS EMPRESAS

As organizações brasileiras, sejam elas públicas ou privadas, assim como a própria sociedade civil, ainda não perceberam a importância dos dados pessoais para a lógica de funcionamento da internet e das redes sociais, com desdobramento em todas as esferas das nossas vidas. Portanto, a cultura de proteção de dados no país é ainda embrionária, sendo esta constatação um empecilho para a boa adaptação da LGPD nas organizações.

Diante desta realidade, acreditamos que um projeto de adaptação das empresas à LGPD não pode perder de vista o aspecto cultural, na tentativa de sensibilizar os gestores para a importância da proteção de dados para o futuro das organizações. É uma mudança lenta, gradual e que requer uma mudança de mentalidade.

2º DESAFIO - ALTA ADMINISTRAÇÃO

Este desafio decorre do primeiro, pois a alta administração, em muitos casos, não está devidamente sensibilizada para a proteção de dados e, em alguns casos, também está mal-informada principalmente quanto às consequências que a má gestão em privacidade pode causar à organização.

No Brasil e no mundo temos inúmeros exemplos de vazamento de dados e de outras práticas que interferem negativamente na imagem das empresas, no mercado em que atuam. Grandes empresas perdem seu valor de mercado rapidamente após este tipo de incidente ser divulgado pelas mídias.

Percebe-se a importância de as organizações desenvolverem um procedimento interno para os incidentes, tanto preventivamente como posteriormente

aos danos ocorridos após um incidente cibernético. Na era da hiperconectividade, precisamos dar respostas precisas e rápidas a respeito de um incidente de segurança a toda a sociedade. Estas respostas estão atreladas à imagem e reputação das empresas no mercado.

3º DESAFIO - GESTÃO DE PESSOAS

As organizações possuem ótimos profissionais de tecnologia da informação, de segurança da informação e da área jurídica. Entretanto, o profissional que vai lidar com as questões de privacidade e proteção de dados precisa ter conhecimentos e habilidades que perpassam mais de uma área do conhecimento.

Além disso, treinar o profissional para esta nova profissão requer tempo e investimento na carreira. Isto sem falar na importância de certificações para que se possam comprovar os conhecimentos adquiridos.

Temos visto muitos encarregados de proteção de dados serem nomeados sem possuírem o conhecimento necessário para a função. Entretanto, acreditamos que com empenho e muito estudo este profissional poderá adquirir as habilidades para ter sucesso em sua nova função. O importante é que o profissional possua algumas habilidades interpessoais, como se comunicar bem com o público interno e externo, ter facilidade e interesse para aprender assuntos de outra área de formação, para que possa levar adiante os temas de privacidade e proteção de dados dentro da organização, como treinamentos e elaboração de novas políticas.

4º DESAFIO - RECURSOS FINANCEIROS

Algumas pessoas e organizações apostaram que a LGPD não entraria em vigor em 2020, embora desde 2018 soubéssemos que a lei produziria seus efeitos a partir de agosto de 2020. É evidente que não podemos desconsiderar o impacto da pandemia nas organizações, mesmo sabendo que a crise econômica brasileira já assolava boa parte das pequenas e médias empresas no país. Vale frisar que a pandemia trouxe um cenário ainda mais agudo do ponto de vista econômico-financeiro para essas empresas que já sofriam com a crise político-econômica nacional. Além disso, a pandemia acelerou o processo de digitalização das atividades empresariais.

Esta digitalização também impacta significativamente as questões atinentes à privacidade e proteção de dados pessoais.

Dessa forma, a elaboração de projetos de implementação da LGPD passa por restrições orçamentárias e financeiras. Diante deste cenário, observa-se que as empresas precisam aproveitar seus quadros internos nas adequações e contratar consultorias que apresentem boas metodologias a um preço justo. Além disso, é importante a valorização da criatividade e de boas ideias trazidas pelas pessoas da organização e de consultorias especializadas. A criação de soluções caseiras para o mapeamento de dados e de gestão do consentimento é um dos exemplos que temos visto no nosso dia a dia.

Outra constatação que fazemos é que etapas dos projetos de adequação estão sendo reservadas para 2022, justamente para haver um planejamento orçamentário dessas ações. A contratação de *softwares* de gestão em proteção de dados é um bom exemplo. No geral, eles possuem preços elevados para a maioria das *startups* e pequenas empresas brasileiras. Além do mais, os encarregados de proteção de dados e suas equipes podem aproveitar esta fase inicial para testar metodologias e sistemas, inclusive para não errar na contratação de soluções tecnológicas.

5º DESAFIO - GESTÃO DE PROCESSOS

Nossa *expertise* mostra que a maioria das empresas brasileiras não possui seus macroprocessos desenhados e atualizados. Esta deficiência impacta de forma expressiva a governança de dados na organização. Os dados pessoais, além de terem um ciclo de vida próprio, passam por diversos departamentos das instituições.

Observa-se ser difícil e ineficaz desenhar um procedimento e um fluxo para os processos que envolvem os dados pessoais, se os demais processos não estiverem desenhados. Certamente, há inúmeros processos e fluxos internos que coletam, classificam, transferem e descartam os dados pessoais dentro da organização.

Uma dica que podemos dar é investir em gestão de processos criando um laboratório de processos, ainda que de forma incipiente. O encarregado de dados poderia dedicar parte do seu tempo melhorando estes processos nas empresas. Isto

facilitaria o trabalho deste profissional diante das inúmeras solicitações de usuários e clientes que irá receber nos próximos meses e anos.

3. RESPONSABILIDADE CIVIL NO DIREITO DIGITAL

Bárbara Franco Gonçalves Pinto
Isabella Pinto Barros de Andrade

INTRODUÇÃO

A sociedade passou por evoluções tecnológicas inimagináveis nos últimos tempos, sendo certo que muitos desses avanços desafiaram, e ainda desafiam, tanto a criação de novas legislações como a reflexão de tais mudanças nos processos e decisões judiciais, ante as inovações que significam. O instituto da Responsabilidade Civil no Direito Digital, sem dúvida, é algo novo que faz parte desse desafio.

Os meios digitais são uma realidade e não há dúvidas de que seu uso passou a ser essencial, não apenas para o acesso a informações, mas também para que se tenha acesso aos mais diversos serviços.

A pandemia trazida pelo coronavírus ampliou ainda mais esse cenário no que diz respeito ao uso de novas tecnologias e da internet: as pessoas passaram a fazer reuniões virtuais, as aulas passaram a ser *online*, as compras a cada dia mais são realizadas pela internet, até mesmo as consultas médicas passaram a ser realizadas a distância.

Ainda, a criação da Lei Geral de Proteção de Dados, por exemplo, trouxe uma enorme gama de direitos aos titulares de dados pessoais, e no contraponto, uma enorme responsabilidade àqueles que detêm tais dados.

Todas essas inovações trazem aos operadores do Direito questionamentos acerca da aplicação da lei vigente, bem como sobre a necessidade de avanços legislativos. No decorrer dos últimos anos, algumas novas legislações voltadas para o Direito Digital trouxeram apontamentos e parâmetros para tais mudanças, mas sem dúvidas é no dia a dia, com a jurisprudência sobre o tema, que verificaremos o maior impacto dessas alterações, sendo de suma importância a reflexão quanto a responsabilidade civil.

O QUE É DIREITO DIGITAL

Antes de se esclarecer o que vem a ser Direito Digital é importante tecer uma rápida análise do início da transformação digital na sociedade civil. Destarte, foi a partir da Quarta Revolução Industrial que os limites entre os mundos físico, biológico e digital foram eliminados, trazendo uma verdadeira interseção entre áreas até então divergentes em uma amplitude e velocidade jamais vistas, dando origem à base da chamada sociedade 4.0, que tem por essência as mais diversas ferramentas tecnológicas.

A convergência desses mundos deu origem a novas formas de organização dos modos de produção e das relações sociais, não apenas considerando a diminuição do tempo e da distância através da internet, mas também por provocar a alteração da forma de pensar, de viver e de agir da população mundial. E, nesse contexto histórico de transformação social, em decorrência do novo cenário disruptivo e globalizado, as ciências jurídicas não poderiam ficar de fora, sendo indispensável a sua adaptação à Era da sociedade digital.

O Direito Digital surge, então, como resultado dessas mudanças sociais e da necessidade de regulação das novas práticas dos atos da vida civil, em especial por meio da internet. Assim, não se trata de uma nova área jurídica, mas sim de uma forma de normatização das diversas áreas já existentes dentro de uma nova realidade de vida, de forma interdisciplinar, como uma evolução das ciências jurídicas de modo geral.

E, considerando que a internet não é juridicamente entendida como um novo "território" ou novo "lugar" a ensejar legislação própria, mas sim apenas uma nova "ferramenta" na prática dos mais diversos atos, lhe deve ser aplicada toda a legislação pré-existente, sempre que compatível, tal como ocorre com outros meios de comunicação.

No entanto, não obstante a regular utilização do ordenamento jurídico ante as particularidades das inovações tecnológicas, veio a ser necessária a criação de outros normativos legais em apreço à nova realidade digital, podendo-se pontuar, *e.g.*, a Lei nº 12.737/2012 (Lei Carolina Dieckmann), o Decreto nº 7.962/2013 (Comércio

Eletrônico), a Lei nº 12.965/2014 (Marco Civil da Internet) e a Lei nº 13.709/18 (Lei Geral de Proteção de Dados – LGPD).

