

RESPONSABILIDADE CIVIL E PROTEÇÃO DE DADOS PESSOAIS.

Katy S. M. Fernandes¹

Sumário

Dados Pessoais mereceu tratamento em diplomas jurídicos ao nível do direito internacional, a começar pela Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, como marco supranacional, fundamental, de proteção destacados aos dados pessoais. Ao nível internacional, merece destaque o Regulamento Europeu sobre a Proteção de Dados da União Europeia, e a Legislação Português de proteção de dados.

A Proteção de dados pessoais, mereceu a mal alta tutela ao nível nacional, sendo considerado um direito fundamental de todas as pessoas, com consagração constitucional na Magna Carta de 1992. A necessidade de proteção de dados pessoas hoje em dia é um fato incontornável. É necessário. O combate à violação da privacidade, o armazenamento e o suo ilegítimo ou incomensurável de dados pessoais, é o desafio da atual sociedade digital, da informação e da economia de vigilância. Nesse sentido, dados pessoais é considerado um direito autónomo, pois que, dele derivam informação relativa a uma pessoa singular identificada ou identificável, através do qual esta pessoa pode ser identificada, direta ou indiretamente, em particular através de referência a um número de identificação ou a um ou vários fatores específicos à sua identidade física, fisiológica, mental, cultural ou social.

De realçar que a informática sob o ponto de vista jurídico-penal e para aquilo de que se está agora a curar, não é, evidentemente, um fim em si mesma. Por existir ponto de confluência entre a informatização da nossa identidade e da nossa vivência a *pari passu* com a sociedade “real”, porque também o “virtual” é uma extensão de nós mesmos, o legislador nacional sentiu a necessidade de elevar a reserva da vida privada a bem jurídico jurídico-penal, como *ultima ratio*, passando pela responsabilidade civil e pelo contencioso administrativo, na atual sociedade de risco, expressão cunhada por Ulrich Beck.

Palavras-chaves: responsabilidade civil, dados pessoais.

¹ Mestre em Direito pela Faculdade de Direito da Universidade do Minho, Jurista (Cabo-Verde).

Abstrait

Les données personnelles méritaient un traitement dans les diplômes juridiques au niveau du droit international, à commencer par la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, en tant que cadre supranational et fondamental pour la protection des données personnelles. Au niveau international, le Règlement européen sur la protection des données de l'Union européenne et la législation portugaise sur la protection des données méritent d'être soulignés.

La protection des données personnelles, méritait une protection faiblement élevée au niveau national, étant considérée comme un droit fondamental de tous, avec une inscription constitutionnelle dans la Magna Carta de 1992. Le besoin de protection des données personnelles est aujourd'hui un fait inévitable. Il est nécessaire. Lutter contre la violation de la vie privée, le stockage et l'utilisation illégitime ou incommensurable des données personnelles est l'enjeu de la société numérique, de l'économie de l'information et de la surveillance d'aujourd'hui. En ce sens, les données personnelles sont considérées comme un droit autonome, car elles dérivent des informations relatives à une personne physique identifiée ou identifiable, à travers lesquelles cette personne peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs facteurs spécifiques à leur identité physique, physiologique, mentale, culturelle ou sociale.

Réalisez que l'informatique d'un point de vue pénal et juridique et pour ce qu'elle guérit actuellement, n'est évidemment pas une fin en soi. Parce qu'il y a un point de confluence entre l'informatisation de notre identité et notre expérience a pari passu avec une société "réelle", parce qu'aussi ou "virtuelle" est un prolongement de nous-mêmes, le législateur national a besoin d'élever la réserve de la vie privée à patrimoine juridico-pénal, en ultima ratio, à travers la responsabilité civile et le contentieux administratif, dans la société du risque actuelle, expression forgée par Ulrich Beck.

Mots clés : responsabilité civile, données personnelles.

Introdução

Dados Pessoais mereceu tratamento em diplomas jurídicos ao nível do direito internacional, nomeadamente, a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais², o Regulamento Europeu sobre a Proteção de Dados da União Europeia³, e a Legislação Português de proteção de dados pessoais⁴, em 2011 cita-se a Legislação Angolana, a de São Tomé e Príncipe e, mais “*recentemente*”, a Brasileira.

A Proteção de dados pessoais, mereceu a mais alta tutela ao nível nacional, sendo considerado um direito fundamental, com consagração constitucional na Magna Carta de 1992.

A necessidade de proteção de dados pessoais hoje em dia é um fato incontornável. Aquela proteção, vis-à-vis, é necessário, essencial e merecedor de tutela, num mundo altamente conectado, que se guia ao ritmo acelerado do fluxo de informação. O combate à violação da privacidade⁵, o armazenamento e o uso ilegítimo, desmedido e incomensurável de dados pessoais, é o desafio da atual sociedade digital, da informação e da economia de vigilância⁶.

Nesse sentido, dados pessoais são considerados um direito autónomo de personalidade⁷, pois que, dele derivam informações relativas a uma pessoa singular identificada ou identificável, através do qual esta pessoa pode ser identificada, direta ou indiretamente, em particular, através de referência a um número de identificação ou a um ou vários fatores específicos à sua identidade física, fisiológica, mental, cultural ou social”. Inclusive, o endereço de uma pessoa pode ser considerado um dado pessoal, segundo o acórdão do Tribunal da Relação de Lisboa⁸.

²https://www.apd.ao/fotos/frontend_1/editor2/190709_resolucao_33-19_de_9_julho-convencao_ciberseguranca_proteccao_dados.pdf

³ https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&stabela=leis&so_miolo=

⁴<https://dre.pt/legislacao-consolidada/-/lc/74901117/201704032057/diploma/1?rp=indice>

⁵ Nesta que é “**um dos direitos fundamentais que mais glória obtiveram neste último século**”, segundo nota José Faria da Costa – Direito Penal da Comunicação, alguns escritos, Coimbra editora 1998, pág. 127.

⁶ Especificamente, *a monetização dos dados pessoais formatou uma nova economia*. Do ponto de vista de Bruno Bioni, “uma economia que tem como cerne a *vigilância*. É a observação permanente do comportamento dos indivíduos que a movimenta, sendo as suas informações pessoais a matéria-prima a ser explorada para a geração de riqueza. Mais do que isso, há um “varejo dos dados pessoais”. Para a operacionalização desse modelo de negócio, há uma complexa rede de atores que transaciona as informações pessoais dos consumidores, agindo cooperativamente para agregar mais e mais dados e, em última análise, tornar a mensagem publicitária ainda mais eficiente”, in **Proteção de dados pessoais: a função e os limites do consentimento**, editora forense 2019.

⁷ Daí a pertinência a sua circunscrições à autonomia privada, a autodeterminação informacional. Sem prejuízo dos direitos de personalidade indisponíveis.

⁸ “O endereço de alguém é um dado pessoal e pode ser dado a conhecer para prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados” -

Ora, é consensual que, *onde existe o homem, há sociedade; onde existe sociedade, há direito*, disse Ulpiano no *Corpus Iuris Civilis*: “*Ubi homo ibi societas; ubi societas, ibi jus*”, não por acaso, as normas jurídicas, éticas ou morais, ainda que costumeiras ou advindas dos usos sociais, exsurgem para regimentar os comportamentos humanos.

Destarte, “o campo de direito nunca esteve completamente desarmado, ao ponto de ser surpreendido em inapelável contra-pé pela vertiginosa sucessão dos avanços tecnológicos: mesmo aí onde as normas do direito positivo tardem em preencher o espaço aberto por essas conquistas, os princípios jurídicos que entretecem a ordem jurídica asseguram, no próprio plano operacional da busca das soluções, que esse não é – longe disse – um espaço “livre de Direito”⁹, afirma Manuel A. Carneiro da Frada. Segundo o mesmo autor, “não há por conseguinte razão para, diante dele nos desesperarmos numa “angústia do vazio” porventura pressentida”.

Este pequeno estudo objetiva aclarar a matéria da responsabilidade civil ao nível do regime jurídico geral de proteção de dados, no que ao tratamento dos dados pessoais concerne - na legislação Cabo Verdiana, contudo, pela inexistência de subsídios doutrinários no país, iremos analisar as contribuições ao nível do direito comparado em outras ordens jurídicas, como sejam as realidades de Portugal, Brasil, Angola, São Tomé e Príncipe, não sendo um estudo comparado, pretende-se, perceber como interpretar e enquadrar certos conceitos que a legislação traça, numa plano prático, quando há tido lugar a violações de dados pessoais, e descortinar quais as estratégias de *Compliance* como forma de proteção.

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e922d7c5a0ca56aa8025851200533efd?OpenDocument>

⁹ Direito da Sociedade da Informação, Vol. II, Coimbra editora, 2001, pág. 7.

I. Considerações Gerais – Responsabilidade Civil e Dados Pessoais

Ab initio, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados na sinonímia e tenham sido utilizados de maneira intercambiável ao longo deste trabalho. O dado é o estado primitivo da informação, pois não é algo *per se* que acresce conhecimento. Dados são simplesmente *factos brutos* que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação¹⁰.

Toda a emergência de proteção de dados pessoais, deriva do fato de o *dado pessoal* ser considerado “o novo petróleo”, em efeito, uma *commodities* da indústria denominada 4.0, inserida no contexto da Quarta Revolução Industrial. Alguns autores preconizam que tecnologias como *big data*, Internet das Coisas (*IoT*), Inteligência Artificial (*AI*), *Blockchain*, entre outras, *geram o ganho em eficiência e escala de determinada atividade econômica devido à operação denominada tratamento de dados pessoais*¹¹.

O uso e a propagação de dados pessoais hoje é emergente, essencialmente também, como diz Fernando Antonio Tasso, porque,

*“hoje, diferentemente do que ocorria há duas décadas, as pessoas não mais “entram” na internet, porquanto já estão absolutamente imersas no ambiente virtual. Perfis fantasma, existentes no ambiente das plataformas digitais de redes sociais; o monitoramento de atividade e do próprio sono do usuário por meio de dispositivos vestíveis, como smart watches ou smart bands, ou portáteis, como smartphones ou tablets, são tecnologias que ancoram a existência humana no ambiente virtual, ainda que sem sua ciência ou de acordo com sua plena concordância. Nesse contexto, em que é impossível se desconectar de modo absoluto da rede mundial de computadores, a internet, normas reguladoras em todo o globo têm a pretensão de traçar regras que, ao invés de inibirem ou vedarem o tratamento de dados pessoais, buscam permitir um adequado fluxo informacional, preservada a autodeterminação informativa, que foi consagrada como um dos fundamentos da Lei Geral de Proteção de Dados, ao lado do respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem*¹².

