

# LGPD & Compliance empresarial: da premente necessidade de responsabilização objetiva das provedoras de internet pela proteção dos dados digitais à luz do capitalismo humanista

Luciana Sabbatine Neves\*

Theodoro Luís Mallmann de Oliveira\*\*

## Introdução

A pesquisa em apreço tem por foco a questão dos percalços decorrentes das condutas ilícitas perpetradas por meio da rede mundial de computadores (internet), prática estas que estão crescendo vertiginosamente na modernidade, onde estamos vivenciando uma espécie de “Quarta Revolução Industrial”, marcada pela convergência de tecnologias digitais, físicas e biológicas.

Faz-se mister admitir que a Era Digital que entrou em vigor nas últimas décadas, se por um lado tem acarretado uma vasta gama de benefícios para a humanidade, com aumento exponencial dos transportes, comunicações, transações contratuais, prestação de serviços mais eficientes aos consumidores etc., por outro tem dado margem para uma série de ilicitudes cometidas por pessoas mal-intencionadas, valendo-se muitas vezes do anonimato dos perfis virtuais falsos e das invasões de dispositivos eletrônicos alheios, demandando providências por parte não só das autoridades públicas, mas das empresas provedoras de internet responsáveis pela manutenção de sites e domínios digitais.

Tendo esse norte, o presente texto tem por problema de pesquisa a ser respondido o questionamento: em caso de ser juridicamente viável, a responsabilização objetiva das

---

\* Doutoranda em Direito econômico pela Universidade Nove de Julho; Mestre em Direitos Humanos pela Pontifícia Universidade Católica de São Paulo; Membro acadêmico do ICAPH – Instituto do Capitalista Humanista; Pesquisadora do Instituto ETHIKAI; Advogada.

E-mail: luneves@yahoo.com.br

\*\* Pós-graduado em Direito Tributário pela Universidade Federal do Rio Grande do Sul (UFRGS). Pós-graduado em Direito Processual Civil (Anhanguera). Especialista em Direito do Trabalho e Processual do Trabalho (UNOPAR). Especialista em Direito Previdenciário (Centro Dom Alberto). Servidor público do Ministério da Justiça (PRF).

E-mail: supertheodoro@gmail.com

empresas provedoras de sites e domínios na internet contribuiria para uma eficiente diminuição dos casos de violação de dados de seus usuários?

A partir do problema de pesquisa retromencionado, a hipótese que se apresenta refere que a previsão normativa de responsabilidade objetiva das provedoras de sites e domínios no mundo virtual será juridicamente possível tão-somente a nível cível, mas não na esfera criminal, contudo certamente contribuiria sobremaneira para a redução da impunidade e das violações de dados digitais.

Sobrevoado esse patamar, destaque-se ainda a inadiável necessidade das empresas fornecedoras de serviços digitais adotarem os princípios do Capitalismo Humanista, enquanto dimensão econômica do princípio da Fraternidade, visando não somente o lucro e usura a qualquer custo, mas harmonizando-se com uma responsabilidade social, sob a ótica de que os programas de *compliance* corporativo são a maneira mais salutar de se alcançar esse objetivo.

Sendo assim, o trabalho vem subdividido em três tópicos, debatendo, no primeiro deles, acerca das implicações cíveis decorrentes das condutas violadoras de dados pessoais digitais. No segundo capítulo, serão abordadas as consequências penais dessas condutas, sempre na perspectiva da interdisciplinaridade. O tomo final trata da viabilidade jurídica da responsabilização objetiva das empresas fornecedoras de serviços de internet onde ocorrem os ilícitos cibernéticos. Em epílogo, serão explanadas nossas conclusões acerca do tema, sempre havendo uma preocupação constante com a clareza e um compromisso sincero com a objetividade.

## Das consequências civis da inobservância da proteção de dados cibernéticos

Se por um lado a globalização e a disseminação da rede mundial de computadores através da crescente tecnologia de novos dispositivos eletrônicos de comunicação (smartphones, computadores e *tablets*) favoreceu o aumento e velocidade dos mecanismos de interação, por outro lado abriu margem para o surgimento de uma série condutas delituosas ocorridas no espaço virtual, a exemplo dos crimes contra a honra, pornografia infantil, pedofilia, furtos de dados e valores, crimes contra a propriedade intelectual, espionagem industrial, sabotagem, estelionatos e outras fraudes diversas. Nesse diapasão, frise-se a necessidade que a ciência do Direito possui em acompanhar essa evolução, normatizando situações advindas das relações cibernéticas.