O Direito Digital, portanto, como matéria multidisciplinar, impõe à sociedade o uso consciente da tecnologia e dos meios digitais, em especial da internet, de modo não só a aperfeiçoar as ações e relações cotidianas, mas também a resguardar o direito de quem tiver as suas prerrogativas desrespeitadas, garantindo, inclusive, a possibilidade de responsabilização civil do ofensor.

CONCEITO BÁSICO DE RESPONSABILIDADE CIVIL

A Responsabilidade Civil (Cód. Civil, arts. 186, 187, 927 e ss.) é o ramo do Direito que possibilita a uma pessoa, física ou jurídica, ter reparado eventual dano, seja patrimonial ou moral, individual ou coletivamente, provocado por outrem. Em apertada síntese, é um dever jurídico sucessivo que surge para recompor o dano decorrente da violação de um dever jurídico originário (CAVALIERI FILHO, 2010, p. 2).

Dentre as suas espécies, contratual e extracontratual, há no Direito Brasileiro duas principais teorias sobre a Responsabilidade Civil: a subjetiva e a objetiva. Em ambas é necessária a demonstração da ação ou omissão do ofensor, do(s) dano(s) e do correspondente nexo causal. Já a diferença é que, na primeira, é necessária, também, a comprovação da culpa do ofensor, fundamento o qual é dispensado na segunda teoria, que preconiza, por sua vez, o risco criado – gênero do qual nasceram espécies oponíveis em cada situação lesiva, como “risco proveito e do empreendimento” (por exemplo, no Direito do Consumidor); “risco administrativo” (no Direito Administrativo Constitucional); “risco profissional” (no Direito do Trabalho), entre outros (VIEIRA, 2006, p. 88-89).

Registre-se, porém, que não há, na lei civil atual, regra e exceção no trato das teorias de responsabilidade civil — ou seja, uma modalidade de responsabilidade civil não deve sobrepujar a outra, quando da prestação jurisdicional (VIEIRA, 2006, p. 22). O Direito Brasileiro passou, pois, a aceitar a convivência de ambas as modalidades. Por consequência, não se pode dizer que a regra será uma ou outra, mas sim que, *a priori*, a responsabilidade será subjetiva, ou seja, dependerá da comprovação de

culpa. Contudo, nos casos em que a lei assim determinar ou em que houver constatação de risco de danos para terceiros ante a atividade desenvolvida, haverá responsabilidade objetiva. (PINTO; VIEIRA, 2014, p. 46).

Como, porém, toda regra tem a sua exceção, o instituto em comento também possui hipóteses em que pode ser excepcionado. Assim, são excludentes da responsabilidade civil os casos de força maior, de fortuito externo, a culpa exclusiva da vítima ou de terceiro e os atos praticados no exercício regular de um direito, em legítima defesa ou em estado de necessidade.

Pode-se dizer, portanto, que o instituto da responsabilidade civil se aplica às mais diversas áreas do Direito, seja de forma isolada ou ainda de forma conjunta a regras de outras disciplinas, tais como penal, administrativo, consumerista e, inclusive, digital – que, como visto, pode englobar todas as matérias jurídicas.

A RESPONSABILIDADE CIVIL NO DIREITO DIGITAL

Considerando, pois, que a internet trouxe uma nova forma de interação entre as pessoas, e que no âmbito do Direito Digital utiliza-se tanto a legislação pré-existente como novas regras jurídicas a tal meio de comunicação, não é apenas possível, como devem os agentes de atos ilícitos responder civilmente pela violação a direitos e/ou garantias de outrem no mundo digital.

Isso porque, apesar de se tratar de uma realidade virtual, o alcance dos atos nela praticados adentram diretamente a vida real dos envolvidos, de forma muito rápida e com extensão incontrolável. Se por um lado a velocidade da propagação de informações na internet facilita o nosso dia a dia, por outro lado também proporciona a célere proliferação de ações criminosas, facilitando as mais diversas práticas danosas, sejam públicas ou privadas.

E a doutrina que trata da matéria afirma que tanto o usuário quanto o provedor de internet podem responder civilmente por eventual dano causado a outrem, de forma solidária ou subsidiária, não podendo nenhuma das partes alegar sua própria torpeza para se eximir de culpa concorrente (PINHEIRO, 2016, p. 514).

Em regra, a responsabilidade civil do provedor é subjetiva, devendo ser

apurada a sua culpa na manutenção do conteúdo danoso na rede ou na omissão e/ou demora na sua retirada. Isso, pois, como é vedado o anonimato, é obrigação do provedor prestar informações quanto à identidade do usuário, sob pena de responder civilmente pela publicação danosa.

No que tange à jurisdição, apesar da internet conectar o mundo inteiro, deve-se levar em conta, como acima narrado, que se trata tão somente de um novo "meio" de comunicação e não de um novo território. Assim, tem-se a aplicação da lei brasileira sempre que qualquer operação de coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet ocorra em território nacional, mesmo que apenas um dos dispositivos da comunicação esteja no Brasil e mesmo que as atividades sejam feitas por empresa com sede no estrangeiro (STJ RE no REsp: 1745657 SP 2018/0062504-5) (BRASIL, 2021).

A jurisprudência do Superior Tribunal Justiça, inclusive no acórdão acima destacado, é incisiva quanto à impossibilidade de utilização da internet como verdadeiro porto seguro e, ao mencionar a doutrina que trata do tema, afirma que, não sendo assim, poder-se-ia colher a sensação incômoda de que a internet é um refúgio, uma zona franca, por meio da qual tudo seria permitido sem que daqueles atos adviessem responsabilidades (Apud PAESANI, 2006, p. 36/60).

E foi nesse novo cenário, após muitas discussões sobre o alcance da responsabilidade civil nesse novo meio, que foram surgindo novas leis, nacionais e internacionais.

Em 2013, por exemplo, o Decreto nº 7.962/2013 veio a regulamentar o Código de Defesa do Consumidor, dispondo sobre o comércio eletrônico, estabelecendo condições e deveres para aqueles que exercem comércio eletrônico. Na sequência, o Marco Civil da Internet (Lei nº 12.965/2014) foi promulgado com o objetivo de estabelecer garantias e princípios aplicados ao uso da internet, na busca de ampliar o acesso à rede, bem como de delimitar direitos, deveres e garantias no uso desta.

Por fim, a entrada em vigor da Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados – LGPD, a qual se presta a tutelar os dados pessoais,

inclusive indicando severas multas para aqueles que descumprirem as obrigações ali previstas, sem dúvidas, significará enorme mudança conceitual, tanto daqueles que passaram a ter as obrigações, quanto dos cidadãos que passam a ter ali reconhecido seus direitos.

CONCLUSÃO

A partir das considerações tecidas, verifica-se que o Direito Digital, apesar de sua inovação, já possui tutela na legislação pátria, principalmente no que diz respeito à responsabilidade civil.

A verificação dos limites dessa responsabilidade, porém, talvez seja o maior desafio no âmbito do Direito Digital, já que no ambiente virtual nem sempre é possível delimitar adequadamente os agentes responsáveis por eventuais danos.

As legislações mais recentes sobre o tema buscam tutelar algumas questões que antes não encontravam qualquer guarida, como, por exemplo, a responsabilização pelo tratamento de dados pessoais, no caso da LGPD, e a responsabilidade criminal por delitos informáticos, como é o caso da Lei nº 12.737/2012 (Lei Carolina Dieckmann).

No entanto, sem qualquer dúvida, o Direito Digital ainda desafiará outras leis e ensejará muita reflexão do Judiciário, seja para exigir o cumprimento das inovações legislativas, seja para aplicar a legislação já em vigor às constantes e céleres mudanças trazidas com o progresso da tecnologia.

REFERÊNCIAS

BRASIL. **Decreto nº 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Brasília: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 19/07/2021

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19/07/2021

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19/07/2021

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19/07/2021

BRASIL. Superior Tribunal de Justiça. **Recurso Extraordinário no Recurso Especial 1745657 SP 2018/0062504-5**. Recurso Extraordinário. Direito Internacional. Fornecimento de Registro de Acesso de Endereço de e-mail. Marco Civil da Internet. Matéria Infraconstitucional. Ofensa Reflexa à Constituição Federal. Reexame do acervo fático probatório. Impossibilidade. Enunciado 279 da Súmula do Supremo Tribunal Federal. Recurso não admitido. Recorrente: Microsoft Informática Ltda. Recorrido: TAM Linhas Aéreas S/A. Relator: Min. Jorge Mussi. DJe de 18/02/2021.

CAVALIERI FILHO, Sérgio. **Programa de Responsabilidade Civil**. 9. ed. São Paulo: Atlas, 2010.

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

PINTO, Bárbara Franco Gonçalves; VIEIRA, Patrícia Ribeiro Serra. Desapropriação: Espécie de Ato Lícito Motivadora de Responsabilidade Civil Objetiva. **Revista da Seção Judiciária do Rio de Janeiro,** v. 21, n. 40, p. 45-67, 2014.

VIEIRA, Patrícia Ribeiro Serra. **A responsabilidade civil objetiva no direito de danos**. Rio de Janeiro: Forense, 2006.

4. DIREITO DIGITAL: O DIREITO À PRIVACIDADE E A VEDAÇÃO AO ANONIMATO NA ERA DIGITAL

Iasmin Neiva
Tarcila Bairral

Desde o surgimento dos primeiros computadores até os celulares com acesso à internet, o caminho árduo da inclusão digital veio se consolidando de maneira ampla, mas trouxe à baila uma questão vastamente discutida, o anonimato. Aliás, como ser anônimo com redes e mais redes de segurança que funcionam sem o usuário sequer ter a noção de que, a cada *site* aberto, os navegadores já captam a localização de quem os utiliza para as informações de busca?