¹⁰ Fernando Antonio Tasso, A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor - Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020, pág. 97 e seguintes.

¹¹ Fernando Antonio Tasso, A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor - Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020, pág. 97 e seguintes.

¹² Op. Cit.

A autodeterminação informativa ou informacional é um direito do titular de dados e se baseia no pressuposto de que, a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informação» (Gomes Canotilho/Vital Moreira)¹³.

Os direitos assegurados aos titulares de dados pessoais, funcionam como verdadeiros mecanismo de empoderamento dos mesmos, configuradas em extratos normativos que elevam o próprio titular dos dados pessoais como o seu grande protagonista. Esse *empowerment* descortina-se *de principio*, pela própria ideia do que seja um tratamento de dados pessoais, adjetivado de justo e lícito, quando vinculada ao consentimento do indivíduo (a jusante ou a montante).

Para Fernando Antonio Tasso, o caráter autónomo do direito à proteção de dados “advém da constatação de que novas situações de fato ensejam proteção legal, por decorrerem do puro e simples tratamento de dados pessoais, como o perfilhamento racial, as listas negras de trabalhadores que ingressam na *Justiça Obreira* contra seus patrões, testes genéticos pré-admissionais e identificações biométricas em gravações de vídeo de espaços públicos”. Enfatiza o mesmo, que “tais fatos, isoladamente considerados, não violam a honra, intimidade ou vida privada”. Mas, se, “no contexto do tratamento e utilização massiva de dados pessoais, passam a ser geradores de novos valores passíveis de garantia legal, uma vez que repercutem em direitos e garantias fundamentais como a igualdade, do livre exercício profissional, da dignidade da pessoa humana e da liberdade de reunião e locomoção”¹⁴.

No entendimento de autor acima citado, é mister que se estude a responsabilidade pelo potencial latente, porém, potente, dos dados pessoais porque, neste novo contexto, existem desafios tanto nos relacionamentos interpessoais como na relação pessoa-máquina sem precedentes que instigam a doutrina e a própria jurisprudência, a tratar dessa nova espécie de “risco”¹⁵. Além dos dados, segundo Fernando Antonio Tasso, “a responsabilidade civil tem por desafios novas relações jurídicas decorrentes de novas espécies contratuais, como contratos de transporte celebrados por intermédio de plataformas digitais, ou prestados por veículos autônomos, contratos de transporte de coisas por *drones* e contratos coligados de serviços

¹³<http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/c3ca422fd42da4ba80257de0003469cf?OpenDocument>

¹⁴ Op. Cit.

¹⁵ “A tecnologia não é boa ; não má, mas também não é neutra” (adaptado), Melvim krnazberg.

prestados pela Internet, assim como de novas condutas como espionagem industrial realizada por *softwares* invasores”¹⁶.

Para Fernando Antonio Tasso “o embate doutrinário é travado entre posições que afirmam ter a lei estabelecido um sistema baseado na responsabilidade objetiva ou subjetiva”¹⁷. Sendo portanto, em palavras,

“cediço ser todo o sistema de responsabilidade civil na Lei Geral de Proteção de Dados intrinsecamente vinculado ao elemento culpa. De tal sorte, a adoção como regra do sistema

¹⁶ Para efeitos de determinação de responsabilidade, adianta que o artigo 42.º “caput” da Lei Geral de Proteção de Dados prevê o dever de reparação civil por dano patrimonial, moral, individual ou coletivo, imposto aos agentes de tratamento, controlador ou operador, quando executarem operação de tratamento de dados em violação à legislação de proteção de dados. Sobressai de sua leitura que, se por um lado não prevê o elemento culpa, por outro não o exclui expressamente. Ainda, traz como requisito da obrigação de reparar a circunstância de ter sido a operação de tratamento lesiva realizada em violação à legislação de proteção de dados. É legítimo concluir, que são utilizados apenas dois critérios objetivos para fundamentar a responsabilidade, quais sejam, o exercício da atividade de tratamento de dados e a violação da legislação de proteção de dados- A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor - Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020, pág. 97 e seguintes.

¹⁷ Em todas as situações jurídicas em que o legislador excecionou a regra da responsabilidade subjetiva no direito privado, o fez de modo expresso e inequívoco, a exemplo do emprego da expressão “independentemente da existência de culpa” nos artigos 12.º e 14.º do Código de Defesa do Consumidor ou singelamente se referindo à obrigação de reparar o dano “independentemente de culpa”, como na cláusula geral do artigo 927.º, parágrafo único do Código Civil. Não há na Lei Geral de Proteção de Dados qualquer artigo que se valha da expressão “independentemente de culpa” ou “independentemente da existência de culpa”, a indicar de modo inequívoco que o regime jurídico adotado fora o da responsabilidade objetiva. Outro argumento eloquente a indicar a escolha da regra da responsabilidade subjetiva consiste no fato de que a Lei é pródiga na imposição de uma série de deveres de ação e de abstenção aos agentes de tratamento. Esses deveres estão presentes em todos os segmentos da lei e vão desde a observância cumulativa e incondicional de todos os princípios de proteção de dados; a disponibilização de forma clara, adequada e ostensiva das características do tratamento de dados; a publicitação acerca dos tipos de dados coletados; a abstenção de coleta de dados desnecessários, a disponibilização de informações claras no tratamento de dados de crianças e adolescentes; a manutenção de dados em formato interoperável e estruturado; a comunicação de convênios de uso compartilhados de dados à Autoridade Nacional; a divulgação ostensiva da identidade e das informações de contato do encarregado; a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito desde a concepção do produto ou serviço (*privacy by design*)⁶⁸; passando pela adoção das melhores práticas de segurança da informação⁶⁹; pelo dever de comunicação de incidente à Autoridade Nacional e ao titular dos dados; e, finalmente, pela publicação das regras e boas práticas de governança. À evidência, tais regras não consistem em meras recomendações tendentes a evitar incidentes de segurança. Antes, o legislador estabeleceu um *standard* de conduta e cobra o cumprimento desses deveres. O tratamento regular de dados consiste em uma obrigação de resultado e não de meio. Assim sendo, caso o sistema de responsabilidade civil fosse da modalidade objetiva, a prescrição exaustiva e detalhada dos deveres seria algo absolutamente inócuo, sobretudo porque redundaria na conclusão de que de nada adiantaria o cumprimento dos deveres se, qualquer que fosse o incidente, a responsabilidade pela reparação estivesse configurada, o que é um contrassenso. Op. Cit.

de responsabilidade civil objetiva resultaria em autêntico desincentivo à observância dos deveres específicos de proteção, prevenção e segurança impostos aos agentes de tratamento, desprestigiando, igualmente, a ideia de um adequado fluxo informacional como solução para uma economia global baseada em dados. Com a evolução tecnológica e o impacto nas relações pessoais e negociais, a concepção tradicional da reparação que pressupunha a existência de culpa passou a não mais atender ao reclamo social pela proteção da vítima, dando ensejo ao desenvolvimento da teoria do risco. A interpretação dialógica entre as fontes deve ser feita com cautela, na medida em que não se pode admitir como risco toda e qualquer situação, sob pena de banalização do instituto”.

O direito da proteção de dados, fruto da digitalização da sociedade, das vivências e das práticas sociais, não ficam de fora, como bem o disse Joel Timóteo Ramos Pereira, “qualquer prática individual ou coletiva, qualquer prestação de bens ou serviços que se realize no ambiente da internet não fica de fora da alçada do direito, designadamente a responsabilidade civil”¹⁸. Quando as soluções penais, contraordenacionais, administrativas, não se adequem ou não couberem ou não forem passíveis de serem aplicados a determinado resultado típico, ilícito ou ilegítimo, cedem, cabendo espaço ao regime de responsabilidade civil, pelo risco ou extracontratual.

Fora do âmbito das casos vedados por lei, o tratamento de dados pessoais ou pessoalíssimos, só pode ser efetuado, se o seu titular tiver prestado de forma inequívoca, o seu consentimento ou, quando for necessário para as situações que a própria legislação de proteção de dados prevê, *infra* especificados.

Do tratamento de dados pessoais resultam certos direitos para o seu titular, como sejam, o direito à informação, o direito de acesso aos dados objeto de tratamento, o direito de oposição (nomeadamente em se tratando de *marketing* direto), esses direitos devem ser assegurados dentro de um prazo razoável, sob pena da intempestividade.

A breve trecho, importa analisar o tratamento dos dados pessoais na nossa Carta Magna, a Constituição de 1992 (ou CRCV) mais precisamente, dentro do *status* de direito fundamental, segundo os termos exarados do artigo 45.º.

De acordo com a clássica divisão dos direitos fundamentais em gerações, a primeira geração apontando para a ideia de liberdade negativa clássica; a segunda geração, a de direitos sociais e económicos (ou de igualdade), exigia, a partir do século XX, que o Estado interviesse de modo a assegurar as garantias individuais, especialmente em relação à educação, saúde, alimentação,

¹⁸ Compêndio Jurídico da Sociedade da Informação, notas Práticas, legislações, jurisprudências, *Quid Juris* -2004, Pag. 869.

trabalho, moradia, lazer, segurança etc., marcado profundamente pela ideia do Estado do bem estar social. A terceira geração, consolidada após a Segunda Guerra Mundial, fortaleceu a importância de direitos transindividuais, direcionados à globalização, intrinsecamente ligados aos valores de fraternidade e solidariedade. São voltados ao desenvolvimento, à paz, ao meio ambiente, ao direito de propriedade sobre o patrimônio comum da humanidade e ao direito de comunicação.

Conforme o preconizado por Rafael de Freitas Valle Dresch e Lílian Brandt Stein, “a consolidação da era da informação, convida a uma importante reflexão acerca da imprescindibilidade de se resguardar os dados pessoais, seja frente ao Estado, seja em relação a outros particulares”¹⁹.

A quarta geração dos direitos fundamentais, segundos os autores citados, tem a sua origem, nos direitos ligados à democracia, à informação e ao pluralismo. Identificam justamente nesse cenário, a emergência da contemporânea sociedade globalizada, extremamente dependente e condicionada pelo fluxo sem precedentes da informação. A informação se quer dinâmica e volátil, e é nesta instância, que nos parece repousar o direito fundamental à proteção de dados pessoais.

A ser assim, a proteção de dados pessoais²⁰ se afigura como um direito fundamental autônomo. Ela não se restringe unicamente a salvaguardar a privacidade²¹ e a intimidade, questões que também é-lhe inerente, tendo em conta o caráter personalísticos ou pessoalíssimos daqueles direitos.