Nesse ínterim, com a globalização da sociedade moderna, impulsionando os meios de comunicação por conta do aumento exponencial da tecnologia em todos as searas,

surgiu a necessidade de se regulamentar os limites e a acessibilidade a esses novos aparatos, no que tange ao chamado “mundo digital”. Mazzuoli (2019) explica, assim, a gênese dos direitos humanos de quarta geração, ligados também ao direito à informação, buscando a expansão dessas normas em todos os âmbitos de convivência.

Existe um certo limbo conceitual acerca da precisa dimensão em que tais direitos digitais se enquadrariam nos Direitos Humanos. Afirma Bobbio (2004, p. 96), tratarem-se de direitos de quarta geração, na medida que entramos em uma época pós-moderna em que o progresso irreversível acarretou uma evolução tecnológica e tecnocrática global, propiciando um novo naipe de direitos que se surgiram após as três gerações predecessoras.

Nada obstante, nos tempos ainda mais modernos, há quem posicione os direitos virtuais na quinta geração, a exemplo do ilustre Ministro do STJ Reynaldo Soares Fonseca, para o qual seriam os “[...] direitos oriundos da realidade virtual [...] como propagação e desenvolvimento do direito eletrônico na atualidade. Envolve, assim, [...] rompimento das fronteiras físicas por meio da internet” (FONSECA, 2021, p. 125).

Nessa perspectiva, pode-se definir ilícitos virtuais como condutas realizadas preponderantemente através de computadores, celulares, *tablets* e outros aparelhos com tecnologia análoga, com intuito de causar prejuízo, normalmente pela utilização da internet, seja rede pública, seja rede privada, gerando danos a uma ou grande quantidade de vítimas, que chegam às vezes a ser incalculáveis. Tais comportamentos ilícitos virtuais afetam a segurança orgânica cibernética, que tem como elementos a confidencialidade, integridade e disponibilidade (ROSSINI, 2004).

Nessa análise, a expansão meteórica do mundo cibernético traçou uma estrada sem volta, onde são inventadas novas formas de comunicação (redes sociais), negócios jurídicos (contratos, acordos, reuniões virtuais), que necessitam ser perfunctoriamente regulamentados para que indivíduos de má-fé não se valham da internet como forma de mascarar condutas ilícitas, criando uma preocupante “terra virtual sem lei” dominada por hackers e crackers<sup>1</sup>.

Nesse cenário, os ordenamentos jurídicos brasileiro e internacional vêm estabelecendo uma série de instrumentos tecnológicos com o objetivo de coibir condutas cibernéticas ilícitas e resguardar os direitos fundamentais, como o que

---

<sup>1</sup> Enquanto o termo *hacker* se refere aos detentores de altos conhecimentos acerca de redes digitais, *softwares* e programação, descobrindo e alertando sobre possíveis falhas nos sistemas, o *cracker* é o especialista em informática que utiliza os dados e conhecimentos a que tem acesso para o lado negativo, utilizando a quebra da segurança virtual com motivações criminosas. Portanto, o que diferencia os dois é justamente o *animus/dolo* específico do agente (COSTA, 2020).

ocorre, conforme ensina Avanci (2009), no caso das assinaturas digitais, criptografia, funções unidirecionais de *hash* e outros instrumentos previstos na Infraestrutura de Chaves Públicas no Brasil (ICP - Brasil)<sup>2</sup>.

Acompanhando essa tendência, a Norma Ápice brasileira de 1988, através da Emenda Constitucional No 115 de 2022, acrescentou ao Art. 5º o inciso LXXIX, elevando a proteção de dados pessoais, incluindo os relativos ao mundo virtual, à categoria de direito fundamental do cidadão. *In verbis*:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Uma hipérbole de novidades legislativas acerca do Direito Digital foi confirmada pela promulgação da Lei de Acesso à Informação (Lei 12.527/2011), que estipulou procedimentos a serem seguidos por órgãos públicos e entidades provadas que recebam recursos públicos, para o acesso a informações de interesse público aos interessados (sem exclusão dos sítios oficiais na rede mundial de computadores), em atenção aos princípios da publicidade, controle e transparência da Administração.