Esse tipo de informação já tem contribuído em muitos casos para reaver o celular, *tablets*, *notebooks* ou outros pertences, como carros e até mesmo para encontrar pessoas sequestradas, tal a dimensão que esse tipo de conhecimento pode alcançar. Em contrapartida, pode gerar conflitos de interesses e de privacidade, também abarcados pela Constituição, e que ficariam cada vez mais mitigados nesse processo de rastreamento frente às questões de segurança.

Nessa direção, o Direito Digital torna-se um "híbrido" no que tange a harmonizar o saber jurídico com a realidade dos sistemas de informação.

4.1. DO DIREITO À PRIVACIDADE SOB O PRISMA DA CONSTITUIÇÃO FEDERAL

Compreende-se que qualquer ato, seja ele de natureza digital ou não, deverá seguir os princípios constitucionais vigentes. Um dos princípios exaltados na Constituição Federal em vigor está expresso em seu artigo 5.º, XII, que preconiza a inviolabilidade da correspondência ou dos dados:

> Art.5.º, XII - É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Desta forma, esse enunciado estabelecido na parte de Direitos e Garantias Fundamentais diz claramente que o envio de *e-mail* deverá ter seu sigilo resguardado. Ainda sobre o tema, o professor Mario Antônio Lobato Paiva ensina que a Carta Magna determina de maneira taxativa o respeito à vida privada e à intimidade do cidadão, que tem o direito de se corresponder via *e-mail*, sem que possam intervir, por tratar-se de informações de caráter íntimo, tendo a garantia de não as ver violadas por terceiros curiosos ou interessados.

É importante salientar que na ausência de leis que decidam esse conceito no mundo virtual, como bem elucida o Doutor Demócrito Reinaldo Ramos, "o instrumento do jurista no trato desses assuntos será inevitavelmente a Constituição Federal, onde estão assentes os princípios basilares desse direito personalíssimo" (RAMOS, 2002).

4.2. DA RESOLUÇÃO DO DIREITO À PRIVACIDADE NA ERA DIGITAL

Em 2015, o Conselho de Direitos Humanos da ONU aprovou uma resolução designando o mandato de um relator do direito à privacidade na era digital. Onde os integrantes daquele Conselho determinaram que o direito à privacidade é uma garantia:

> Segundo o qual ninguém será sujeito a interferências arbitrárias ou ilegais em sua privacidade, família, lar ou correspondência, bem como o direito à proteção da lei contra tais interferências, conforme estabelecido no artigo 12 da Declaração Universal dos Direitos Humanos e no artigo 17 do Pacto Internacional sobre os Direitos Civis e Políticos (ONU, 2015).

Com isto, o Conselho reconheceu o propósito de globalização e de abertura da internet bem como do progressivo desenvolvimento da tecnologia, da informação e da comunicação como alavanca para estimular o conhecimento em direção ao avanço em suas diferentes apresentações, reiterando ainda que os "mesmos direitos que as pessoas têm *offline* também devem ser protegidos *online*, incluindo o direito à privacidade" (ONU, 2015). O projeto de resolução solicitou ao relator especial que o coordenasse com foco nos desafios oriundos do mundo virtual e das novas técnicas aplicadas com o objetivo de coletar informações, verificar as tendências, formular as recomendações, opor-se aos obstáculos e violações e gerar princípios.

4.3. DA VEDAÇÃO AO ANONIMATO PELA CONSTITUIÇÃO FEDERAL DE 1988

O primeiro registro legal à vedação ao anonimato foi encontrado na Constituição Republicana Brasileira de 1891, onde se encontra expresso em seu art. 72, §12:

> Em qualquer assunto é livre a manifestação de pensamento pela imprensa ou pela tribuna, sem dependência de censura, respondendo cada um pelos abusos que cometer nos casos e pela forma que a lei determinar. *Não é permitido o anonimato*. (grifou-se)

Clara foi a intenção do legislador ao vedar esse tipo de postura a fim de coibir possíveis excessos, com o intuito de prevenir ofensas ao patrimônio moral nas publicações de livros, revistas e periódicos, como era de se esperar, dado o contexto da época da sua vigência, o que não queria dizer que não fosse assim respeitada a liberdade de pensamento.

O veto ao anonimato tem a sua abrangência aos meios de comunicação na Constituição Federal de 1988, no art. 5º, IV, pois estes envolvem a liberdade de expressão e a garantia da privacidade, do sigilo e dos direitos também previstos por esta. Antes de qualquer coisa, e muito óbvia, é a intenção da preservação da imagem daquele que se prevalece do anonimato, seja por ação ou omissão, como atualmente ocorre pela internet. Essa incógnita recai sobre o nome, a imagem, o endereço físico ou virtual (*e-mail*) e o endereçamento, ou número IP, ou um tipo de “véu” que oculte a real identidade do autor, que impossibilite a individualização do transmissor de dados.

Entretanto, apenas o sigilo das comunicações telefônicas pode ser “quebrado” para acrescentar uma investigação ou instrução de processo criminal. Pode parecer que nisso ocorra um tipo de “amparo” aos anônimos pelo sigilo, acarretando condutas irresponsáveis devido à sensação de impunidade que pode ser suscitada. Todavia, o sigilo está em um contexto que acata a razoabilidade e a moderação, como preconiza o sistema jurídico vigente, tanto que um fato é a quebra do sigilo, outro, é a permissão da transmissão desses dados.

O Ministro Carlos Velloso defendeu a tese de que acatar as condutas anônimas é conferir ao anônimo a respeitabilidade que ele não tem, pois o homem não precisaria esconder-se sob a capa do anonimato para dizer do caráter ou da conduta de alguém,

se se afasta a possibilidade desse alguém esclarecer as informações, realizar aquilo que é básico num Estado de Direito, que é o direito de defesa.

4.4. DO ANONIMATO ABSOLUTO E RELATIVO

Considera-se anônimo, de maneira absoluta, aquele que se oculta e que de maneira alguma consegue ser identificado. Mas, quando, mesmo agindo anonimamente, a um terceiro é possível alcançar a discriminação de sua identidade ou quando o agente é anônimo para determinada pessoa ou situação, diz-se que ela é relativa.

Há circunstâncias em que a identificação é forçosa, mas cada usuário está, na maioria das vezes, anônimo para os demais, incumbindo ao provedor de serviços ou de acesso, em seu domínio de competências, violar esse anonimato, concedendo a identificação ao solicitante, sendo considerado, obviamente, o devido processo legal. Caso não, o anonimato seria uma prática contumaz em que se prevaleceria a má-fé e a inidoneidade das informações prestadas, o que, taxativamente, é vedado pela Constituição.

4.5. DO DINAMISMO ÀS INOVAÇÕES DO DIREITO DIGITAL

Não há como negar que a extensão da vida particular, acadêmica e social repercute na internet, de maneira direta ou indireta, onde os efeitos da vida real se propagam, sendo algumas vezes o contrário! o virtual acarreta consequências no mundo real. Como não há que se falar em mero uso para uma simples troca de informações, é reconhecidamente um ambiente para realizar relações de consumo, de negócios, e isso não é em um lugar, não é em um território à parte, mas em um meio que demonstra cada vez mais palpável a sua interferência nas relações que se criam a cada *touch*.

De acordo com as especialistas em Direito Digital Patrícia Peck Pinheiro e Cristina Moraes Sleiman, devem levar em consideração alguns aspectos importantes:

> a) Toda mudança tecnológica é uma mudança social, comportamental, portanto, jurídica. Chegamos a "R" *Society* - Sociedade de Relações, de Indivíduos interconectados, acessíveis e interativos. Neste cenário um dos grandes desafios é de como fazer a gestão jurídica e logística

> das empresas e da sociedade de modo a gerar vantagem competitiva para os negócios e para o Brasil na era digital.
>
> b) Além do mais, é preciso considerar que se tratando da revolução do conhecimento cresce o valor da informação enquanto ativo intangível, e esta, por sua vez, passa a ser cobiçada pelos concorrentes, exigindo das empresas ações que garantam a segurança de sua informação.
>
> c) As relações humanas e a expressão de manifestação de vontade tomam nova forma, ou seja, ocorrem por diferentes meios eletrônicos e em tempo real e por sua vez exigem novos conhecimentos na busca de provas. Deve-se considerar que, na Sociedade Digital, integra-se ao quadro de testemunhas, não apenas o ser humano, mas também as máquinas. Imagine que em uma troca básica de *e-mails* entre duas pessoas, temos quatro testemunhas máquinas: a máquina do emissor e seu servidor (duas testemunhas) e a máquina do destinatário, bem como o servidor por ele utilizado caso seja diferente do emissor. Portanto, o meio digital permite que busquemos vestígios de uma ação por todo lugar onde passamos, ou melhor, por onde passam as informações.
>
> d) Os Negócios e as Relações da Era Digital são *E-mocionais* e há um limite entre tecnologia e ser humano. Embora as tecnologias se refiram às máquinas, não se pode esquecer que esta é comandada por um ser humano, ou seja, uma pessoa, que tem emoções e que utiliza a máquina como meio para manifestar sua vontade, seja em uma transação comercial ou em uma simples troca de mensagem pessoal, portanto, lidamos com pessoas e não apenas máquina.
>
> e) A questão da Territorialidade não pode ser esquecida, vez que temos transações e relações sejam de consumo ou simplesmente de comunicação entre diversos ordenamentos jurídicos, ou ainda crimes que se iniciam pela máquina que se encontra fisicamente em um determinado país, mas o resultado ou o serviço de *internet* utilizado se encontra em outro. Ou seja, temos o desafio de traçar a melhor estratégia (PECK; SLEIMAN, 2019).