Dentro das panóplas dos desafios regulatórios presente na atual esfera social, e dentro de uma economia cada vez mais movidas por dados, os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjatividade), mas, configura-se como prerrogativa essencial e

¹⁹ Direito Fundamental à proteção de dados e Responsabilidade Civil, *in*

<https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

²⁰ Exemplos de Dados pessoais, como atributos particulares de cada indivíduo, podem ser, seu nome, tipo sanguíneo, número de telefone, endereço de e-mail, características físicas e informações biométricas. À essa lista se somam as ações (compras, pesquisas, publicações, reações, comentários) praticadas diariamente em buscadores, lojas *online* e redes virtuais acabam, que também acabam por muito dizer sobre um indivíduo – inclusive em sua ausência.” Direito Fundamental à proteção de dados e Responsabilidade Civil, *in* <https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

²¹ *Vide*, Bruno Bioni, in Proteção de Dados Pessoais - A Função e os Limites do Consentimento (2019), **em sua perspectiva**, “Seria contraproducente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade. O eixo da privacidade está ligado ao controle de informações pessoais do que seja algo íntimo ou privado do sujeito. A proteção dos dados pessoais não se satisfaz com tal técnica normativa, uma vez que a informação pode estar sob a esfera pública, discutindo-se, apenas, a sua exatidão, por exemplo. Pág. 99 e 100.

instrumental para que a pessoa possa livremente desenvolver a sua personalidade. Desse modo, esclarece Bruno Bioni, “a tutela jurídica dos dados pessoais configura um imperativo que impõe uma nova fronteira aos direitos da personalidade, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana, e por tabela, ao livre desenvolvimento de sua personalidade. Por isso, o direito à proteção dos dados pessoais reclama uma normatização própria que não pode ser reduzida a uma mera “evolução” do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação”. Ao fim e ao cabo, trata-se da nossa própria capacidade de autodeterminação²².

Vendo a responsabilidade civil, sob o prisma dos operadores dos serviços de telecomunicações, é preciso esclarecer quem são os referenciados. Para Manuel A. Carneiro da Frada, operadoras de serviços de telecomunicações “são aquelas entidades que, intervindo de forma autónoma, permanente e organizada no circuito informático, prestam, normalmente com escopo lucrativo, serviço, na, ou através, da rede eletrónica”²³. Ressalva, todavia, que tendencialmente, os “cibernautas” não se limitam a apenas a serem meros destinatários dos serviços das operadoras, pois que, assumindo uma conduta ativa, passam a intervir na difusão de informações e ideias ou participando em fóruns de discussão. Assim, esse “amadorismo e o caráter eventual e esporádico que caracterizam a sua conduta não os eximem de toda a responsabilidade, pois estão seguramente adstritos a deveres genéricos de comportamento (*on line*).²⁴

Na linha do preceituado no Decreto-lei n.º 5/94 de 7 de Fevereiro, operadores dos serviços de comunicação, são os organismos ou entidades públicas ou privadas, que efetuem o transporte ou a transmissão de mensagens ou informações pelos meios técnicos adequados. Sendo que, de harmonia com a natureza das comunicações os operadores respetivos podem ser dos tipos seguintes: a) Operadores de serviços de correios ou de serviços postais; b) Operadores de telecomunicações. E, por outra banca, em função da natureza dos utilizadores das comunicações, os operadores respetivos podem ser dos tipos seguintes: a) Operadores de comunicações públicas; b) Operadores de comunicações privadas (artigo 5.º).

Porém, é pertinente ressaltar, que existem atos próprios que são levadas a cabo apenas pelas ditas operadoras, evidentemente no exercício das sua atividade ou como profissionais do ramo da atividade, assumem, contratualmente certas e determinadas obrigações e, por inerência, a correlacionada responsabilidade, que advém da prática dos seus próprias atos. Nada obstante, é

²² Op. Cit. Pág. 123.

²³ Direito da Sociedade da Informação, Vol. II, Coimbra editora, 2001, pág. 10.

²⁴ Direito da Sociedade da Informação, Vol. II, Coimbra editora, 2001, pág. 11.

preciso saber quando e sob que condições alguém está vinculado a ressarcir um dano sofrido por outrem²⁵. Esse questionamento está intrinsecamente ligada aos pressupostos e as circunstâncias que justifiquem a que uma operadora, por exemplo, seja obrigada a indenizar um prejuízo causado ou dano alheio.

Estamos ante a clássica figura de responsabilidade civil. No que à matéria de proteção de dados diz respeito, teremos de ver se se trata de uma responsabilidade civil contratual ou aquiliana²⁶. O divisor de águas entre as duas tipologias de responsabilidade, reside no fato de a responsabilidade civil obrigacional existir sempre que haja a violação de uma obrigação assumida de um lado e a proteção configura a outra parte da mesma prestação obrigacional, que conduz à obrigação de indenizar. E, por seu turno, a responsabilidade aquiliana requer a evidência de uma situação fática ilícita e exige que o ato seja culposos.

No Brasil, segundo Rafael de Freitas Valle Dresch e Lílian Brandt Stein, remontando às origens do direito à privacidade, do famoso artigo *The right to privacy*, de Samuel D. Warren e Louis D. Brandeis²⁷, entendem os mesmos que é nítido que “a necessidade de tutela dos dados

²⁵ Direito da Sociedade da Informação, Vol. II, Coimbra editora, 2001, pág. 12.

²⁶ A culpa aquiliana tem sua origem no Direito Romano especificamente na Lex Aquilia – “um reconhecido marco legislativo se deu com o advento da “Lex Aquilia”, que trouxe a responsabilidade aquiliana substituindo a multa fixa por uma pena proporcional ao dano causado. Tal Lei representou um divisor de águas para o estudo da responsabilidade civil, tratando da responsabilidade extracontratual, cujo conceito se funda na inexistência de contrato, observando-se regras referentes a direitos reais ou pessoais, sem existência de prévio vínculo, bastando haver a violação de um dever expresso em norma Legal, que cause dano. Como exemplo, podemos citar o dever de indenizar que surge a partir de um acidente de trânsito. A princípio, a “Lex Aquilia” foi uma legislação de uso bem restrito, tendo alcançado importante dimensão no governo de Justiniano, e, outrossim, atingido a hodierna concepção de responsabilidade extracontratual, porquanto considerava o ato ilícito algo autônomo, independente de contrato obrigacional preexistente”(vide <https://carneirocunha.adv.br/artigos/>).

²⁷ “The right to privacy does not prohibit any publication of matter which is of public or general interest. In determining the scope of this rule, aid would be afforded by the analogy, in the law of libel and slander, of cases which deal with the qualified privilege of comment and criticism on matters of public and general interest. There are of course difficulties in applying such a rule; but they are inherent in the subject-matter, and are certainly no greater than those which exist in many other branches of the law, -- for instance, in that large class of cases in which the reasonableness or unreasonableness of an act is made the test of liability. The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented. The distinction, however, noted in the above statement is obvious and fundamental. There are persons who may reasonably claim as a right, protection from the notoriety entailed by being made the victims of journalistic enterprise. There are others who, in varying degrees, have renounced the right to live their lives screened from public observation. Matters which men of the first class may justly contend, concern themselves alone, may in those of the second be the subject of legitimate interest to their fellow-citizens. Peculiarities of manner and person, which in the ordinary individual should be free from comment,

personais vai muito além – especialmente ante disposição do art.º 5º, inciso XII da Constituição Federal, que assegura a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, para referir expressamente a necessidade de tutela do direito fundamental autônomo à proteção de dados pessoais”²⁸.

No Direito Brasileiro, em sede da responsabilidade pela violação das normas de proteção de dados, parte da doutrina defende a hipótese de se tratar da responsabilidade subjetiva, o que segundo essa corrente doutrinária, reclamaria a análise da culpa dos agentes ou responsáveis pelo tratamento, em casos de danos aos titulares de dados pessoais; outra fração doutrinária defende que a Lei Geral de Proteção de Dados do Brasil – LGPD²⁹ apontaria para a responsabilidade objetiva, baseada na teoria do risco; e, uma terceira corrente, posiciona-se favoravelmente a uma responsabilidade objetiva especial. Ou seja, aquela em que,

“se enquadra em uma categoria especial de responsabilidade objetiva, que se dará ante o cometimento de um ilícito: o não cumprimento de deveres impostos pela legislação de proteção de dados, em especial o dever de segurança por parte do agente de tratamento. Esse é o entendimento extraído da análise do dever geral de segurança do qual esse se incumbe, nos termos do art.º 46.º, e cuja violação acaba por ensejar sua responsabilização civil, conforme disposição do art.º 44.º da LGPD.”

Para Rafael de Freitas Valle Dresch e Lílian Brandt Stein,

“o essencial à responsabilização civil dos agentes de tratamento, portanto, é a existência de um ilícito. Contudo, o ilícito previsto nos artigos 42.º e 44.º d LGPD não está centrado na culpa do agente, como ocorre no artigo 186.º do Código Civil Brasileiro, mas no ilícito objetivo, pois não se indaga sobre dolo ou culpa em sentido estrito. Não há a necessidade da análise subjetiva – interna ao sujeito – com base na sua intenção ou falta de cuidado, caracterizada pela negligência, imprudência ou imperícia. O ilícito objetivo previsto na LGPD, assim como o

may acquire a public importance, if found in a candidate for public office. Some further discrimination is necessary, therefore, than to class facts or deeds as public or private according to a standard to be applied to the fact or deed per se. To publish of a modest and retiring individual that he suffers from an impediment in his speech or that he cannot spell correctly, is an unwarranted, if not an unexampled, infringement of his rights, while to state and comment on the same characteristics found in a would-be congressman could not be regarded as beyond the pale of propriety”. https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

²⁸ Direito Fundamental à proteção de dados e Responsabilidade Civil, *in*

<https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

²⁹ Lei Nº 13.709, de 14 de agosto de 2018. (http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)

do artigo 187.º do Código Civil, demanda apenas a análise externa das práticas do agente de tratamento, de sua conduta de forma objetiva, para verificar se tal conduta está em conformidade (compliance) ou não com o padrão de conduta exigível a um agente de tratamento com base em standards técnicos de mercado e regulatórios.³⁰