De grande destaque foi também o chamado Marco Civil da Internet (Lei nº 12.965/2014), que norteou princípios, garantias e deveres para as interações virtuais, tachando outrossim o acesso à internet como direito humano do cidadão, apto para o desenvolvimento da personalidade e da cidadania (art. 2º).

Esse discurso derridiano é reforçado pela criação da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018, com o escopo de reger o uso, proteção e transferência de dados pessoais, quer em âmbito público, quer privado. seja em território nacional, seja internacional, representando um divisor de águas no resguardo, não somente aos direitos humanos, mas também aos direitos fundamentais<sup>3</sup> como privacidade, intimidade, liberdade e dignidade da pessoa humana, entre outros.

---

<sup>2</sup> Cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão nos mais variados documentos, buscando inclusive credenciar, descredenciar, supervisionar e realizar auditorias.

<sup>3</sup> Ramos (2020, p. 74) leciona que a terminologia “direitos fundamentais” refere-se aos direitos humanos a nível nacional, melhor dizendo, aos direitos reconhecidos nas Constituições e leis internas do país,

Nessa tônica, quando ocorre o desrespeito aos dados pessoais de um cidadão contidos no mundo virtual, ocorrerá um ato ilícito típico do art. 186 do Código Civil brasileiro, gerando necessidade de reparação tanto por danos materiais (vinculados aos prejuízos econômicos do ofendido), quanto morais (ligados à honra da vítima). Tais danos, podem ser reparados com base na chamada responsabilidade extracontratual (aquiliana), pois é fundamentada não em um instrumento contratual, mas no referido ato ilícito ou no uso abusivo de um direito (TARTUCE, 2020).

Ainda segundo aponta Tartuce (2020), essa responsabilidade civil extracontratual é via de regra subjetiva apresentando quatro requisitos: 1<sup>a</sup>) comportamento humano: pode ser uma ação ou omissão (conduta positiva ou negativa, respectivamente); 2<sup>a</sup>) culpa lato sensu, dividida em dolo (intenção do agente) e em culpa stricto sensu, subdividida, por sua vez em: a) imprudência: falta de cuidado + ação; b) negligência: falta de cuidado + omissão; c) imperícia: falta de qualificação técnica; 3<sup>a</sup>) dano, o qual pode ser material (prejuízo econômico) e/ou moral (afetando a honra da vítima); 4<sup>a</sup>) nexos de causalidade entre a conduta e o dano.

Frise-se, contudo, que a questão da garantia de proteção de dados virtuais no Brasil está longe de ser trivial. Embora na teoria a proteção a nível de direito material pareça ser completa, na prática processual há grande dificuldade em se identificar os responsáveis pelas condutas ilícitas de desrespeito aos dados pessoais, bem como em comprovar a conduta dolosa ou culposa prevista na responsabilidade aquiliana, mesmo porque muitos deles se valem do anonimato da internet e residem até mesmo em outros países, passando-se pelo perfil virtual de outras pessoas ou criando os chamados “perfis fake<sup>4</sup>”. O cerne da questão, portanto, vem justamente na prova processual deste dolo/culpa, pois às vezes sequer há viabilidade em se descobrir quem praticou a conduta.

O resultado em muitos casos acaba sendo a impunidade, fazendo muitas pessoas sequer registrarem as ocorrências nas delegacias ou, mesmo após o registro, muitas desistem de cobrar os danos, face a uma série de prováveis fatores, como custos do processo (muitas vezes dependendo de carta precatória/rogatória<sup>5</sup>, pois o agressor reside em outra localidade), dificuldade em identificar o ofensor (que se vale do

---

representando uma forte aproximação entre o Direito Internacional e os Ordenamentos Jurídicos internos.

<sup>4</sup> Criação de contas privadas na rede mundial de computadores (internet) contendo dados pessoais (nome, profissão, endereço etc.) fictícios ou de outras pessoas verdadeiras, em não raras ocasiões com o intuito de praticar ilícitos virtuais.

<sup>5</sup> Artigos 260 a 268 do Código de processo Civil.

anonimato), falta de capacitação em Direito Digital dos policiais investigadores, aparato tecnológico reduzido nas delegacias.

Mergulhando nesse raciocínio, jogar-se-á ao vazio as normas suso analisadas se não houver também a exigência, ainda que indireta, de que as empresas provedoras de sítios na internet não se coadunem com as normas do chamado capitalismo humanista, que não visa somente o lucro desenfreado a qualquer custo, mas uma responsabilidade social e respeito aos direitos humanos, inclusive o da proteção de dados pessoais, traduzindo uma ideia de ressignificação do sistema econômico em vigor, segundo a concepção de que a supracitada exclusão socioeconômica implica também em negar aos cidadãos o acesso aos direitos humanos e fundamentais, os quais também gozam de dimensão econômica (SAYEG; NEVES; SAYEG, 2020).