Pensamento este corroborado pela doutora e autoridade em Direito Digital no Brasil Patrícia Peck Pinheiro, que entende que o virtual permite a existência legítima do estar “não-presente”. Do manifestar-se por intermédio de sistemas de comunicação telemática através de encontros móveis e transitórios de mensagens, com a desconexão em relação a um meio particular, com diversos meios de registro e transmissão oral, escrita e audiovisual em redes digitais, e ainda ressalta que:

> Se a *Internet* é um meio, como é o rádio, a televisão, o fax, o telefone, então não há que se falar em Direito de *Internet*, mas sim em um único Direito Digital cujo grande desafio é estar preparado para o desconhecido, seja aplicando velhas normas ou novas normas, mas com a capacidade de interpretar a realidade social e adequar a

> solução ao caso concreto na mesma velocidade das mudanças da sociedade (PINHEIRO, 2009).

Devido à celeridade do desenvolvimento tecnológico, é de se esperar que o Direito Digital faça mais uso dos princípios que dão normatividade legislativa, por isso essa competência jurídica. A tendência dessa disciplina jurídica é de se alongar para a autorregulamentação; os componentes diretos do assunto criam soluções práticas devido ao dinamismo exigido pelas relações do Direito Digital. Outra inovação é a publicidade de um termo de responsabilidade ou aviso legal na própria página de quem presta o serviço, que notifica o leitor de um determinado documento das responsabilidades adquiridas ou não ante aquele ato (*disclaimers)*, desse modo, o público tem conhecimento para aderir àquele produto ou serviço, o que potencializa a sua eficácia.

O Direito Digital nortear-se-á por princípios. Os novos institutos jurídicos que venham a tratar do tema necessitam vir em formato genérico e flexível para resistirem e darem conta da agilidade das mudanças, para não se tornarem obstáculo na evolução jurídica das formas que ainda poderão ou mesmo irão surgir.

4.6. CONSIDERAÇÕES FINAIS

É razoável que no mundo virtual, em que tudo e todos estão atrelados através do fluxo de informações quase que instantâneo, a definição de limite ceda lugar para a de compartilhamento. Este, por sua vez, surge como inquietação no cenário jurídico pelos desdobramentos da conectividade; grande troca de informações e armazenamento de dados, intensificados à medida que mais equipamentos têm a possibilidade de interação virtual, que impacta os direitos constitucionais de privacidade e dados pessoais como preferências, localizações, rotinas e informações confidenciais. Afinal, onde começaria o direito à privacidade do outro e de que forma isso seria garantido pelas vias legais caso fosse obstruído?

O Ordenamento Jurídico prevê no art. 5º, inciso X da Constituição que “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”.

O direito à privacidade é devidamente assegurado como direito personalíssimo por se tratar de atos da vida pessoal, abarcando as pessoas físicas como as jurídicas. Isso implica dizer que a própria pessoa tem a capacidade de domínio da sua imagem e da sua reputação, da mesma maneira que poderá ou não disponibilizar as informações a seu respeito e acreditar pertinentes, ou seja, seria mais próximo de uma presunção de privacidade.

Considera-se o anonimato um obstáculo à segurança no ambiente virtual por conta da probabilidade de o agente adentrar-se sigilosamente para o cometimento do ato ilícito e isso o torna distintamente oposto ao sentido do direito à privacidade.

Como bem exemplificou o ilustre doutor Alexandre de Moraes citando Pinto Ferreira, “o Estado democrático defende o conteúdo essencial da manifestação da liberdade, que é assegurado tanto sob o aspecto positivo, ou seja, proteção da exteriorização da opinião, como sob o aspecto negativo, referente à proibição da censura” (MORAES, 2014).

Ao Direito cabe se encaixar nesta nova configuração, discutindo soluções para acompanhar uma sociedade cada vez mais digital. Logicamente, o mundo é outro, mas é primordial lidar com conflitos de maneira sensata. Deste modo, não se deve defender a existência de lacuna impreenchível derivada da tecnologia, uma vez que os princípios vigentes satisfazem a matéria, sendo mister uma interpretação coerente.

Por fim, compreende-se que o Direito deve partir do fato de se respirar e se relacionar em uma sociedade globalizada e um de seus máximos desafios é possuir um completo ajustamento entre culturas díspares, sendo fundamental instituir uma flexibilidade de raciocínio e não as mordaças de uma legislação positivada que pode ficar obsoleta em sua negação. Nesse cenário, o Direito brasileiro tenta acompanhar as mudanças sociais e tem dado passos para a evolução do Direito Digital e suas aplicações.

REFERÊNCIAS

BRASIL. **[Constituição (1891)].** Constituição da República dos Estados Unidos do Brasil. Rio de Janeiro: Senado Federal, 1891. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao91.htm. Acesso em: 01 maio 2021.

BRASIL. **[Constituição (1988)].** Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 maio 2021.

MORAES, Alexandre de Moraes. Direito Constitucional. Editora Atlas. 30.ª Edição. 2014.

ONU - Conselho de Direitos Humanos da ONU resolução 2015 – Declaração Universal dos Direitos Humanos. Disponível em: http://www.humanrights.com/pt/what-are-human-rights/universal-declaration-of-human-rights/articles-11-20.html. Acesso em: 01 maio de 2021.

PAIVA, Mário Antônio Lobato de. **Os institutos do direito informático.** Jan, 2003. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/30390-31543-1-PB.pdf. Acesso em: 01 maio 2021.

PAIVA, Mário Antônio Lobato de. **Primeiras linhas em Direito Eletrônico**. jan 2003. Disponível em: https://jus.com.br/artigos/3575/primeiras-linhas-em-direito-eletronico. Acesso em: 01 maio 2021.

PINHEIRO, Patrícia Peck; SLEIMAN, Cristina Moraes. Direito digital e a questão da privacidade nas empresas. Disponível em: https://ambitojuridico.com.br/edicoes/revista-55/direito-digital-e-a-questao-da-privacidade-nas-empresas/ Acesso em: 01 maio 2021.

RAMOS, Demócrito Reinaldo. Privacidade na “Sociedade da Informação”. In Direito da Informática: Temas polêmicos. Editora Edipro, 1.º edição, 2002, p. 28.

5. O PAPEL DO *DATA PROTECTION OFFICER:* FRENTE AOS DESAFIOS DA PROTEÇÃO À PRIVACIDADE E CIBERSEGURANÇA

Fernanda Couzzi Velasco
Mona Freitas O. Meirelles

O *Data Protection Officer*, ou DPO, é uma das principais figuras do sistema brasileiro de proteção de dados pessoais. Também chamado de “encarregado pelo tratamento de dados pessoais”, o DPO é definido pela própria Lei Geral de Proteção de Dados, em seu artigo 5º, VIII, como a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados".

A necessidade de nomeação de um encarregado por parte do controlador em face das atividades e ações relativas ao tratamento de dados busca garantir que as informações fiquem centralizadas e que a aplicação da norma seja efetiva.

Também definidas pela GDPR, o DPO tem na referida lei as seguintes funções:

- É envolvido de forma adequada e em tempo útil em todas as questões sobre proteção de dados;
- Possui amplo acesso aos dados pessoais e às operações de tratamento;
- Não recebe instruções;
- Não pode ser penalizado pelo exercício de suas funções;
- Reporta ao mais alto nível;
- Possui ponto de contato com os titulares;
- Possui o dever de confidencialidade; e
- Não pode haver conflito de interesses.

No Brasil, busca-se, com a determinação do art. 41 da LGPD, garantir que as informações fiquem centralizadas e que o controlador se certifique de que a aplicação das normas receberá efetiva validação.

Registre-se que, conforme preconiza o §2º do referido artigo, o DPO (encarregado), aquele indicado pelo controlador para tratamento de dados pessoais, possui as seguintes atribuições:

- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- receber comunicações da autoridade nacional e adotar providências;
- orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- executar as demais atribuições (controlador ou Autoridade)

Portanto, veja-se que o papel do DPO nada mais é do que garantir que os dados de clientes e/ou colaboradores de uma empresa sejam coletados, armazenados e utilizados de forma ética, legítima - isto é, coletados com consentimento do usuário, de forma transparente, inequívoca e segura, adotando medidas técnicas, operacionais e legais dentro das empresas para que ajam em conformidade com a lei, uma vez que ele é o elo que liga o titular do dado pessoal à própria empresa e à Autoridade Nacional de Proteção de Dados (ANPD).

Quando falamos em proteção de dados não podemos esquecer a importância de se atuar sobre três pilares estratégicos: a própria **tecnologia**, ou seja, os recursos tecnológicos que irão garantir a segurança das informações; o **aspecto jurídico**, que engloba questões sobre como esses dados serão utilizados e quem irá consumir esses dados; e, por fim, a **operação**, ou seja, todos os processos de estruturação de negócios.

Porém, a escassez sobre uma visão multidisciplinar para montar uma estrutura de, por exemplo, Segurança da Informação e Proteção de Dados, para que haja atuação integrada, pode ser considerada, hoje, um dos maiores desafios enfrentados

pelas companhias e pelos próprios profissionais da área, o que pode comprometer o sucesso de uma organização.