Nas palavras de Dov Seidman (2011, p. 99, 100)³¹

“nas sociedades democráticas, consultamos as regras – na forma de leis – na busca da necessária certeza, consistência e previsibilidade. Na época do capitalismo protecionista, demos-nos muito bem criando regras, mas chegando ao final do século, começamos a nos decepcionar com elas. Existem boas razões para isso. Por um lado, o modo como criamos as regras muitas vezes as tornam ineficazes quando regidas pela conduta humana. As regras, naturalmente, não surgem do nada. O legislativo e as organizações as adotam geralmente para proibir comportamentos indesejados, mas tipicamente como reação diante de fatos. Elas estabelecem a redução nos limites de velocidade depois de acidentes automobilísticos demasiadamente frequentes, proibem a criação de pit bulls depois de uma série de ataques de cães dessa raça, ou instituem novos procedimentos de controle de gastos depois de alguém ser pego tentando um reembolso pela compra de um novo iPod. As regras são estabelecidas por uma razão, mas a maioria das pessoas desconhece o raciocínio e o espírito da motivação. Elas não lêem a história do legislativo e assim mantêm uma relação fraca e superficial com as regras. Isso, dado o conjunto adequado de circunstâncias, faz as pessoas explorarem formas de escapar delas, encontrarem brechas. Steve Adams, por exemplo, funcionário do correio e nativo do Alasca, queria expressar sua individualidade, aparecendo para trabalhar usando uma gravata com a imagem dos Três Patetas e de personagens do Looney Tunes. Essa atitude não repercutia bem diante dos chefes, que durante meses brigou com ele até finalmente obrigá-lo a seguir as regras especificando o tipo de gravata permitido. Ele obedeceu. Depois, ele examinou todas as regras e descobriu que não havia proibição específica sobre o uso de suspensórios. Agora, ele veste com orgulho suspensórios com desenho do Taz, o diabo da Tasmânia. As regras são falhas porque é impossível elaborá-las contendo todo comportamento possível do vasto espectro da conduta humana. Sempre

³⁰ Direito Fundamental à proteção de dados e Responsabilidade Civil, in <https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protacao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

³¹ Como. Por que o Como Fazer Algo Significa Tudo, 2011.

existirão áreas nebulosas, e, assim, dadas as circunstâncias, oportunidades ou pressões externas corretas, algumas pessoas podem ser motivadas a burlá-las. Quando elas agem assim, a reação típica é simplesmente criar mais regras. As regras, assim, acabam virando parte do problema. As regras atingem bons patamares, padrões mínimos de comportamento, e evitam a ocorrência de fatos desagradáveis – se as pessoas as cumprirem”.

Com isso, fica claro o entendimento de Freitas Valle Dresch e Lílian Brandt Stein quando opinam que, “há que se notar que não seria viável estabelecer todos os riscos do tratamento de dados – porque, junto à incessante evolução tecnológica, novos questionamentos e demandas hão de surgir. É daí que se faz tão relevante estimular que os agentes de tratamento busquem as melhores práticas, ainda que essas não tenham, até o momento, sido pormenorizadamente identificadas. Nesse sentido, a garantia da segurança não deve partir tão somente da lei, mas também do agir voluntário dos próprios agentes”³².

Sendo falhos, os sistemas e, sobre a insuficiência natural das regras, os autores citados concluem que ,

“seria demasiado pretensioso esperar – sobretudo considerando os constantes e irrefreáveis avanços tecnológicos – que inexistissem, ainda que adotadas as mais seguras medidas, falhas ou violações em razão do tratamento de dados. Tampouco seria coerente confiar que a legislação pudesse se ocupar de apontar expressamente tudo o que pode e deve ser feito pelo agente nesse sentido. Isso posto, cabe à norma e, mais ainda, à interpretação conferida à norma, atuar como uma ferramenta capaz de estimular as melhores práticas, assegurando-se que, sob o ponto de vista da ponderação entre custos e benefícios, a esses agentes seja interessante fazê-lo. De outro lado, sendo a responsabilização afastada caso o agente tenha realizado tudo que estava ao seu alcance para proteger os dados e tutelar os direitos que a LGPD busca resguardar, notórios são os incentivos para que as referidas medidas sejam adotadas, pois protegeriam, ao final, não apenas os dados, mas também o agente. Sendo aplicada uma responsabilização indiscriminada de todos os agentes apenas pelos risco da atividade ou pelo risco proveito, com base na premissa, por exemplo, do cheapest cost avoider, se estaria a desincentivar a adoção de medidas efetivas de proteção

³² Direito Fundamental à proteção de dados e Responsabilidade Civil, in <https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protacao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

de dados pelos agentes de tratamento e reduzindo o nível de proteção ao direito fundamental à proteção de dados pessoais”³³.

Concluem, que “ao se adotar a teoria objetiva especial centrada no ilícito objetivo, dispensa-se, para fins de responsabilização civil, a análise da culpa, de um lado; também se afasta a responsabilidade tão somente a partir da teoria do risco, de outro. O critério de imputação pelo risco (seja risco proveito, da atividade ou integral), em especial, trata indistintamente “bons e maus” agentes – e, nesse caso, pela ausência de distinção, acaba por não incentivar comportamentos cooperativos de proteção de dados da pessoa humana e incentivar comportamentos estratégicos omissivos em relação à segurança.”³⁴

Segundo Liliana Minardi Paesani, “quem pratica um ato, ou incorre numa omissão de que resulte dano, deve suportar as consequências do seu procedimento. Trata-se de uma regra elementar de equilíbrio social, na qual se resume, em verdade, o problema da responsabilidade. Vê-se, portanto, que responsabilidade é um fenómeno social”³⁵.

Para a autora em análise, podemos concluir que “o ato ilícito não é o único fato gerador da responsabilidade civil”. Para a mesma, o verdadeiro elemento constitutivo é a ação geradora do dano, sendo esse o elemento essencial ao ordenamento civil para que seja cabível a imputação do resultado ao agente, daí que, para tanto, interessa apenas o ressarcimento desse dano.

Defende Liliana Minardi Paesani que o instituto da responsabilidade civil integra o direito das obrigações e acarreta a obrigação de reparar o dano ocasionado, independentemente de culpa ou dolo. Para ela, essa obrigação é de natureza pessoal e resolve-se em perdas e danos conforme dispõe o atual Código Civil no art.º 389.º – “não cumprida a obrigação, responde o devedor por perdas e danos[...]”.

Um dos pressupostos da responsabilidade civil principais, é a existência de *nexo causal* ou liame causal, entre o ato e o dano por ele produzido. Para o que, sem essa relação de causalidade, não se admite a obrigação de indenizar.

³³ Direito Fundamental à proteção de dados e Responsabilidade Civil, *in* <https://revistadireitorresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

³⁴ Direito Fundamental à proteção de dados e Responsabilidade Civil, *in* <https://revistadireitorresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

³⁵ Direito e Internet (Liberdade de Informação, Privacidade e Responsabilidade Civil), 6ª ed. Atlas, 2013 (e-ISBN 978-85-224-7892- 7), páginas 59 e seguintes

Ainda no direito brasileiro, as fontes das obrigações previstas no Código Civil são: a lei, a vontade humana (contratos e declarações unilaterais da vontade) e os atos ilícitos. O art.º 927.º inclui o dever de indenizar entre as obrigações. E, portanto, quem comete ato ilícito tem a obrigação de indenizar. Responsabilidade subjetiva ou aquiliana baseada na culpa do agente da Ação, culpa esta ainda que, *in lege Aquilia et levíssima culpa venit*, ou seja, ainda que levíssima, obriga a indenizar³⁶.

Por sua vez, a responsabilidade pelo risco, surge associado à industrialização e a multiplicação da atividade das máquinas, que intensificaram o aumento de acidentes e motivaram uma nova análise da responsabilidade civil (*teoria do risco*) e a doutrina e a jurisprudência passaram a fornecer novos subsídios para a solução dos incontáveis litígios submetidos a apreciação do Judiciário.

Nada obstante, a generalização global da responsabilidade civil pela reparação de um dano, ainda que a culpa seja levíssima, O Código de Napoleão desenvolveu a noção de culpa *in abstracto* e distinguiu a culpa delitual da culpa contratual que inspirou a redação dos arts.º 1.382.º e 1.383.º do diploma legal francês. A partir daí, a responsabilidade civil fundada na consciência de que o dano ou prejuízo, que acarreta a responsabilidade, não é apenas o material. Para tanto, segundo esse pressuposto, o Direito, não deve deixar sem proteção as vítimas de ofensas morais, preconiza Liliana Minardi Paesani³⁷.

O direito pátrio consagra a responsabilidade civil no artigo 483.º do código civil (CC). Segundo se dispõe no n.º 1, aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação. A responsabilidade existe ainda, como obrigação de indemnizar independentemente de culpa nos casos especificados na lei (nº 2).

Quanto à responsabilidade pelo risco, segundo se denota do artigo 499.º do CC são extensivas aos casos de responsabilidade pelo risco, na parte aplicável e na falta de preceitos legais em contrário, as disposições que regulam a responsabilidade por factos ilícitos.

No entendimento de Orides Mezzaroba e Fernando Galindo,

³⁶ Direito e Internet (Liberdade de Informação, Privacidade e Responsabilidade Civil), 6ª ed. Atlas, 2013 (e-ISBN 978-85-224-7892-7), páginas 59 e seguintes.

³⁷ Direito e Internet (Liberdade de Informação, Privacidade e Responsabilidade Civil), 6ª ed. Atlas, 2013 (e-ISBN 978-85-224-7892-7), páginas 59 e seguintes.

“Com o passar dos tempos a tecnologia se tornou fator preponderante no processo de produção e transformação da própria humanidade, diminuindo os perigos e aumentando os riscos. O perigo, portanto, é o risco que a cada dia se realiza e materializa na atualidade. Os riscos decorrentes do processo evolutivo são intrínsecos, eles são proporcionais a maior ou menor dependência material e psicológica do homem em relação as suas criações (máquinas). O inverso dessa lógica, ou seja, máquinas inteligentes dependendo, nos mesmos termos, do homem não parece ser hoje uma ideia tão absurda. Pelo menos essa hipótese já é devidamente considerada pela indústria cinematográfica, restando a dúvida de até onde a máquina pode ir sem depender do homem. Certamente, as máquinas não substituirão o homem, mas o envolverão completamente, dando-lhe mais poder sobre a natureza e a sociedade. Mais real é a preocupação com processos que somente as máquinas podem realizar ou cujo controle humano é precário. O risco da falta de controle estará sempre presente. A palavra chave nessas situações de risco está na responsabilidade. Este é o antídoto sobre qualquer risco que se torne um perigo. Quem é quem entre os agentes que em diversos níveis são responsáveis pelas consequências de atos ou omissões realizadas? Definir este cenário parece mais inteligente e com certeza é uma tarefa regulatória de difícil realização, haja vista que, bem ou mal, a responsabilidade das decisões recai cada vez mais sobre os sistemas e as pessoas não se sentem mais repensáveis por elas. Não há ninguém para culpar se algo não funcionar: culpa-se o sistema. É o sistema que não funciona. Afinal, que sistema é esse? Onde está o sistema?”⁶⁸

Ao fim e ao cabo, a questão fundamental, consiste em saber a quem atribuir a eventual responsabilidade por um eventual dano. Sendo de fundamental importância que, quanto à proteção aos direitos da personalidade, a o *ciberespaço* não pode ser considerada um espaço anárquico, sem regras, onde não existem sanções para os arrogantes e tutela para os fracos. Porém, elucidam Orides Mezzaroba e Fernando Galindo³⁹, é todo o contrário, pelo que se constata, pela “natureza global da *internet*, o mesmo comportamento ilícito pode ser tutelado, regulamentado ou sancionado por vários ordenamentos jurídicos com igual aplicabilidade e submetidos a jurisdição de mais juízes igualmente competentes. Parece que alcançamos não urna

³⁸ DEMOCRACIA eletrônica, Orides Mezzaroba e Fernando Galindo (eds.). — Zaragoza : Prensas Universitárias de Zaragoza, 2010, Página 20, 21. (LEFIS Series ; 11).