## Da violação de dados virtuais e suas implicações penais

Além das consequências na área cível, os comportamentos ilícitos de violação de violação de dados digitais obviamente acarretam responsabilização penal, considerando que se tratam de instâncias via de regra independentes. Uma que é costumeiramente verificada é a da criação dos já citados perfis falsos na internet (com dados pessoais verdadeiros de outras pessoas ou fictícios), subsumindo-se à norma do art. 307 do Código Penal, que prevê como crime a atribuição de falsa identidade para obtenção de vantagem ou causar dano.

Mesmo que o perfil falso não tenha o desígnio de auferir lucro, há ainda a possibilidade conduta de falsidade ideológica, pois quando o indivíduo preenche virtualmente documentos públicos ou particulares na internet (ex: sites bancários) com informações falsas (ex: registro de identidade, foto, CPF) estará cometendo o delito do art. 299 do CP<sup>6</sup>.

Em grande parte das circunstâncias a violação dos dados pessoais das vítimas ocorre através da invasão de seus aparelhos eletrônicos com acesso à internet (celulares, computadores, *tablets*, etc.), o que, por si só, também a infração penal do art. 154-A do CP: invasão de dispositivo informático.

---

<sup>6</sup> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:  
Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, de quinhentos mil réis a cinco contos de réis, se o documento é particular

Esses falsos perfis, não raras vezes, são utilizados com a finalidade de aplicar os chamados “golpes do pix”, por meio dos quais o meliante descobre os dados pessoais da vítima (foto, nome, número de telefone) e cria uma conta em aplicativos de mensagens (whatsapp, facebook, etc.), fazendo-se passar por esta, solicitando dinheiro emprestado para vários de seus contatos via transferência bancária, aproveitando-se da boa-fé dos conhecidos da vítima, o que configura também o delito de estelionato (art. 171 do CP), por auferir vantagem indevida induzindo o erro das vítimas.

Perfis falsos são utilizados também para a prática do estelionato em sites de relacionamento, onde o golpista se faz passar por outra pessoa (utilizando fotos de terceiros sem estes terem ciência) e busca relacionamento amoroso virtual com as vítimas (alegando que residem em outros países), que, após terem a confiança conquistada e serem movidas pela paixão e ingenuidade, transferem quantias vultuosas para os amantes virtuais, na esperança de conhecê-los pessoalmente, custeando supostos problemas financeiros do consorte. Os chamados “estelionatos sentimentais” aumentaram bastante em face do isolamento social decorrente da pandemia COVID19 (BRENOL, 2021).

O uso de contas virtuais falsas também pode ter por escopo a prática da pedofilia, quando o agressor busca se relacionar virtualmente com menores de idade, solicitando vídeos e fotos íntimas para satisfazer sua lascívia pelo armazenamento desses arquivos e se faz passar por outra pessoa para evitar ser identificado pelas autoridades, numa clara configuração do crime do art. 241-A do Estatuto da Criança e do Adolescente (Lei n. 8.069/1990).

Destaque-se ainda para as hipóteses de sequestro de dados digitais (*ransomware*), pelos quais os *crackers*, valendo-se de aplicativos maliciosos, obtêm acesso aos arquivos cibernéticos de indivíduos e corporações, exigindo valores monetários para devolvê-los, numa clara situação de crime de extorsão, nos ditames do art. 158 do CP.

Outra prática comumente dos golpistas que se enquadra no estelionato é o uso de perfis falsos com todos e nomes de outras pessoas (sem estas terem ciência) para alugar ou vender bens pela internet (ex: imóveis, veículos etc.) pedindo adiantamento dos valores como sinal para concluir o negócio, sem que os compradores/locadores tenham contato físico com o criminoso, acabando por não receberem os bens que compraram/alugaram e perdendo os valores que adiantaram. Infelizmente, o inverso também ocorre, quando golpistas furtam dados pessoais usando o espaço virtual e realizam compras e empréstimos vultuosos se passando pelas vítimas (MIGALHAS, 2020).