Por se tratar de uma temática recente no Brasil, este problema tem sido acentuado pela falta de mão de obra especializada efetivamente qualificada para a função, dificultando ainda mais o acesso por parte das empresas interessadas em aperfeiçoar a segurança da informação de seus ambientes de TI, sejam eles presenciais ou remotos.

Contudo, ficam algumas questões a respeito deste desafio: Como serão monitoradas as áreas da empresa que têm acesso a dados pessoais? Como evitar os vazamentos? Quais as consequências?

É nesse momento que empresas especializadas em serviços de cibersegurança têm assumido um papel fundamental nas estratégias das organizações ao apoiá-las na criação e desenvolvimento de padrões, de pessoal e de fluxos de trabalho, a fim de estabelecer uma cultura de privacidade e segurança da informação, fazendo uma análise macro da infraestrutura do ambiente de TI, mapeando todos os processos para levantar as fragilidades e riscos da rede, agregando valor a esse mercado na relação custo-benefício, unificando os resultados obtidos, planejando as ações de melhorias com a gestão de riscos e acompanhamento de toda a execução, mantendo sob controle total o ambiente virtual corporativo de todos os tipos de ataques cibernéticos.

O DPO precisa criar relacionamentos sólidos com áreas-chave da empresa para garantir o desempenho do seu papel, principalmente com aquelas que lidam com uma grande quantidade de dados como por exemplo, o Marketing, o Jurídico e a Segurança da Informação. Isso quer dizer que ele vai precisar "costurar" muito bem com esses líderes a necessidade de implementar políticas e processos que vão garantir a privacidade dos dados, sem impactar negativamente o resultado de uma área.

Outro grande desafio a ser enfrentado é a falta de protocolos para a proteção de dados. Apesar da existência das normas ISO, como a 27001, voltada para o Sistema de Gestão de Segurança da Informação (ABNT, 2006), o DPO, na grande

maioria das vezes, necessita criar processos, metodologias e pontes de relacionamento com outras áreas, atuando, então, sozinho, tendo que chegar para “arrumar a casa”, antes de iniciar a caminhada para a formação de uma área específica.

Por isso, seu grande desafio nesse sentido é convencer seus líderes ou o *board* da empresa para a criação de uma nova área para proteção e fomentar uma cultura organizacional de privacidade.

Além disso, some-se essa responsabilidade ao trabalho do dia a dia:

- Administrar regras de proteção de dados
- Monitorar a conformidade com a LGPD
- Registrar a conformidade das atividades de processamento de dados
- Visualizar todas as práticas de processamento
- Prever e avaliar riscos
- Realizar avaliações DPIA (avaliação de impacto de proteção de dados), quando aplicável
- Gerenciar solicitações de acesso aos dados
- Confirmar legítimo interesse dos usuários em receber comunicações e compartilhar seus dados

Ademais, ainda que o DPO possua como um grande desafio a implementação de uma cultura preventiva a vazamento de dados, obter processos e ferramentas para garantir a visibilidade sobre possíveis sinais de vazamentos, ainda é essencial.

Sabe-se que hoje, cada vez mais, existem eventos de fraudes e é preciso que sejam tomadas rápidas atitudes para que esses danos não sejam de grandes proporções. Vale lembrar que a identificação de um incidente nem sempre é algo simples e rápido, não sendo raros os eventos em que os sistemas permanecem invadidos e sob ameaça durante alguns meses, antes que seja efetivamente constatada sua violação.

Assim, é mais do que recomendável que exista um responsável por esse trabalho, que conte com, no mínimo, representantes dos Departamentos de

Tecnologia, Segurança da Informação, Jurídico, Relações Públicas e Comunicações, sendo estes acionados para compor o “Comitê de Crise” e executar as ações necessárias para responder eficientemente ao eventual incidente.

A atuação desse profissional é bastante ampla, já que envolve os conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente os relativos aos temas de privacidade e proteção de dados pessoais; análise jurídica; gestão de riscos; governança de dados e acesso à informação no setor público.

A conclusão é que, hoje, muitas empresas e/ou entidades acabam tendo dificuldade na hora de contratar alguém com tal especialidade, uma vez que esta é uma função relativamente nova e que combina habilidades de diferentes áreas.

Por isso, é comum que inúmeras organizações terceirizem o serviço, contando com empresas de consultoria e escritórios de advocacia especializados em segurança de dados.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: Tecnologia da informação. Técnicas de segurança. Sistemas de gestão de segurança da informação. Requisitos. Rio de Janeiro: ABNT, 2006.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19/07/2021

6. A Aplicação da Lei Geral de Proteção de Dados no E-Commerce

Fernando Galba
Louana Costa

O avanço tecnológico e as novas ferramentas criadas para viabilizar as relações estabelecidas por meio virtual trouxeram consigo a explosão de negócios jurídicos celebrados por este meio alternativo, fomentando e impulsionando o comércio eletrônico – *e-commerce*.

A consequência lógica, apesar da existência de uma norma geral que trata sobre a relação de consumo, Lei nº 8.078 de 11 de setembro de 1990, popularmente conhecida como Código de Defesa do Consumidor, legislação que dispõe sobre os direitos e obrigações dos polos envolvidos, composto, em regra, por fornecedores, prestadores de serviços e consumidores, é que percebeu-se a necessidade do desenvolvimento de um regramento próprio, que contivesse no seu bojo essa nova perspectiva de comércio eletrônico.

Em um primeiro momento, entrou em vigor a norma conhecida como Lei do E-commerce (Decreto nº 7.962 de 15 de março de 2013), com o objetivo de dispor sobre a contratação do comércio eletrônico, impondo a obrigatoriedade de informações claras a respeito do produto, serviço e do fornecedor, atendimento facilitado ao consumidor, respeito ao direito de arrependimento, bem como a necessidade de utilização de mecanismos de segurança eficazes para o pagamento e para tratamento de dados do consumidor.

Apesar do avanço da legislação, propiciando regras mais claras para a realização do comércio eletrônico, o tratamento dos dados dos usuários, especialmente o dos consumidores, carecia de regras objetivas e sanções administrativas específicas, ainda que o Judiciário, utilizando normas constitucionais e infraconstitucionais, inclusive a Lei nº 12.965, de 23 de abril de 2014 (conhecida como Marco Civil da Internet), condenasse os fornecedores e prestadores de

serviços na ocorrência de abuso ou na falta do dever de cuidado no tratamento de dados dos usuários, na obrigação de fazer ou deixar de fazer, além de perdas e danos.

A consequência lógica foi a necessidade da criação de um regramento próprio para o tratamento de dados pessoais, o que veio a ocorrer através da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O escopo da legislação é bastante amplo e atinge o tratamento de dados por meio físico ou digital, mas afetou direta e significativamente as empresas que prestam serviços ou comercializam os seus produtos por meio do comércio eletrônico, e que tiveram aumento abrupto de vendas e negócios celebrados em decorrência da pandemia causada pela COVID-19 e pelo isolamento social imposto pela administração pública em 2020/2021, fatalmente aumentando o banco de dados pessoais dos usuários.

As empresas que utilizam o comércio eletrônico deverão tratar os dados de seus usuários, o que acarreta a necessidade de tratamento de toda a operação em que seja necessário o uso dos dados pessoais, como a que se refere à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A obrigação basilar para as empresas que exploram o comércio eletrônico é observar as regras impostas pela LGPD no momento da coleta das informações pessoais do usuário/consumidor, garantindo que a manipulação dos dados ocorra somente mediante expressa autorização, indicando ainda os limites de utilização dos dados para o fim específico a que se destina, sob pena de, não o fazendo, ficarem expostas a sanções administrativas, sem prejuízo das perdas e danos causados ao consumidor lesado.

Por isso, é essencial que as empresas atualizem o seu Termo de Uso, seu aviso de privacidade, políticas de *cookies*, entre outros, adequando-se ao que dispõe a LGPD, prestando informações claras e de forma detalhada sobre o uso e o tratamento de dados pessoais, bem como sobre a finalidade da coleta, para que o usuário possa ter ciência inequívoca e possa, de forma consciente, consentir de forma expressa por meio de autorização específica.

As atualizações necessárias nos citados documentos poderão variar, dependendo da atividade ou serviço prestado pelas empresas, mas a regra geral é que deverá conter e resguardar os seguintes direitos dos usuários:

• O detalhamento da finalidade da coleta de dados, desde o acesso ao sítio de internet, aplicativo ou similares utilizados para o comércio eletrônico;

• A garantia de que os seus dados pessoais serão tratados;

• A garantia de que poderá acessar os seus dados pessoais;

• O acesso e a possibilidade de corrigir os dados pessoais que considerar incompletos, com informações equivocadas ou que não estejam atualizados;

• A garantia de que, no tratamento de dados pessoais, em relação àqueles que julgar excessivos ou em desconformidade com as regras da LGPD, poderá eliminar ou anonimizar os dados;

• A informação sobre o compartilhamento dos seus dados e a garantia de que poderá obter as informações sobre quem recebeu os seus dados;

• A garantia de que o usuário será informado em caso de alterações das informações e, no caso em que é exigido o consentimento, a possibilidade de revogação em caso de discordância;

• Definição das políticas de segurança e proteção de dados.

É importante ressaltar que o usuário deverá ser informado sobre a política de *cookies* (TECMUNDO, 2018), que é um pequeno arquivo enviado ao navegador do usuário que registra as suas preferências quando do acesso à página de comércio

eletrônico de determinado prestador de serviço ou fornecedor. Essa informação deverá ocorrer de forma imediata e simples, quando do acesso pelo usuário, necessitando ainda de um consentimento específico.