³⁹ DEMOCRACIA eletrônica, Orides Mezzaroba e Fernando Galindo (eds.). — Zaragoza : Prensas Universitárias de Zaragoza, 2010, Página 20, 21. (LEFIS Series ; 11).

carência, mas, ao contrário, um excesso de normas”. Surge, portanto, o problema de individualizar a lei aplicável e o juiz competente.

Entende-se que, configurada a situação acima, de conflito de normas ou de competência, toma-se necessária a adequação do conflito às práticas de autorregulamentação e coregulamentação, para os serviços Internet – isto é, surge a alternativa necessária do sistema da Arbitragem Virtual. Para os autores últimos citados, “a Arbitragem Virtual será composta por urna Corte, definida pelas duas partes, com especialistas no assunto, que vão julgar o caso sem jamais se encontrarem. A grande diferença da Corte de Arbitragem Virtual vai estar na seleção de qualquer país como foro competente, e o *acordo* será assinado como se tudo tivesse acontecido lá, embora nenhuma das partes tenha fisicamente pisado no local”⁴⁰.

Para Patrícia Peck Pinheiro (2013, p. 262)⁴¹ “a responsabilidade civil é um fenômeno social”, sendo que um de seus principais pressupostos é a existência de nexos causal entre o ato e o dano por ele produzido. Para a mesma, mais importante que o ato ilícito que causou o dano, é o fato de que esse dano deve ser ressarcido.

Assinala que, “o Direito Digital, por sua necessidade de dinamismo, introduz algumas modificações dos conceitos tradicionais de responsabilidade civil no âmbito jurídico”, imprimindo novas roupagens ao mesmo conceito. Porém, há que recorrer ao conceito clássico da responsabilidade civil e a sua divisão e posteriormente adaptar a nova realidade. Segundo a mesma, se para o direito tradicional, “o conceito de responsabilidade civil adota duas teorias: a teoria da culpa e a teoria do risco. A principal diferença entre elas está na obrigatoriedade ou não da presença da culpa, mesmo que levíssima, para caracterizar a responsabilidade e o dever de indenizar”. Assina-la que, especificamente, no Direito Digital, “a teoria do risco tem maior aplicabilidade, uma vez que, nascida na era da industrialização, vem resolver os problemas de reparação do dano em que a culpa é um elemento dispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações, em virtude do princípio de equilíbrio de interesses e genérica equidade”⁴².

Justifica-se a incidência da responsabilidade pelo risco, porque, segundo Patrícia Peck, “a internet, que é mídia e veículo de comunicação, seu potencial de danos indiretos é muito maior que de danos diretos, e a possibilidade de causar prejuízo a outrem, mesmo que sem culpa, é

⁴⁰ DEMOCRACIA eletrônica, Orides Mezzaroba e Fernando Galindo (eds.). — Zaragoza : Prensas Universitárias de Zaragoza, 2010, Página 20, 21. (LEFIS Series ; 11).

⁴¹ Direito digital — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 — São Paulo : Saraiva, 2013, pág. 262.

⁴² Idem.

real". Para a mesma, no direito digital, "a responsabilidade civil tem relação direta com grau de conhecimento requerido de cada prestador de serviço e do consumidor-usuário também. Nenhuma das partes pode alegar sua própria torpeza para se eximir de culpa concorrente"⁴³. A autora aqui faz alusão ao brocado latino *nemo auditur propriam turpitudinem allegans*.

Outro ponto de assaz importância se prende com a responsabilidade pelo conteúdo. Pois que, segundo o entendimento de uma larga maioria doutrinária, "é o conteúdo que atrai as pessoas para o mundo virtual e que ele deve estar submetido aos valores morais da sociedade e atender aos critérios de veracidade, é importante determinar os limites de responsabilidade dos provedores, dos donos de *websites*, das produtoras de conteúdo, dos usuários de *email* e de todos os que tenham de algum modo participação, seja em sua produção, seja em sua publicação". Para Patrícia Peck, a solução pode residir no "determinar uma norma-padrão pela qual, em princípio, os responsáveis pelo conteúdo publicado em um *website* são seus proprietários ou quem eles indicarem como responsáveis editoriais. Cabem aqui as mesmas normas utilizadas para o conteúdo jornalístico convencional"⁴⁴.

Para tanto, levanta-se a pertinente questão em saber se os mesmos provedores são também responsáveis pelos conteúdos dos quais não tinham prévio conhecimento? Ou, "melhor dizendo, devem os responsáveis por tais provedores responder por atos ilícitos cometidos em seus domínios independentemente de culpa?" Para Patrícia Peck, estes questionamento questões suscitam muitas sérias dúvidas. Para e mesma, "esperar, por exemplo, que a empresa Google monitore todos os vídeos postados em seu sítio eletrônico "YouTube", de maneira prévia, é tarefa hercúlea e humanamente impossível"⁴⁵.

A solução porém, segundo a mesma, pode estar no fato de uma vez, comunicada ao provedor, seja por uma autoridade, seja por um usuário, de que determinado vídeo/texto possui conteúdo eventualmente ofensivo e/ou ilícito, deve tal empresa agir de forma enérgica, retirando-o imediatamente do ar, sob pena de, daí sim, responder de forma solidária juntamente com o seu autor ante a omissão praticada. Solução com a qual concordamos.

Para Patrícia Peck, "o próprio mercado tende a se autorregular no momento em que os *websites* que não tenham responsáveis editoriais percam credibilidade, determinando que serão os consumidores da informação os principais controladores da qualidade do conteúdo que querem aceder e os principais responsáveis por sua denúncia junto às autoridades no caso de qualquer lesão. Quanto ao dano moral, há muitas controvérsias da matéria no próprio mundo real, que dirá

⁴³ Idem.

⁴⁴ Idem.

⁴⁵ Idem, pág. 263.

no mundo virtual. O ideal é a análise caso a caso, considerando que a legislação existente é perfeitamente aplicável, sobretudo se a Internet for entendida como um veículo de comunicação e mídia⁴⁶.

Ainda no entendimento de Patrícia Peck, deve-se atentar, segundo a mesma, para fato de que,

“no ambiente digital, talvez o mais difícil de definir seja o momento exato no qual uma “não conduta”, um “não agir”, gera uma omissão passível de penalidade por negligência. Ou seja, quanto tempo da solicitação de remoção do ar de um determinado conteúdo poderia se considerar que a parte que tem meios técnicos para tanto está sendo relapsa ou mesmo conivente com a situação?”, para a mesma, não chega a haver um padrão de tempo limite para a remoção de conteúdo definido nas decisões judiciais brasileiras para retirada de conteúdo da internet, até pelo tema ser recente. Considerando os provedores de serviço e de hospedagem como “meio” para violação a direitos no meio digital, e tendo em vista a responsabilidade por culpa (especialmente a omissão ou negligência a partir da ciência da publicação do conteúdo que muitas vezes contraria seu próprio termo de uso ou política), ou mesmo ainda a responsabilidade pelo risco do próprio negócio, não se pode deixar de lado sua fundamental importância na obtenção de resultado prático equivalente, frente à dificuldade de identificação, à primeira vista, dos responsáveis diretos pelos ilícitos cometidos”. Aclarou que, o provedor não pode ser responsabilizado pela publicação em si, pois não há censura prévia, mas por deter os recursos técnicos que permitem sua remoção, quando muitas vezes inclusive é impossível identificar o autor até pela condição de anonimato permitida pelas suas próprias ferramentas. Se ficar inerte, mesmo frente a um pedido formal (escrito), por certo se torna responsável pela omissão e até mesmo conivente e cúmplice da lesão”. Para Peck, os provedores de serviços na internet, têm, sem sombra de dúvida, capacidade técnica para implementar formas de controle e contingência, possibilitando a preservação de direitos e a cessação da sua violação quando determinado judicialmente.

Pela análise dos termos *Europe’s Information Society*, a autora verificou que, existe “possibilidade técnica de análise e reposta às notificações de abuso feitas pelos usuários dentro do prazo de 24 horas. Destacando a importância de se utilizar esse tipo de mecanismo de retirada

⁴⁶ Idem, pág. 266.

de conteúdo do ar sem ordem judicial de forma cautelosa, pois, independentemente do benefício da maior proteção da vítima da ofensa, considerando o princípio da liberdade de expressão, que se coaduna também com o da ampla defesa, sugere, que toda e qualquer remoção de conteúdo deva ser devidamente documentada com a denúncia formal realizada ao provedor, para evitar que haja arbitrariedade e que a justificativa de suspensão e remoção de conteúdo acabe sendo distorcida e utilizada com finalidade de cercear a livre manifestação do pensamento, com intuito inclusive político.

Deve-se evitar a todo o custo o laxismo de quem tenha outros objetivos que não a mera “eliminação” do conteúdo de um determinado site, por exemplo, para tanto deve se criar mecanismos que acatelem e que efetivamente, garantam o devido processo legal, a vítimas de censuras. Segundo Patrícia Peck, “pelo princípio do menor dano, é melhor remover do que manter no ar, mas, sendo infundada a denúncia, deve-se garantir a volta ao ar do conteúdo e também a punição daquele que tenha sido leviano, visto que aí a lesão será à liberdade, em vez de à privacidade (como vem ocorrendo mais comumente, em geral, ferindo a honra e a reputação). Sendo assim, como vimos, a legislação vigente no tocante à responsabilidade civil é totalmente aplicável à matéria digital, devendo apenas observar as particularidades do meio virtual ou dos demais meios convergentes, como já ressaltamos”⁴⁷.