Há ainda a possibilidade de utilização de perfis profissionais na internet com a utilização de dados verdadeiros de outros especialistas em determinada área (advogados, médicos, corretores, engenheiros etc.), com vistas a angariar clientes. Muitas vezes os golpistas sequer possuem habilitação profissional e registro no conselho de classe para exercer a profissão, o que pode configurar infração penal do art. 282 do Código Penal (para médicos, farmacêuticos e dentistas) ou do art. 47 da Lei das Contravenções Penais.

Perfis *fakes* contribuem também para a proliferação dos crimes contra a honra, previstos no Capítulo V da Parte Especial do Código Penal: i) calúnia, que é imputar a alguém falsamente um crime, ferindo sua honra objetiva (art. 138); ii) difamação, pela imputação de fato desonroso à reputação da vítima, independentemente de ser verdadeiro ou não (art. 139); iii) injúria, que é a atribuição de qualidade negativa à vítima, ofendendo sua honra subjetiva (dignidade e decoro) - art. 140. Importante frisar que muitas dessas injúrias nas redes sociais possuem conotação racista (injúria qualificada pelo preconceito (art. 140, §3º do CP), motivo pelo qual vêm sendo equiparadas aos crimes de racismo do art. 20 da Lei 7.716/89 na condição de imprescritíveis, conforme o magistério do penalista Rogério Sanches Cunha<sup>7</sup>:

O STJ, julgando recurso de agravo regimental no recurso especial nº 86.965/DF, considerou que a injúria racial está na seara dos crimes relativos ao racismo e é imprescritível, pois tem sentido de segregação, somando-se às definições da Lei nº 7.716/89, que não traz um rol taxativo (CUNHA, 2016, p. 425).

Há ainda a possibilidade de difusão pelas redes sociais mediante perfis falsos de nefastas ideias fazendo apologia a crimes ou a criminosos, configurando crime do art. 287 do CP, o que pode ocorrer muitas vezes em função de fanatismos políticos, religiosos, futebolísticos, dentre outros.

Dito isto, a criação dos perfis falsos também pode se direcionar para a disseminação das *fake news*: notícias de conteúdo intencionalmente falso com o objetivo de ganhar mais visibilidade através de um sensacionalismo apelativo e sórdido com exacerbado potencial para denegrir a imagem das pessoas ou fazer apologia a crimes e criminosos, utilizadas com perigosas intenções por ofensores com tendências

---

<sup>7</sup> “**Lei 7.716/89**: Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

Pena: reclusão de um a três anos e multa.”

**Constituição Federal**: “Art. 5º (...) XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;”

racistas, misóginas, homofóbicas, nazifascistas, mesmo porque, quanto mais disseminadas forem, mais dificultosa se torna a possibilidade de desmenti-las. E o mais pernicioso: fazendo-se passar por outras pessoas, que têm seus dados pessoais violados (BARROS; OLIVEIRA, 2021).

## Da responsabilização objetiva dos provedores de internet pela proteção de dados

Conforme sobredito, o desrespeito aos dados pessoais dos cidadãos através da rede mundial de computadores (*word wide web*) é suscetível de uma série de consequências jurídicas tanto na seara civil como criminal, todavia, conquanto na teoria do direito material seja relativamente fácil caracterizar o enquadramento das condutas, na prática do direito processual ainda tem sido bastante dificultosa a punição dessas infrações.

Acompanhando esse dissabor, dessume-se que as vítimas de violação de dados pessoais no âmbito virtual encontram-se na qualidade de consumidoras<sup>8</sup> desses serviços de internet, sendo, portanto, partes hipossuficientes, muitas vezes sequer dispondo de conhecimentos avançados de informática para se proteger dos ataques cibernéticos, ao passo que os *hackers* e *crackers* aperfeiçoam cada vez mais seus mecanismos para fazer novas vítimas e garantir o anonimato (OLIVEIRA; DANI, 2011).

Já as empresas provedoras de sites e domínios na internet estão em manifesta condição de superioridade em relação aos consumidores vítimas da violação, pois muitas daquelas se coadunam na definição de *big techs*: corporações multinacionais que dominam o mercado da tecnologia, em uma espécie de oligopólio que às vezes impede até que empresas concorrentes surjam (CORRÊA, 2019).

*Data vênia*, resta público e notório que os usuários desses serviços digitais que têm seus dados violados estão em manifesta desvantagem na relação consumerista, portanto deveria haver uma expressa previsão legislativa de que as provedoras, na

---

<sup>8</sup> Dispõe o Código de Defesa do Consumidor em seu art. 2º: “Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou **serviço como destinatário final**. Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo.