O não atendimento às regras previstas na LGPD poderá acarretar ao infrator as sanções administrativas impostas pela Autoridade Nacional de Proteção de Danos, responsável por fiscalizar o cumprimento da norma, que poderá ser desde a advertência, suspensão, bloqueios, proibição e eliminação de dados até a aplicação de multas de até 2% (dois por cento) do faturamento da empresa, limitada ao teto de R$ 50.000.000,00 (cinquenta milhões de reais). As sanções poderão ser aplicadas a partir do dia 01 de agosto de 2021 (BRASIL, 2018).

Portanto, concluímos que a LGPD trouxe grande avanço no tratamento de dados, com regras objetivas e sanções coercitivas e punitivas, que obrigam os prestadores de serviços e fornecedores que utilizam o comércio eletrônico a diligenciarem para garantir o direito de tratamento adequado dos dados pessoais dos usuários, desde a coleta até a eliminação.

REFERÊNCIAS

BRASIL. **Decreto nº 7.962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Brasília: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 19/07/2021

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19/07/2021

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19/07/2021

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19/07/2021

TECMUNDO. **O que são cookies?** 01 dez. 2018. Disponível em: https://www.tecmundo.com.br/web/1069-o-que-sao-cookies-.htm. Acesso em: 19/07/2021

7. O Poder Público e o Tratamento de Dados Pessoais

William Lima Rocha
Rodrigo Borges Valadão

A informação passou a ser um bem jurídico essencial para as mais simples vidas individuais e para as mais poderosas empresas e nações. O progresso tecnológico cresce, mas aumentam também os perigos de falta de respeito aos direitos humanos.

Matéria de Direito Civil e previsão constitucional, a proteção de dados pessoais pode ser interpretada como um desdobramento do direito fundamental à privacidade, protegido pela Constituição Federal de 1988 - CRFB, em seu artigo 5º, inciso X, que prevê que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação".

Com a edição da Lei nº 13.709, em 14/08/2018, a chamada LGPD - Lei Geral de Proteção de Dados Pessoais –, o Brasil passou a ter sua própria lei de proteção dos dados pessoais[1]. Deve-se destacar que o texto original da LGPD teve alguns dispositivos modificados pela Lei nº 13.853, de 08/07/2019, especialmente no tocante à constituição e ao funcionamento da Autoridade Nacional de Proteção e Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Além disso, a LGPD tem capítulo específico sobre o tratamento de dados pelo Poder Público, no qual explicita sua aplicabilidade a todos os entes da administração direta e indireta da União, dos Estados, dos Municípios e do Distrito Federal, inclusive

[1] LGPD - Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)
I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)
I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)
II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)
*II - em 3 de maio de 2021, quanto aos demais artigos. (Redação dada pela Medida Provisória nº 959, de 2020)
*OBS.: Com a não aprovação deste item da MP 959, voltou a valer a redação anterior do inciso II

suas Cortes de Contas, Ministérios Públicos e entidades privadas sem fins lucrativos que recebam recursos públicos.

Como já é sabido, a LGPD não se limita a regular o tratamento de dados pessoais nas relações privadas. Em seu Capítulo VI há uma série de dispositivos direcionados especificamente ao tratamento de dados pessoais pelo Poder Público. Embora submetidos a um tratamento especial, seja no que diz respeito aos limites materiais de incidência, seja no que diz respeito aos limites das sanções aplicáveis ao Poder Público.

Desta proposta de incidência *a posteriori* do princípio da finalidade, no tratamento de dados pessoais que independem do consentimento, decorre outra diretriz não menos importante e que poderia ser apresentada como uma espécie de diretiva de *design* de privacidade mínimo para a formulação de políticas públicas e da própria legislação editada pelo Poder Público (*Privacy by Design*). Explica-se.

Como foi visto acima, há hipóteses de tratamento de dados pessoais em que o consentimento livre e informado do titular não é exigido. Essas hipóteses são, sobretudo, aquelas hipóteses em que a lei assim autoriza. A ideia aqui proposta é simples: ao autorizar o tratamento de dados sem a manifestação do consentimento prévio do titular – ou em qualquer outro caso, a legislação deve sempre garantir que ele possa tomar conhecimento do tratamento realizado com os seus dados de forma precisa. Exatamente nesse sentido posicionou-se o Tribunal Constitucional Federal da Alemanha ao declarar a inconstitucionalidade da Lei do Censo de 1983, que permitia o tratamento indistinto de dados pessoais para fins administrativos e estatísticos, o que tornaria impossível permitir que o indivíduo conhecesse como seus dados foram efetivamente tratados pelo Poder Público.

Quando dirigido ao Poder Público, o princípio da finalidade do inciso I do art. 6º da Lei nº 13.709/2018 parece indicar que a própria concepção da política pública, já durante o processo legislativo legal ou infralegal, deve levar em conta em seu *design* esta exigência finalística, garantindo que o titular, ainda que em momento posterior ao tratamento dos seus dados pessoais, tenha pleno conhecimento de tudo o que foi feito com eles. Isso, claro, sem prejuízo do dever de que o *design* normativo garanta outros direitos dos titulares, como o direito de que seus dados sejam tratados de forma

adequada, no volume necessário, com o registro de todas as operações de tratamento e eventual responsabilização do agente que realizar o tratamento irregular.

O conceito de dados pessoais surgiu com a internet, *autodeterminação na sociedade da informação (jurisp. Alemanha*) vindo a exigir a transparência sobre coleta, finalidades, utilização, direito de acesso, retificação. (ALBERS, Marion. 2005)

Na União Europeia: pessoa identificada ou identificável, direta ou indiretamente por meios com razoável probabilidade de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa (*ex. nome, número de identificação, dados de localização, elementos específicos próprios à sua identidade física, fisiológica, genética, psíquica, econômica, cultural ou social) (correlações).*

Qual o conceito de dado pessoal? A LGPD traz um conceito bem abrangente de dado pessoal, definindo-o como toda informação relacionada à pessoa natural (pessoa física) identificada ou identificável.

São exemplos de dados pessoais: *nome, CPF, RG, filiação, e-mail, endereço, data de nascimento, hábitos de consumo, geolocalização, identificadores eletrônicos, entre outros.*

Quem é o titular dos dados pessoais? O titular dos dados pessoais é a pessoa natural (pessoa física) a quem se referem os dados pessoais que são objetos de tratamento.

Toda decisão de solicitação de dados deve ser motivada, ou seja, precisa ficar documentado qual o objetivo do pedido de informações. A LGPD, inclusive, traz um capítulo específico sobre o tratamento de dados pessoais pelo Poder Público.

O principal requisito permissivo para o tratamento de dados pessoais pela Administração Pública é o que está presente no artigo 7º, III, como se vê da transcrição:

> *Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
>
> *III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em*

> *leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta lei; (grifado)*

A execução de políticas públicas é, portanto, a principal e indubitavelmente a melhor justificativa para que o setor público realize qualquer tipo de tratamento de dados. Sendo este um conceito muito amplo, dando larga margem para a manipulação dos dados pessoais pelo setor público, uma vez que é inerente à própria existência do Estado a consecução de políticas públicas.

O fato é que o nosso sistema de proteção de dados gira em torno dos direitos do titular e, como consequência, na regulação do consentimento. No entanto, sem diminuir a importância que o consentimento livre e informado do titular desempenha no nosso sistema, parece que há diversas exceções onde o tratamento de dados pessoais, independentemente do consentimento do titular sobre uma finalidade determinada, torna-se possível.

É o que ocorre, por exemplo, no caso de um tratamento de dado pessoal por terceiro para a preservação da saúde do titular. Suponha uma situação em que determinada pessoa seja ferida com gravidade e, sem consciência, seja encaminhada para um hospital público. A toda evidência, a unidade hospitalar teria autorização legal (art. 7º, incisos VII e VIII da LGPD) para tratar os dados pessoais do paciente enquanto durar seu estado de inconsciência. Informar a finalidade do tratamento para, a partir daí, obter o consentimento do titular, seria não apenas completamente dispensável, mas simplesmente impossível de ser obtido.

Ao que parece, o princípio da finalidade, na forma nominal apresentada pelo inciso I do art. 6º da LGPD, deverá nortear principalmente as operações de tratamento de dados pessoais que tenham sua base legal (remota) na manifestação livre e informada da vontade do titular, como, por exemplo, ocorre com o consentimento (art. 7º, inciso I) e execução de contrato (art. 7º, inciso V). Nas operações de tratamento que independem, como regra, da manifestação de vontade do titular, parece que o princípio da finalidade tem uma forma de incidência um pouco diferente. Nestes casos, sua incidência é posterior ao tratamento, no sentido de garantir ao indivíduo a possibilidade de que ele possa tomar conhecimento a qualquer momento de quais dos seus dados foram tratados, por quem foram tratados e como foram tratados.

Com a opção legislativa por exigir somente o propósito legítimo – e não legítimo interesse – para fundamentar o tratamento de dados disponíveis publicamente, depreende-se que a intenção do legislador foi criar um fundamento legal mais flexível para esse tipo de tratamento, reconhecendo a importância e a finalidade de fontes públicas de dados pessoais. Na própria exposição de motivos da emenda parlamentar que levou à criação do Art. 7º, § 7º, o relator reconhece que, *"quando ele é publicamente acessível, o dado pessoal passa a ser um importante elemento para a realização de análises e estudos, […] promovendo competividade, inovação, empregabilidade e prosperidade"*.