À panóplia dos direitos do titular de dados pessoais, correspondem um rol de deveres, pertencente aos responsáveis pelo tratamento. Tanto na legislação pátria, como a sua fonte principal, ou seja a legislação de Portugal, também na Lei Geral de Proteção de Dados do Brasil, Angola e STP, diferenciam esses deveres conforme a relação do responsável com o tratamento, denominando aquele que exerce a decisão sobre o tratamento de **controlador**, enquanto aquele que executa o tratamento, sob as ordens do controlador, de **operador**. Juntos, eles são os “**agentes de tratamento**”. Considera Walter Aranha Capanema, sob um pendor civilística, que o controlador seria o **mandante**, e o operador, o **mandatário**. Para o mesmo, deve-se mesmo arriscar, “aventar a hipótese de que a relação controlador-operador constitua modalidade especial de mandato, própria das relações que envolvam tratamento de dados pessoais”⁴⁸.

Decompondo a relação na qual se entrelaça o tratamento de dados, podemos identificar nesta encadeamento jurídico um outro ator, ante ao direito Brasileiro, o encarregado, pessoa natural ou jurídica, integrante ou não dos quadros do controlador ou do operador, que exerça, dentre outras funções, a intermediação entre os demais atores, especialmente a Autoridade Nacional de

⁴⁷ Idem, pág. 266.

⁴⁸ // Responsabilidade civil na Lei Geral de Proteção de Dados, Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020, página 163 e seguintes .

Proteção de Dados (ANPD) e, ainda, orienta a aplicação das normas de proteção de dados. Essa complexa relação de múltiplos atores e deveres aqui relatada em resumo evidencia o desafio que as empresas privadas e órgãos públicos encontrarão para estar em conformidade com a LGPD daquele país. Os efeitos do não-atendimento passam não só pelas sanções administrativas que podem ser eventualmente impostas pela ANPD, mas em maior escala, por ações de responsabilidade civil, ressalva Walter Aranha Capanema⁴⁹.

Naquela relação jurídica, a responsabilidade surge do exercício da atividade de proteção de dados que viole a “legislação de proteção de dados”. Por essa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. Com a ressalva de que, em Cabo verde, existem leis esparsas ou infralegais e setoriais, cuja a proteção de dados é salvaguardada, *verbi gratia*, as leis de comunicação social, as leis fiscais e bancárias, leis de saúde e de proteção dos consumidores (a legislação de cabo verde contém lacunas que devem ser supridas a respeito), pelo que, a legislação de proteção de dados é a lei geral, existindo leis especial que merecem salvaguarda, o responsável por aquela salvaguarda é, por exemplo na esfera pública a entidade publica responsável pelo seu tratamento. Cabendo em situações de violações o recurso à comissão nacional de proteção de dados.

À título exemplificativo, sem prejuízo da complexidade da atividade de segurança da informação, seguindo um pouco as pegadas da experiência brasileira, cuja legislação, cremos ser necessário considerar apenas aquelas medidas previstas em padrões devidamente reconhecidos, como as denominadas normas ISSO⁵⁰. Em destaque, duas situações de responsabilidade civil demarcado na LGPD do Brasil, identifica-se, a) violação de normas jurídicas, do microssistema de proteção de dados e b) violação de normas técnicas, voltadas à segurança e proteção de dados pessoais⁵¹. Sendo o fator determinante para que haja lugar à responsabilidade do agente, a violação de norma jurídica ou técnica, que ocasione um dano material ou moral a um titular ou a uma coletividade.

Sobre as hipóteses de exclusão da responsabilidade civil, sugere Walter Aranha Capanema que as mesmas vêm elencadas no artigo no art.º 43.º da LGPD do Brasil. Parafraseando o autor,

⁴⁹ Op. cit.

⁵⁰ ISO é o acrônimo de Internacional Organization for Standardization, uma entidade internacional que estabelece normas e padrões. O padrão ISO 27001, por exemplo, é destinado à segurança da Informação.

⁵¹ // Responsabilidade civil na Lei Geral de Proteção de Dados, Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020, pág. 163 e seguintes .

*Sendo que o inciso I trata da situação em que o agente não realizou o tratamento de dados a que lhe foi atribuído. Ou seja, houve um tratamento de dados, mas o réu não tem qualquer vínculo com ele. Aproxima-se muito da figura da ilegitimidade passiva, que a LGPD trata como matéria de mérito. Já o inciso II exclui a responsabilidade na situação em que o agente realizou o tratamento, mas “não houve violação à legislação de proteção de dados”. Aqui, o dano ocorreu por um ato lícito. Seria o caso, por exemplo, de uma decisão automatizada, baseada em critérios transparentes, informados (presentes em termos de uso) e sem viés, que negue um empréstimo a um possível consumidor. O presente inciso prevê expressamente apenas a situação em que não houve violação à proteção de dados. Deve-se interpretar este artigo em conjunto com os arts. 42, 44, 46 e parágrafo único, conforme as razões já apresentadas, de modo a admitir, também a alegação de ausência de violação de **norma técnica**. A alegação de culpa exclusiva do titular ou de terceiro está prevista no inciso III do art.º 43. Serão os casos em que o dano for causado por exclusiva ingerência do titular, por terceiro, ou por uma atuação conjunta do titular com o terceiro⁵².*

Contudo, se o dano a dados pessoais decorrer do não-atendimento de uma norma técnica, omissão, supomos, ainda que, relativa a uma vulnerabilidade já conhecida e documentada, fica, assim, evidenciada a negligência do agente de tratamento. Admitindo-se, também, que seja possível que o dano tenha resultado do emprego das chamadas “vulnerabilidades não-documentadas”, também conhecidas como *0-day*. Nesse caso, para Walter Aranha Capanema “seria incabível a responsabilização civil, afinal, se não se sabe ainda da sua existência, não tem como exigir o dever de segurança. Logo, não é possível se atribuir aos agentes de tratamento o dever de segurança/proteção dos dados pessoais em toda e qualquer hipótese, mas apenas no estado da arte/técnica existente à época. E, mais, deve-se entender que a obrigação de segurança é de meio, e não de resultado. É impossível ao agente de tratamento garantir, com 100% de certeza, que os dados dos titulares estarão seguros contra qualquer incidente. É preciso, portanto, razoabilidade⁵³”.

São tipologias de danos correlacionados aos dados pessoais, os seguintes: vazamentos/*data leaks*, consiste na fuga (provocada) de dados (código de acesso, *ID*, dados biométricos), que posteriormente podem ser usados para praticas de outros atos criminosos, como a criação e uso de identidade falsas, acesso a contas como se fosse o seu titular, acesso indevido, etc.

⁵² Op. Cit.

⁵³ Responsabilidade civil na Lei Geral de Proteção de Dados, Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020, pág. 163 e seguintes .

A desconsideração dos direitos do titular do dado pessoal, pode acarretar um dano moral para o mesmo, sendo possível imputar ao agente infrator a assunção de um dano não patrimonial, cumulável com os lucros cessantes ou dano emergente, quando haja lugar.

II. O tratamento da Proteção de Dados na Lei n.º 121/IX/2021, de 17 de março

A Lei n.º 121/IX/2021, de 17 de março, procede à segunda alteração da Lei n.º 133/V/2001, do Regime Jurídico Geral de proteção de dados pessoais de pessoas singulares – RJGPD de 22 de janeiro, alterada pela Lei n.º 41/VII/2013, de 17 de setembro.

Para efeitos do artigo 4.º do RJGPD “o tratamento de dados pessoais deve processar-se no estreito respeito pelos direitos, liberdades e garantias fundamentais das pessoas singulares, em especial pelo direito à reserva da intimidade da vida privada e familiar e pelo direito à proteção dos dados pessoais”, em cumprimento do desiderato Constitucional, garantia reconhecida na Magna Carta de Cabo Verde. Segundo os termos da *norma normarum*, no artigo 45.º sob a epígrafe “*Utilização de meios informáticos e proteção de dados pessoais*”, e paralelamente nos artigos 44.º, quando fala sobre inviolabilidade de correspondência e das telecomunicações, e no artigo 41.º, com o teor mais abrangente, sobre o direito à identidade, à personalidade ao bom nome, à imagem e à intimidade.

À luz do n.º 1 do artigo 5.º, na alínea a) o legislador define “dados pessoais” como sendo, “qualquer informação, de qualquer natureza e independentemente, do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável, titular de dados”. Sendo considerada identificável, uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular, segundo os termos do artigo 5.º n.º 2.

Por tratamento de dados pessoais, no âmbito da mesma norma (alínea b)), entende-se qualquer operação ou conjunto de operações sobre dados pessoais, por meio automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação, a interconexão, a limitação, o apagamento, ou a destruição, bem como a realização de operações lógicas e/ou aritméticas, sobre esses dados”.

Considera-se o responsável pelo tratamento (alínea d)) a “pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determina as finalidades e os meios de tratamento de dados pessoais”.

Segundo o preceituado no artigo 6.º do RJGDP, exige-se ao responsável pelo tratamento de dados pessoais, uma atuação ancorada, imperativamente, no princípio do tratamento lícitude e da transparência dos dados pessoais, assim com se exige uma atuação baseada no princípio da boa fé. A partir dali, para efeitos da norma, se determina a qualidade dos dados.

Bem andou o legislador angolano quando por questões de razoabilidade e de melhor entendimento regulamenta vários dos princípios vinculados ao tratamento de dados pessoais, nomeadamente, o princípio da lícitude, da transparência, da proporcionalidade, da veracidade, da finalidade, da durabilidade da conservação, etc., (artigos 6.º e seguintes da Lei n.º 22/11 de 17 de julho).

É uma exigência prática que os dados sejam coletados tendo por matriz principal uma finalidade específica definida, de forma determinada, explícitas e legítimas – o princípio do fim – artigo 6, n.º 1, alínea b).

A exigência de dados é um dos pontos centrais da representação do indivíduo na esfera digital, por isso mesmo, a autodeterminação informacional afigura-se como o princípio que está na base da identificação dos fins do tratamento de dados. Em cada caso concreto, caberá ao titular de dados emitir o seu consentimento (previa ou posteriormente, em casos de dados sensíveis, uma autorização para tratamento), para o uso de seus dados pessoais de acordo com um propósito especificado. Esse liame entre a estrita especificação de uma finalidade e o consentimento do titular ou autorização da CNPD, é o que se chama de princípio da limitação dos propósitos (*purpose limitation principle*) o uso dos dados pessoais deve-se limitar àquela finalidade autorizada, sendo que qualquer outro uso demandaria um novo consentimento, realça Bruno Bioni⁵⁴.

Mais, imperiosamente se exige que os dados pessoais sejam adequados – princípio da adequação, e se pautem por critérios temporais limitados, sendo apenas admitidos quando sejam pertinente e limitados ao mínimo necessário às finalidades para que são tratados, alínea c, n.º 1 do artigo 6.º - limitação da conservação. Todavia segundo argumenta Mafalda Miranda Barbosa, “agora, que os dados pessoais podem ser conservados durante períodos mais longos, desde que

⁵⁴Proteção de dados pessoais : a função e os limites do consentimento, editora forense 2019.

sejam tratados exclusivamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos”⁵⁵.