Art. 3º Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.”

qualidade de fornecedoras de serviço ao consumidor, possuam responsabilidade objetiva pelos danos causados.

Na vereda do Direito Penal, é incabível a responsabilização objetiva por duas razões: a) pelo princípio da culpabilidade, só responderá por um crime quem o houver causado de forma dolosa ou, ao menos, culposamente (princípio *do nulla poena sine culpa*; b) é terminantemente proscrita a responsabilização penal (ainda que subjetiva) de pessoas jurídicas no Direito Penal brasileiro, à exceção dos atos lesivos ao meio ambiente (GRECO, 2017).

Porém, com relação aos danos materiais e morais no âmbito civil, entendemos plenamente possível a possibilidade da responsabilidade objetiva das provedoras de internet, mesmo porque, conforme Garcia (2016), elas deverão seguir certos princípios do direito consumerista, tais como vulnerabilidade e hipossuficiência do consumidor, controle da qualidade e segurança dos serviços e compatibilização da proteção do consumidor com o desenvolvimento tecnológico. Acrescente-se, ainda, a possibilidade de desconsideração da pessoa jurídica prevista no art. 28 do Código de Defesa do Consumidor (CDC) nos casos em que essa personalidade representar um obstáculo ao ressarcimento dos danos aos consumidores internautas.

A LGPD, em seu art. 42, prevê de forma expressa que, em havendo violação de dados pessoais, ocorrerá responsabilização civil solidária entre controlador (pessoa jurídica que decide quais dados serão tratados) e operador (empresa que processa os dados), possibilitando ainda a inversão do ônus da prova (§2º). Mas o grande dilema deste diploma é que não traz com clareza se essa responsabilidade será subjetiva ou objetiva, o que nos leva a crer que ela poderia ser alterada para melhor clareza.

Nesse acalorado debate, não se pode olvidar ainda da dúvida se, em caso de criação de contas virtuais a título gratuito nessas provedoras de sites e domínios, haveria de fato relação de consumo, posto que o art. 3º, §2º do CDC prevê expressamente que deve haver remuneração pelo serviço objeto do consumo. Boa parte da doutrina, assim como a Terceira Turma do STJ, através do Recurso Especial n. 1308830 RS 2011/0257434-5, entendem que ainda assim haverá vínculo consumerista em face do chamado lucro indireto: estas provedoras auferem vantagens com veiculação de propaganda de outras empresas, para as quais venderam espaço (também denominado *cross marketing*). Todavia, a questão ainda não está pacificada nem na doutrina nem na jurisprudência, o que nos leva a conceber que a melhor solução seria essa previsão de responsabilidade objetiva estar expressamente prevista na LGPD, ainda que não se configurasse relação de consumo (SABATOVSKI, 2012).

Salvo melhor juízo, a previsão dessa responsabilidade objetiva deveria se dar de forma expressa a nível internacional, visto que a proteção de dados pessoais conferida pelos arts. 7º e 8º da Carta dos Direitos Fundamentais da União Europeia, além de não prever essa modalidade de responsabilidade, mostra-se antiga (promulgada no ano 2000).

Dessa forma, fica óbvio que violações de dados pessoais ferem uma série de Direitos humanos das vítimas como honra (ofendendo a reputação e imagem) dignidade humana (propalação da misoginia, LGBTfobia, racismo, xenofobia etc.), patrimônio (estelionato, furto), privacidade, intimidade, dentre outros. Proteger valores desse quilate pela responsabilização objetiva das provedoras de sites e domínios é uma inequívoca expressão do princípio da Fraternidade. Fonseca e Rossetto (2019) concebem que a Fraternidade é a mola mestra que confere o equilíbrio entre todas as dimensões de direitos humanos, incluindo as relações no ciberespaço.

A Fraternidade mostra-se o arauto axiomático da evolução do capitalismo liberal para um Capitalismo humanista nas empresas fornecedoras dos serviços virtuais. Um capitalismo que supera a busca gananciosa do lucro e usura, visa também o bem-estar nas relações econômicas, sendo um fator de transformação para a direção do Humanismo – o Fator CapH, constituindo-se na Dimensão econômica dos Direitos Humanos (SAYEG; BALERA, 2019).