7.1 CONCLUSÃO

Fatos que envolvam órgãos públicos, pela LGPD, não estarão sujeitos às sanções de multas, apenas a advertências e à eliminação de dados. Entretanto, isso não significa que servidores públicos envolvidos nos casos não sejam punidos ou penalizados.

Para o setor público, o tratamento de dados pessoais não se inicia, em geral, a partir de uma decisão voluntária do titular, mas como decorrência das exigências do próprio pacto social disposto no ordenamento jurídico pátrio, já que conhecer seus cidadãos é, para o Estado, um pré-requisito para o próprio exercício de desempenho de suas finalidades públicas.

Concluindo, faz-se necessário encontrar um ponto de equilíbrio entre os direitos existentes no que toca à coleta de dados dos usuários dos serviços públicos, realizando um juízo de ponderação entre a autonomia da vontade e a liberdade de contratar, traduzida pelo princípio da livre iniciativa (art. 1º, IV da CF. c/c art. 2º, VI da LGPD) e o direito à privacidade e à proteção de dados pessoais, cumprindo a Lei Geral de Proteção de Dados um relevantíssimo papel neste sentido.

REFERÊNCIAS

ALBERS, Marion. **Informationelle Selbstbestimmung**. Berlin: Nomos, 2005, p. 153ss

BRASIL. **[Constituição (1988)].** Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19/07/2021

BRASIL. **Decreto nº 10.474, de 26 de agosto de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Brasília: Presidência da República, 2020. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm. Acesso em: 19/07/2021

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em:19/07/2021

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Altera a Lei no 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm Acesso em: 19/07/2021

MULHOLAND, Caitlin et MATERA, Vinicius. **O Tratamento de Dados Pessoais pelo Poder Público**. In: MULHOLLAND, Caitlin (Coord). A LGPD e o Novo Marco Normativo no Brasil, Porto Alegre: Arquipélogo, 2020, p. 224.

WIMMER, Miriam. **Proteção de Dados Pessoais no Poder Público: incidência, bases legais e especificidades**. *In*: Revista do Advogado (ASSP), nº 144, nov/2019, p. 126-133; ALVES, Fabrício da Mota. **Desafios da Adequação do Poder Público à LGPD**. *In*: PALHARES, Felipe (Coord.). Temas Atuais de Proteção de Dados, São Paulo: Thompson Reuters Brasil, 2020, p. 171-195;

8. DIREITO DIGITAL E A VIOLÊNCIA DE GÊNERO

***Carla Maria Martellote Viola*[2]**

Os benefícios que o desenvolvimento das Tecnologias de Informação e Comunicação (TICs) e da internet trazem para as sociedades não são vivenciados e experienciados de forma equânime por homens e mulheres. Além disso, como a ideologia da sociedade global da informação é a do mercado, a liberdade de expressão comercial tem, neste quadro, toda a prioridade sobre a liberdade de expressão dos cidadãos.

Em 2005, a UNESCO publicou o seu *Relatório Mundial – Rumo às Sociedades do Conhecimento* com o objetivo de mudar o foco do debate global sobre "sociedades da informação" para o conceito mais amplo, complexo e empoderador de "sociedades do conhecimento" (UNESCO, 2005). Essa foi uma grande contribuição da UNESCO para a *World Summit on the Information Society* - WSIS (Cúpula Mundial da Sociedade da Informação), em colaboração com a União Internacional de Telecomunicações (UIT) e outros parceiros. Para a UNESCO, sociedades do conhecimento são aquelas que se beneficiam de sua diversidade e de suas capacidades de incentivar o compartilhamento do conhecimento. Essas sociedades oferecem muitas oportunidades novas para o desenvolvimento com apoio de inovações tecnológicas e participação em larga escala na produção e no consumo de informação. O relatório apontou quatro dimensões das sociedades do conhecimento: liberdade de expressão e liberdade de informação, acesso universal à informação e ao conhecimento, educação de qualidade para todos e respeito à diversidade linguística e cultural (UNESCO, 2005).

A diversidade e as capacidades de incentivar o compartilhamento do conhecimento do qual essas sociedades deveriam se beneficiar, a partir das TICs, tangenciam os direitos de gênero em ambiente digital que acabaram por propiciar uma

[2] Advogada, publicitária e doutoranda em Ciência da Informação do PPGCI-IBICT/UFRJ, viola.carla@gmail.com.

gama de desdobramentos positivos e negativos, dentre os quais, neste último caso, encontramos as violências de gênero na internet.

Sobre violência de gênero, *o Committee on the Elimination of Discrimination against Women* - CEDAW (Comitê sobre a Eliminação da Discriminação contra as Mulheres) pormenoriza as questões a serem observadas sobre as mulheres na *Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres* (ONU, 1979) e em documentos posteriores, como a "Recomendação Geral nº 19", intitulada "Violência contra as mulheres", que logo no art. 1º conceitua a violência baseada no gênero como uma "forma de discriminação que inibe a capacidade das mulheres de gozarem os direitos e liberdades numa base de igualdade com os homens" (ONU, 1992).

Já a "Recomendação Geral nº 35", intitulada "Violência de gênero contra as mulheres", explica que o conceito de "violência contra as mulheres", presente na "Recomendação Geral nº 19" e em outros instrumentos e documentos internacionais, enfatiza que essa violência é baseada no gênero (ASSOCIAÇÃO DE MULHERES CONTRA A VIOLÊNCIA, 2019).

Portanto, este documento utiliza a expressão "violência de gênero contra as mulheres" como um termo mais preciso, que torna explícitas as causas que se baseiam no gênero e os impactos da violência. Essa expressão fortalece ainda mais a compreensão desta violência como um problema social – ao invés de individual - que exige respostas abrangentes, para além de eventos específicos, agressores individuais e vítimas/sobreviventes.

O Estado brasileiro, que se faz presente na ONU desde 1945, ratificou a *Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres* (ONU, 1979) e, consequentemente, deve atender a todas as suas recomendações, obrigando-se a eliminar a discriminação contra as mulheres no seu território.

Outro documento que influenciou a luta das mulheres por seus direitos contra a violência foi a *Convenção Interamericana para Prevenir, Punir e Erradicar a Violência Contra a Mulher - Convenção de Belém do Pará*. No item 6, do artigo 7°, a

Convenção estabeleceu que “os Estados-partes deviam se empenhar em estabelecer procedimentos jurídicos justos e eficazes para a mulher que tenha sido submetida a violência, que incluam, entre outros, medidas de proteção, um julgamento oportuno e o acesso efetivo a tais procedimentos” (OEA, 1994). Esse documento também foi ratificado pelo governo brasileiro.

Corroborando esse compêndio está a Agenda 2030 das Nações Unidas (NAÇÕES UNIDAS BRASIL, [2015]), que descreve os Objetivos do Desenvolvimento Sustentável (ODS) e suas metas, evidenciando, dentre outras, a preocupação com os direitos das mulheres. Esse documento internacional é um instrumento transdisciplinar global-nacional-local que reúne objetivos interdisciplinares e representa as orientações da ONU para a realização de ações e processos efetivos e de qualidade nos países signatários, promovendo a cooperação internacional.

Os ODS foram fixados em 2015 como um plano de ação para as pessoas, para o planeta e para a prosperidade. Trata-se de uma agenda de ação até 2030, com 17 objetivos e 169 metas construídas sobre o legado dos Objetivos de Desenvolvimento do Milênio (ODM). Os ODS são integrados e indivisíveis, e equilibram as três dimensões do desenvolvimento sustentável – econômica, social e ambiental – fundamentais para a saúde da humanidade e do planeta. Neste sentido, os ODS devem ser entendidos a partir de um olhar interdisciplinar, por serem transversais e interdependentes, e com ações transdisciplinares, por contemplarem ações globais, nacionais e locais.

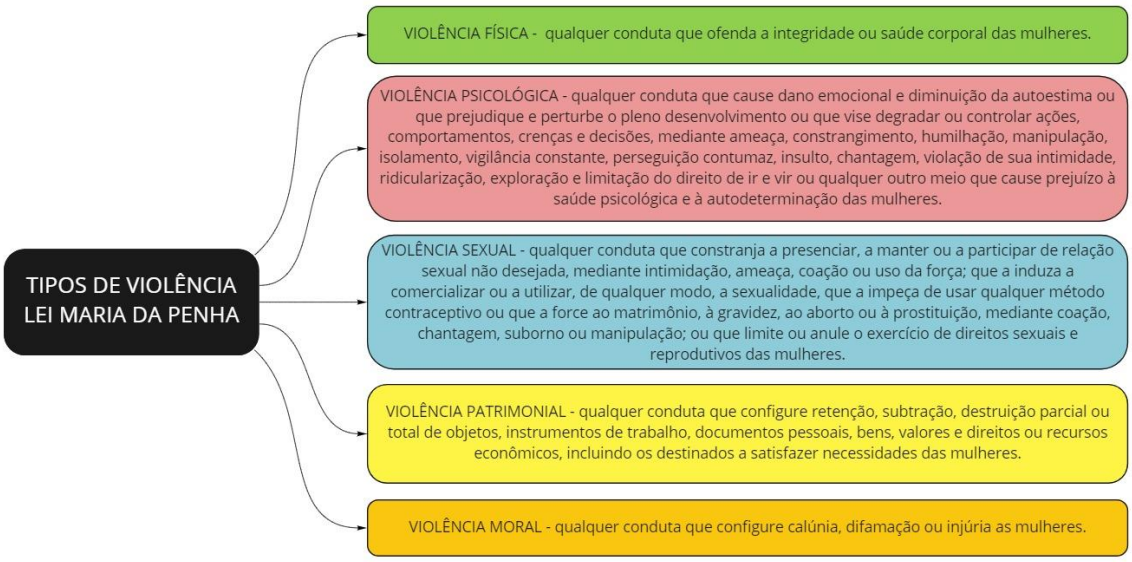
Destaca-se, nesta pesquisa, o Objetivo 5, que descreve a preocupação mundial com as discrepâncias entre homens e mulheres, evidenciando a finalidade de alcançar a igualdade de gênero e de empoderar todas as mulheres e meninas. Essa igualdade não é apenas um direito humano fundamental, mas a base necessária para a construção de um mundo pacífico, próspero e sustentável. O esforço para alcançar o ODS 5 é transversal a toda a Agenda 2030 e reflete a crescente evidência de que o empoderamento de todas as mulheres e meninas tem efeitos multiplicadores no desenvolvimento sustentável.