Com a mesma exigência, os dados devem ser conservados de modo a salvaguardar a sua integridade e devem ser guardados com um nível adequado de segurança e proteção. Não podendo ultrapassar o períodos inicialmente assegurados – garantia assegurada segundo os moldes do o princípio da integridade e confidencialidade.

Segundo o disposto no artigo 7.º do Regime geral, o tratamento de dados pessoais apenas é feita na medida em que haja tido lugar o consentimento informado e lícito do seu titular, salvo se se tratarem dos elencados nas alíneas a), b), c), d), e) do artigo 7.º, ou seja, de dados sem necessidade de consentimento do titular é lícito o tratamento para execução do contrato em que o titular de dados seja parte, para cumprimento de obrigação legal a que o responsável de tratamento esteja sujeito, para proteção de interesses vitais do titular de dados, quando esteja impossibilitado, por incapacidade, de prestar o seu consentimento, execução de interesse público, etc.

Destaca Mafalda Miranda Barbosa que,

“consentimento tem de ser prestado livremente e tem de ser esclarecido. Daí que o titular dos dados tenha direito à prestação de uma série de informações, por parte do responsável, que lhe permitam compreender a natureza e o alcance do ato, bem como lhe permitam, posteriormente, acompanhar o tratamento que deles seja feito. No mais, o consentimento tem de ser específico, isto é, orientado para as finalidades a que o responsável se propõe, nos termos dos artigos 12º e seguintes do Regulamento. De notar, porém, que o direito à informação de que se cura tem um âmbito e uma intencionalidade mais vastas do que de mero instrumento de esclarecimento conducente à licitude do consentimento. Por um lado, ele continua a existir, quando o tratamento dos dados se baseie noutros fundamentos que não essa autorização do titular; por outro lado, ele revela-se essencial para que o titular dos dados pessoais possa acompanhar o tratamento que deles seja feito. Parece, aliás, ser esta a ratio do direito à informação a que se refere o artigo 15º Regulamento e que surge associado ao direito de acesso do titular dos dados. Tal direito de acesso é subseqüente à recolha dos dados.”. conforme o indicado, possui idem o titular de dados na legislação de Cabo-Verde,

⁵⁵Revista de Direito Comercial - Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil,
<https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5b2b4f0b575d1f53ad7ad45e/1529564942011/2018-10.pdf>

*segundo o artigo 13.º do RJGPD. O consentimento, porém, é livremente revogável, a todo o tempo.*⁵⁶

Para efeitos da legislação de Cabo Verde, o n.º 3 do artigo 9.º especifica que “o titular dos dados tem o direito a retirar o seu consentimento a qualquer momento, de forma fácil e sem ser prejudicado, sem prejuízo da licitude do tratamento já realizado com base no consentimento previamente dado”.

Destaca Mafalda Miranda Barbosa, este direito, é concretizável via consagração do direito ao esquecimento, embora a intencionalidade deste ultrapasse as hipóteses de mera revogação do consentimento⁵⁷.

Esta também foi a intenção do nosso legislador, ao consagrar no artigo 16.º do RJGPD, quanto ao direito ao apagamento. Este direito ao esquecimento porém não é ilimitado. Consta-se que, por força do n.º 2 do no artigo 16.º, quando o tratamento se revele necessário ao exercício da liberdade de expressão e de informação, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; quando haja motivos de interesse público no domínio da saúde pública; quando estejam envolvidos arquivos de interesse público, fins de investigação científica ou histórica ou fins estatísticos, e o direito ao esquecimento tornasse impossível ou prejudicasse gravemente a obtenção dos objetivos desse tratamento; ou quando esteja em causa o exercício de um direito num processo judicial, etc.

Para além do direito ao esquecimento, o titular dos dados tem também direito, nos termos do artigo 5.º, a obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito ou que os dados incompletos sejam completados; nos termos do artigo 17.º, a obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma hipóteses previstas no preceito (direito de limitação). Assim como o direito de portabilidade dos dados (artigo 18.º) e da oposição ao seu tratamento (artigo 20.º).

Um dos deveres dos responsáveis (*controllers*) pelo tratamento advém do disposto no 24.º do RJGPD quando à segurança do tratamento, segundo nota Mafalda Miranda Barbosa “o reforço

⁵⁶ Revista de Direito Comercial - Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil, <https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5b2b4f0b575d1f53ad7ad45e/1529564942011/2018-10.pdf>

⁵⁷ *Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil* – Revista de Direito Comercial, 2018 – pág. 436 <https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5b2b4f0b575d1f53ad7ad45e/1529564942011/2018-10.pdf>

da segurança passa, a este nível, *inter alia*, também, pela aplicação, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, de medidas técnicas e organizativas adequadas, como a pseudonimização, a garantir a eficácia dos princípios da proteção de dados”⁵⁸.

O RJGPD no seu artigo 5.º n.º 1, na alínea e), admite que o tratamento de dados seja levado a cabo por um subcontratante, ou seja, uma pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trata os dados pessoais por conta dos responsáveis pelo tratamento. Não percebemos como a lei pressupõe que esta relação se efetive, se via acordo simples ou por contrato, nem quem são os subcontratantes. Outra importante interrogação a ser feita se prende com o fato de saber se o subcontratado pode subdelegar os poderes outorgados.

Entra na cadeia de tratamento de dados pessoais outras entidades, como os designados pelo regime, como sejam, os encarregados de proteção de dados, disposto no artigo 30.º do Regime geral. No caso, ou o responsável principal de tratamento ou o subcontratante por si indicado, podem designar um encarregado de proteção de dados quando: o tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais e o Ministério Público no exercício das suas competências processuais; as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido a natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grandes escala; ou, as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados previstos no artigo 8.º (tratamento de dados especiais) e de dados relacionados a condenações penais e infrações a que se refere o artigo 11.º (registo de atividade ilícitas, condenações penais, medidas de segurança, infrações e contraordenações)

O artigo 47.º do RJGPD reconhece a qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições legislativas ou regulamentares em matéria de proteção de dados, o direito de obter do responsável a reparação pelo prejuízo sofrido, dentro da esfera da responsabilidade civil, porém, essa via não exclui o recurso às vias judiciais (artigo 46.º).

⁵⁸ *Data controllers e data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil – Revista de Direito Comercial, 2018 – pág. 436
<https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5b2b4f0b575d1f53ad7ad45e/1529564942011/2018-10.pdf>

Enfatiza-se no n.º 2 da mesma norma que, o responsável pelo tratamento pode ser parcial ou totalmente exonerado dessa responsabilidade se provar que o fato que causou dano lhe não é imputável.

Em termos amplos, segundo nota Mafalda Miranda Barbosa⁵⁹,

“se o conceito de responsável pelo tratamento de dados nos remete para uma ideia de responsabilidade enquanto assunção de um especial encargo, a implicar especiais deveres, que visam a salvaguarda dos dados pessoais alheios; o referido responsável pelo tratamento de dados pode tornar-se responsável, no sentido da *liability*, em caso de violação de algum ou alguns desses deveres. Fazendo-nos situar a montante ou a jusante do processo de tratamento de dados, as duas responsabilidades com que assim lidamos – responsabilidade pelo tratamento de dados e responsabilidade civil pela violação de dados pessoais – não deixam de apresentar entre si uma linha de continuidade, já que é a responsabilidade pelo tratamento de dados que, ao desenhar uma esfera de controlo associada a especiais deveres de cuidado que têm de ser assumidos, nos permite, a posteriori, determinar quem é o civilmente responsável”.

A mesma autora, considera que “não basta pensar numa esfera de responsabilidade a montante para que a imputação – e, portanto, a responsabilidade civil, a jusante – se possa afirmar, tanto mais que, neste âmbito ela se define em abstrato pelo legislador”. Assim, haveremos de analisar em que medida a lesão que ocorre se liga funcionalmente ao dever omitido. Nesta ordem de ideia, para a mesma, deve-se confrontar a esfera de responsabilidade do *controller* com outras esferas de responsabilidade. “É por isso que se torna particularmente importante – ou mesmo imprescindível – compreender as relações que se podem estabelecer entre o responsável pelo tratamento de dados e outros responsáveis pelo tratamento de dados ou entre o responsável pelo tratamento de dados e os subcontratantes”⁶⁰.

Com relação ao nosso entorno legal, o legislador nacional peca por omissão quando não prevê as responsabilidades dos demais intervenientes na cadeia de tratamento, assim como o fez

⁵⁹ *Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil* – Revista de Direito Comercial, 2018 – pág. 426.

<https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5b2b4f0b575df53ad7ad45e/1529564942011/2018-10.pdf>

⁶⁰ *Idem* – pág. 427.

o legislador da Europeu, e a legislação de Portugal. Esse desiderato se justifica na medida em que, aqueles documento inspiraram *in natura* o nosso regime, logo, pensamos que a salvaguarda dos dados estariam mais claros, se se percebesse quem sejam os responsáveis e quando cada um intervenientes sejam responsáveis pelos seus atos.

Ainda para mais, quando o n.º 2 do artigo 47.º do regime impõe ao responsável pelo tratamento a faculdade de exonerar-se, total ou parcialmente, da responsabilidade se provar que o fato que causou o dano “lhe não é imputável”. Idem para a legislação portuguesa que nas palavras de Mafalda Miranda Barbosa, “a formulação legal peca, contudo, por não perceber que, se o evento não for imputável ao sujeito, não é possível afirmar-se a responsabilidade, não fazendo sentido falar de uma responsabilidade parcial. Teria, portanto, de se tratar de uma não imputação em termos também parciais, a obrigar a uma correção do preceito.”⁶¹

Nesse sentido, dentro da União Europeia, segundo indica Mafalda Miranda Barbosa “o Regulamento prevê, no artigo 82º, que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do referido regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. Acrescenta o nº 2 do preceito que qualquer responsável pelo tratamento que nele esteja envolvido é responsável pelos danos causados por um tratamento que viole o presente regulamento, sendo o subcontratante responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações impostas pelo regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Esta responsabilidade pode ser afastada se o responsável pelo tratamento ou o subcontratante provar que não é responsável pelo evento que deu origem aos danos. Havendo mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, que sejam responsáveis por danos causados pelo tratamento, cada um é responsável pela totalidade dos danos, prevendo-se no nº5 do artigo 82º a possibilidade de exercício do direito de regresso em relação à parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com a regra estabelecida no nº2.”⁶²

Numa acórdão do Supremo Tribunal Judicial de Portugal, considerou-se que os dados pessoais merecem tutela mesmo em sede de divulgação de informação que carácter público, para tanto, o duto acórdão acentuou, que de principio, o *caráter público*, “não basta para que se possa afastar o regime relativo à proteção de dados pessoais; acresce que ocorreu a utilização de informação para finalidades distintas da recolha, em clara violação do regime de proteção de

⁶¹ *Idem* – pág. 439

⁶² *Idem* – pág. 439

dados pessoais. O demandado atuou com dolo direto uma vez que lesou direitos da pessoa legalmente protegidos, e interesses individuais tutelados penalmente através das normas supra citadas.”