Reiteramos mais uma vez a necessidade da adoção dos programas de *compliance* por essas empresas provedoras, no sentido de cumprir rigorosamente a legislação (inclusive as normas de Direito do Consumidor, Direito Penal, Direito Civil etc.), respeitando os princípios éticos e os direitos humanos dos cidadãos, além de garantir a sustentabilidade, respeito e valorização da imagem das empresas que seguem os seus comandos.

## Considerações finais

Analisadas as premissas abordadas ao longo deste artigo, a pesquisa constatou que, com o advento da Era Digital, houve um meteórico crescimento da quantidade e velocidade nas comunicações a nível global, abrindo um grande leque para a ação de meliantes na violação de dados pessoais cibernéticos dos cidadãos, incidindo em ilícitos penais e civis de toda sorte.

Verificou-se ainda a dificuldade nas vítimas de violação desses dados em combater tais ilegalidades, seja pelo anonimato dos *crackers* e *hackers*, seja pelas dificuldades de acioná-lo judicialmente (pois muitas vezes reside em outras localidades), seja ainda pela

carência de conhecimentos informáticos das vítimas, que se encontram numa clara posição de hipossuficiência.

Com o advento da chamada “tecnologia 5G”, amplificando a facilidade dessas relações digitais, a tendência será o crescimento desses “golpes da internet”, daí porque o Direito deve evoluir para acompanhar essas mudanças fáticas, no sentido de responsabilizar de forma objetiva as empresas responsáveis por espaços virtuais, mormente por conta de muitas vezes se tratarem de megacorporações de elevado vulto, em contraposição à manifesta vulnerabilidade dos internautas consumidores. Tal responsabilização contribuiria sobremaneira para uma maior eficiência no cadastro prévio e identificação de *hackers* e *crackers*, reduzindo as ilegalidades no espaço cibernético.

Concluiu-se, que, conquanto não seja possível uma alteração da LGPD para conferir responsabilidade objetiva a nível penal das provedoras de serviços de internet, tal responsabilização poderá ocorrer a nível cível, especialmente em se tratando de relação consumerista, o que é defendido pela maioria da doutrina e Jurisprudência, ainda que não haja remuneração direta pelo serviço digital.

No Brasil impera um deplorável Estado de Coisas Inconstitucional, onde há grave e sistemática violação de direitos fundamentais dos cidadãos em virtude das falhas nas políticas dos Poderes Públicos. Faz-se, portanto, imprescindível a adoção de providências no sentido de aprovar a nível legislativo responsabilização objetiva dessas empresas, bem como dotar as polícias, procuradorias de justiça e Poder Judiciário de aparato logístico e de recursos humanos suficientes para prevenir e punir essas violações.

A chave para uma verdadeira ressignificação na cultura interna das corporações que fornecem os serviços digitais perpassa inexoravelmente pelo seguimento dos princípios do Capitalismo Humanista e adoção das políticas de *compliance* institucional, fazendo valer as suas ações sempre em consonância com os Direitos Humanos em busca de uma sociedade digital fraterna.

## Referências

AVANCI, Thiago Felipe S. Direitos fundamentais: aspectos estruturais. **Revista Jus Navigandi**, Teresina, ano 14, n. 2159, maio 2009. Disponível em: <<https://jus.com.br/artigos/12838>>. Acesso em: 8 out. 2021.

BARROS, Laura Mendes Amando de; OLIVEIRA, Gustavo Justino de. Fake news, liberdade de expressão e moderação nas redes sociais: tendências. **Conjur**, 17 out. 2021. Disponível em: <<https://www.conjur.com.br/2021-out-17/publico-pragmatico-fake-news-liberdade-expressao-moderacao-redes-sociais-tendencias>>. Acesso em: 13 mar. 2022.

Direitos Humanos, Fraternidade e Justiça Social na Sociedade em Rede

LGPD & Compliance empresarial: da premente necessidade de responsabilização objetiva das provedoras de internet pela proteção dos dados digitais à luz do capitalismo humanista

DOI: 10.23899/9786589284284.11

BOBBIO, Norberto. **A era dos direitos**. Tradução de Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.

BRENOL, Lise. Scammers: como identificar golpistas em sites de namoro. **SERASA**, 2021. Disponível em: <<https://www.serasa.com.br/premium/blog/scammers-como-identificar-golpistas-em-sites-de-namoro>>. Acesso em: 13 mar. 2022.