Luciene Medeiros (2016) explica que a ratificação, pelo Brasil, das normativas integrantes do sistema de proteção internacional influenciou de forma contundente a

legislação do país no que tange à violência contra a mulher, devido à pressão do movimento de mulheres e feministas brasileiras, refletindo na elaboração da Lei Maria da Penha.

A Lei Maria da Penha (BRASIL, 2006) é considerada um marco no combate à violência no Brasil. A lei criou mecanismos para coibir a violência contra as mulheres, nos termos do § 8º do art. 226 da Constituição Federal (BRASIL, 1988). A lei aponta cinco (5) formas de violência: física, psicológica, sexual, patrimonial e moral (Figura 1).

Figura 1 – Tipos de violência, segundo a Lei Maria da Penha



Fonte: Brasil (2006)

Embora a referida lei trate da violência doméstica e familiar contra a mulher, essa normativa teve grande importância para dar visibilidade à necessidade de proteger a mulher contra qualquer tipo de violência, incluindo as que acontecem em ambientes digitais, como a violência psicológica.

Portanto, as violências contra as mulheres na internet não estão descoladas do cotidiano diário do “mundo da vida”. Os espaços virtuais reproduzem as discriminações construídas socialmente e podem ser componentes para reforçar violências contra as mulheres, como a violência sexual, quando, por exemplo, um

estupro é gravado, somada à violência psicológica quando a mulher sofre a ameaça de divulgação do conteúdo, virando chantagem para que não haja denúncia.

A distribuição do conteúdo em ambiente digital acontece em efeito cascata, com grande velocidade, e o alcance da mensagem com a violência atinge as mulheres de forma grave, preocupante, difícil de controlar e de ser revertida. Com isso, novas formas de violência contra as mulheres têm surgido, difundidas pela rede de computadores. Contudo, a legislação nacional já conta com instrumentos normativos e medidas jurídicas para combater crimes cibernéticos que redundam em violência contra as mulheres.

Primeiramente, cite-se a **Lei nº 12.737**, de 30 de novembro de 2012 (BRASIL, 2012), que dispõe sobre a tipificação criminal de delitos informáticos e altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Essa normativa ficou conhecida como “Lei Carolina Dieckmann", em referência e diante de situação específica experimentada pela atriz, em maio de 2012, que teve arquivos copiados de seu computador pessoal - 36 fotos em situação íntima e conversas, que acabaram divulgadas na internet sem autorização.

Na sequência, a **Lei nº 12.965**, de 23 de abril de 2014 (BRASIL, 2014), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Conhecida como “Marco Civil da Internet”, determinou que os provedores de internet devem retirar do ar o material após notificação extrajudicial, sob pena de responder pelos danos causados à vítima.

Alguns anos depois, a **Lei nº 13.642**, de 3 de abril de 2018 (BRASIL, 2018), alterou a Lei nº 10.446, de 8 de maio de 2002, para acrescentar atribuição à Polícia Federal no que concerne à investigação de crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres. Lola Aronovich, professora universitária e blogueira feminista, inspirou a criação desta lei, por ter sido alvo de campanha cibernética difamatória e perseguição física sem que os criminosos tenham sido descobertos (BRASIL, 2018b).

Em seguida, a **Lei nº 13.718**, de 24 de setembro de 2018 (BRASIL, 2018c), alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Essa lei tipifica o crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia como aquele que oferece, troca, disponibiliza, transmite, vende ou expõe à venda, distribui, publica ou divulga, por qualquer meio – inclusive por meio de comunicação de massa ou sistema de informática ou telemática –, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia.

Outra lei do mesmo ano, a **Lei nº 13.772**, de 19 de dezembro de 2018 (BRASIL, 2018d), alterou a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar, e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Essa lei é de grande relevância para o combate à violência contra as mulheres em ambiente digital, reconhece a violência psicológica e a inclui na Lei Maria da Penha. E trata da exposição e do registro não autorizados da intimidade sexual, que são definidos como: produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes.

Além das leis citadas, o Código Civil – Lei nº 10.406, de 10 de janeiro de 2002 (BRASIL, 2002) – permite o enquadramento dos crimes em ambiente digital sob a ótica da responsabilidade civil (danos morais) e o Código Penal – Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (BRASIL, 1940), a tipificação nos crimes contra a honra (injúria, calúnia e difamação).

Por ser um espaço relativamente novo, o mundo virtual ainda causa controvérsias nos tribunais brasileiros e, muitas vezes, a responsabilização pelos crimes pode ser comprometida por lacunas jurídicas ou falta de familiaridade dos operadores de Justiça com o tema.

REFERÊNCIAS

ASSOCIAÇÃO DE MULHERES CONTRA A VIOLÊNCA (AMCV). Comité para a Eliminação da Discriminação contra as Mulheres (CEDAW). **Convenção Sobre a Eliminação de Todas as Formas de Discriminação Contra as Mulheres**. Tradução da Recomendação Geral Nº 35 sobre Violência contra as Mulheres com Base no Género. Atualização da Recomendação Geral Nº 19. Lisboa: AMCV, 2019. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/cedaw_recomendacao_35.pdf. Acesso em: 2 maio 2021.

BRASIL. Câmara dos Deputados. **Desafio é tornar lei conhecida, diz blogueira que inspirou legislação sobre misoginia na internet**. Brasília: Câmara dos Deputados, 2018b. Disponível em: https://www.camara.leg.br/noticias/540214-desafio-e-tornar-lei-conhecida-diz-blogueira-que-inspirou-legislacao-sobre-misoginia-na-internet/. Acesso em: 2 maio 2021.

BRASIL. **[Constituição (1988)].** Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 2 maio 2021.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 2 maio 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 2 maio 2021.

BRASIL. **Lei nº 11.340, de 7 de agosto de 2006**. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher, nos termos do § 8º do art. 226 da Constituição Federal, da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres e da Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher; dispõe sobre a criação dos Juizados de Violência Doméstica e Familiar contra a Mulher; altera o Código de Processo Penal, o Código Penal e a Lei de Execução Penal; e dá outras providências. Brasília: Presidência da República, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 2 maio 2021.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 2 maio 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 maio 2021.

BRASIL. **Lei nº 13.642, de 3 de abril de 2018.** Altera a Lei nº 10.446, de 8 de maio de 2002, para acrescentar atribuição à Polícia Federal no que concerne à investigação de crimes praticados por meio da rede mundial de computadores que difundam conteúdo misógino, definidos como aqueles que propagam o ódio ou a aversão às mulheres. Brasília: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13642.htm. Acesso em: 2 maio 2021.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro, tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelecer causas de aumento de pena para esses crimes e definir como causas de aumento de pena o estupro coletivo e o estupro corretivo; e revoga dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Brasília: Presidência da República, 2018c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm. Acesso em: 2 maio 2021.

BRASIL. **Lei nº 13.772, de 19 de dezembro de 2018**. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Brasília: Presidência da República, 2018d. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm. Acesso em: 2 maio 2021.

MEDEIROS, Luciene. **Em Briga de Marido e Mulher, o Estado Deve Meter a Colher**: políticas públicas de enfrentamento à violência doméstica. Rio de Janeiro: Ed. PUC-Rio; São Paulo: Reflexões, 2016.

NAÇÕES UNIDAS BRASIL. **Sobre o nosso trabalho para alcançar os Objetivos de Desenvolvimento Sustentável no Brasil**. [2015]. Disponível em: https://brasil.un.org/pt-br/sdgs. Acesso em: 2 maio 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Comitê para a Eliminação da Discriminação contra as Mulheres. **Recomendação Geral nº 19**: Violência contra as mulheres, 1992. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/rec_geral_19_violencia_contra_as_mulheres.pdf. Acesso em: 2 maio 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres, 1979. Disponível em: https://www.onumulheres.org.br/wp-content/uploads/2013/03/convencao_cedaw.pdf. Acesso em: 2 maio 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Comissão Interamericana de Direitos Humanos. **Convenção Interamericana para prevenir, punir e erradicar a violência contra a mulher, Convenção de Belém do Pará**. 1994. Disponível em: http://www.cidh.org/basicos/portugues/m.belem.do.para.htm. Acesso em: 2 maio 2021.

UNESCO. **Relatório Mundial - Rumo às sociedades do conhecimento**, 2005. Disponível em: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/towards-knowledge-societies-unesco-world-report/. Acesso em: 2 maio 2021.