CORRÊA, Leonardo. Privacidade de dados ou compartilhamento forçado: como lidar com as big techs? **Conjur**, 27 jul. 2019. Disponível em: <<https://www.conjur.com.br/2019-jul-27/leonardo-correa-liar-big-techs-concorrencialmente>> Acesso em: 14 mar. 2022.

COSTA, Michael Nathaniel da. O Ataque Cracker Para se Apropriar de Informações Digitais: Uma Análise Jurídica do Estelionato Digital. **Revista Âmbito Jurídico**, Rio de Janeiro, jul. 2020. Disponível em: <<https://ambitojuridico.com.br/cadernos/direito-penal/o-ataque-cracker-para-se-apropriar-de-informacoes-digitais-uma-analise-juridica-do-estelionato-digital/>>. Acesso em: 10 mar. 2022.

CUNHA, Rogério Sanches. **Código penal para concursos**. 9. ed., Salvador: Juspodivm, 2016.

FONSECA, Reynaldo Soares. Direitos de fraternidade na teoria das gerações de direitos fundamentais. **Revista do Tribunal Regional Federal da 1ª Região**, Brasília, v. 31, n. 1, p. 125, 2021. Disponível em: <<https://revista.trf1.jus.br/trf1/article/view/29/29>>. Acesso em: 29 jan. 2022.

FONSECA, Reynaldo Soares da; ROSSETTO, Geralda Magella de Faria. Dívida fraternal e política compensatória: o dilema da proteção, promoção e defesa dos direitos humanos na civilização tecnológica. In: SOBRINHO, José de Ribamar Froz *et al.* (Org.). **Direitos humanos e fraternidade: estudos em homenagem ao ministro Reynaldo Soares da Fonseca**. v. 2. São Luís: EDUFMA, 2021. p.11.

FRANCO, Isabel. **Guia prático de compliance**. 1. ed. Rio de Janeiro: Forense, 2020.

GARCIA, Leonardo de Medeiros. **Direito do consumidor**. 10. ed. JusPODIVM, 2016.

GRECO, Rogério. **Curso de Direito Penal**. v. 1. 19. ed. Niterói, RJ: Impetus, 2017.

MAZZUOLI, Valerio de Oliveira **Curso de direitos humanos**. 6. ed. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2019.

OLIVEIRA Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. Os crimes virtuais e a impunidade real. **Revista âmbito jurídico**, 01 ago. 2021. Disponível em: <<https://ambitojuridico.com.br/edicoes/revista-91/os-crimes-virtuais-e-a-impunidade-real/>>. Acesso em: 14 mar. 2022.

OLX não é responsável por fraude em locação de imóvel. **Portal Migalhas**, 20 out. 2020. Disponível em: <<https://www.migalhas.com.br/quentes/335731/olx-nao-e-responsavel-por-fraude-em-locacao-de-imovel>>. Acesso em: 13 mar. 2022.

RAMOS, André de Carvalho. **Curso de Direitos Humanos**. 7. ed. São Paulo: Saraiva Educação, 2020.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SABATOVSKI, Emílio. STJ. 3ª T. Internet. Relação de consumo. **LEGJUR**, 16 ago. 2012. Disponível em: <<https://www.legjur.com/noticias/2379/stj-3-t-consumidor-internet-relacao-de->

## Direitos Humanos, Fraternidade e Justiça Social na Sociedade em Rede

*LGPD & Compliance empresarial: da premente necessidade de responsabilização objetiva das provedoras de internet pela proteção dos dados digitais à luz do capitalismo humanista*

DOI: 10.23899/9786589284284.11

consumo#:~:text=Vale%20notar%2C%20por%20oportuno%2C%20que,o%20ganho%20indireto%20do%20fornecedor>. Acesso em: 15 mar. 2022.

SAYEG, Ricardo; NEVES, Luciana Sabbatine; SAYEG, Rodrigo Campos Hasson. Uma análise sobre aspectos do capitalismo humanista a dimensão econômica da sociedade fraterna: pontos em que altera o regime capitalista e sua melhor veiculação para atingir tais finalidades. **Revista Jurídica-UNICURITIBA**, Curitiba, v. 2, n. 59, p. 632-655, 2020.

SAYEG, Ricardo Hasson; BALERA, Wagner. **Capitalismo humanista**: a dimensão econômica dos direitos humanos. São Paulo: Max Limonad, 2019.

TARTUCE, Flávio. **Manual de direito civil**. 10. ed. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020.