Em sede da responsabilidade civil perpetrado por atos *contra legem*, a descoberto da legitimidade cometida pela LGJDP, presume-se a responsabilidade *in re ipsa*, ou seja, o dano moral é presumido, dando lugar à reparação do dano causado, independentemente da comprovação do dano moral ou psicológico efetivamente causado ao titular do dano. Constituindo-se assim, uma exceção à modalidade tradicional da configuração do dano moral, que pressupõe a prova da conduta ilegítima, o dano material efetivo, e onexo causal. Naquele, a única exigência, é a existência dos próprios fatos da conduta desviante – ou ilícita. Sanciona-se, desse modo, a mera conduta antijurídica.

O nosso regime, ao em vez de se pautar pelo caminho da responsabilidade civil para punição de danos decorrentes da violação do regime jurídico de proteção de dados, optou antes, para a aplicação de sanção administrativa (coimas essencialmente), concomitantemente com infrações criminais, desembocando na aplicação de pena de prisão e multas, e sanções acessórias, cumulativamente.

Aqui entendida violação de dados pessoais, conforme o configurado na alínea o9 do artigo 5.º do RJGPD, constituindo uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Ao nível da proteção e nas situações de prejuízos ou tratamentos de dados ilegítimos, cabe a sua avaliação ao nível de infrações administrativas, em sede de contraordenações (artigo 48.º d RJGPD), aplicável subsidiariamente ao *corpus juris* da normativa de proteção de dados.

De entre as infrações específicas elencadas no regime jurídico cabe indicar aquelas praticadas por omissão ou derivadas do cumprimento defeituoso de obrigações sujeitas ao titular do tratamento ou subcontrate. Segundo o artigo 49.º do RJGPD, as entidades, que por negligência, não cumpram a obrigação de notificação à CNPD⁶³ do tratamento de dados pessoais a que se referem os números 1 e 5 do artigo 39.º, prestem falsas informações ou cumpram a obrigação de notificação com inobservância dos termos previstos no artigo 41.º, ou ainda quando, depois de notificadas pela referida comissão, mantiverem o acesso à redes abertas de transmissão de dados a responsáveis por tratamento de dados pessoais que não cumpram as disposições da presente lei, praticam contraordenação punível com coimas.

⁶³ Comissão Nacional de Proteção de Dados, a título de curiosidade, tanto em Angola como em São Tomé, existem Agências de Proteção de Dados, comungando das mesmas funções.

Em se tratando de uma pessoa física ou singular, é incorre na aplicação do montante mínimo de 50.000\$00 e um máximo de 500.000\$00. Se se tratar de ente coletivo ou pessoa jurídica, mesmo que não possua personalidade jurídica, são lhes aplicáveis a título de coima por prática de infrações ao nível da lei de proteção de dados, um valor mínimo 300.000\$00 e um máximo de 3.000.000\$00.

Em ambas as situações, as coimas são agravadas ao dobro quando estiver em causa dados sujeitos ao controle prévio, nos termos exarados do artigo 40.º o artigo 50.º do mesmo diploma ressalva outras situações passíveis de punição. A negligência e a tentativas são sempre puníveis (artigo 52.º).

Em termos e concurso de infrações, segundo o preceituado no artigo 51.º, o legislador pátrio optou, nas situações de um mesmo fato constituir, simultaneamente, crime e contraordenação, punir o agente infrator sempre a título de crime.

Em se tratando de crimes, *verbi gratia*, o não cumprimento de obrigações relativas a proteção de dados (artigo 49.º) o agente é punido com prisão até um ano ou, em alternativa, multa até 120 dias quem intencionalmente: omitir a notificação ou pedido de autorização a que referem os artigo 39.º (obrigação de notificação) e 40.º (controle prévio); fornecer falsas informações na notificação ou nos pedidos de autorização para tratamento de dados pessoais ou neste proceder a modificações não consentidas pelo instrumento de legalização; desviar ou utiliza dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização; depois de ultrapassado o prazo que lhes tiver sido fixado pela CNPD para cumprimento das obrigações previstas na RJGPD ou em outra legislação setorial de proteção de dados, as não cumprir; depois de notificado pela CNPD para não o fazer, mantiver o acesso a redes abertas de transmissão de dados a responsáveis pelo tratamento de dados que não cumpram as disposições da RJGPD. Em se tratando de dados sensíveis⁶⁴, *rectius* “dados especiais” usado pelo nosso legislador, a pena é agravada em dobro em seus limites mínimos e máximos.

A referência à “dados especiais” ao em vez do comumente tratado em outras cearas legislativas de “dados sensíveis” causa estranheza. Os dados sensíveis requerem um maior grau de proteção dado, justamente ao seu cunho especial e específico e às implicações que o seu tratamento implica. Doutrinariamente, jurisprudencial e legalmente os dados de cunho sensíveis são consideradas aquelas que estão sujeitos a condições de tratamento específicas, dados

⁶⁴ Adjetivação que não faz parte do corpus juris da RJGPD, o artigo 8.º do mesmo faz expressa referência “aos dados especiais”, denotando-se uma certa abstração do termo. Legislações estrangeiras (nomeadamente a de São Tomé e Príncipe e a de Angola, reporta especificamente a referencia expressa de “dados sensíveis”, seguindo as pegadas das legislações mais avançadas de proteção de dados, a saber da União Europeia, que inspirou aquelas.

Conclusão

Em jeito de conclusão, depois da tratamento da matéria objeto do estudo, aptamos por deixar contributos de vários autores, que nos enunciam pistas e considerações relativamente à proteção de dados, com relação ao direito de consumo e aos direitos do consumidor, pois que consideramos bastante nítida a determinação da responsabilidade pela violação de dados pessoais. Outras áreas requerem um olhar mais atento por parte do nosso legislador, contudo, está de parabéns pois a lei de proteção de dados de cabo verde além muito avança, é adequada ao desígnio do legislador, de modo que é capaz de atender uma necessidade social e possui as condições necessárias para ser empiricamente aplicada de forma eficaz.

Hoje, convergem para a *Internet* todas as atividades sociais contemporâneas, formando um microcosmo eletrónico. O interesse social pelas redes eletrónicas faz-se acompanhar pelo interesse económico, gerando o *comércio eletrónico*. *A par e passu*, todos deixamos rastros digitais, de informações que, se tratadas analiticamente poderão ser usadas na modelagem comportamental dos internautas. *O microtargeting⁶⁷ chega a ser agressivo, sendo por isso de extrema importância evitar a todo custo a total mercantilização de dados pessoais. É consensual que hoje em dia os dados são as chaves que abrem a porta e dão acesso ao indivíduo a toda a gama de serviços digitais, mas a disponibilidade dados não pode ser feita sem garantias mínimas de seguranças.*

Inovador a discriminação que o legislador Angolano faz relativamente às “espécies de tratamentos” relativamente à finalidade do tratamento dado a dados pessoais em áreas específicas, a saber, dados para fins de publicidade (artigo 18º), para fins de publicidade por via eletrónica (artigo 19.º), tratamento de dados de crédito e de solvabilidade (artigo 16.º), isso porque, imaginamos, o consumidor considerado *hipossuficiente ou hyper-vulnerável*, estaria numa relação assimétrica com relação aos anunciantes ou de entidade financeiras, em termos de disponibilidade de informações. Essas normas pensamos nós que, protege diretamente o consumidor internauta, uma vez que, ao se falar da cibernética, existe um afluxo de informações, que poderão ser consideradas abusivas e ilegítimas, porque periga os direitos do consumidor. Vemos aqui a doutrina concebida do *opt-in* e do *opt-out*, que em outro momento será melhor desenvolvida.

Aplaudimos também a opção legislativa de STP quando reconhece ao titular de dados o direito à indenização, sempre e quando, uma “pessoa que tiver sofrido um prejuízo decorrente do

⁶⁷ Que ultrapassam a esfera do consumo e do comércio eletrónico, chegando a ser usadas em eleições políticas, veja -se o Cambridge Analytica.

tratamento ilícito de dados ou de qualquer outro ato que viole disposição legal ou regulamentar em matéria de proteção de dados pessoais tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido” (artigo 14.º da Lei n.º 03/2016 Visa Garantir e Proteger os dados pessoais das Pessoas Singulares).

A nossa lei de proteção do consumidor é arcaica no sentido de proteção do consumidor digital, porque além de ser antiga é muito reduzida quanto às garantias de proteção do consumidor, urge medidas legislativas nesse segmento, porque o chapéu protetor do consumidor, apesar de outras normas setoriais e específicas existentes salvaguardarem os direitos dos consumidores, a legislação geral não assegura uma proteção adequada à sociedade de informação e de tecnologias digitais, na era da economia digital. Esse é um repto a quem de direito, tomar as medidas cabíveis a fim de suprir essa lacuna, urgentemente. A legislação de proteção do consumidor e do consumo deve imperiosamente estar alinhada às linhas orientadoras do tratamento de dados, sobretudo porque o fluxo de dados e informações pessoais, ou financeiras, contratuais, fiscais, cada vez mais trafegam nos canais digitais. E a legislação atual não coaduna com o desiderato atual da Digitalização de bens e serviços.

A lei de proteção de dados é bastante complexa e a nata classe da sociedade não está familiarizado com os seus contornos, conceitos, é nítida que uma cultura de literais deve ser criada, e nisso deverão aliar-se os contributo em coordenação da associação de defesa dos consumidores, da ANPD e da própria comunicação social publica, posto que é um serviço público que dever ser salvaguardado. O direito de antena que detém a associação de defesa dos consumidores poderá servi a esse propósito. Pessoas, consumidores, munidos de informações certas, saberão melhormente decidir e mais, terão consciência da premissa maior de que os dados pessoais são ativos valiosos, que hoje em dia merecem maior proteção, sob pena vêm-se prejudicados pelo mau uso de seus dados pessoais.

Uma outra área emergente e que merece uma maior atenção tem que vem com a resolução de conflitos de consumo, que envolvem partilha de dados telematicamente, sendo de suma importância precaver o compartilhamento indevido de dados. Claro que não ficam de fora, situações que a lei já prevê de extravio, de acesso indevido ou de roubo de dados pessoais, situações extremas de violação aos dados pessoais, considerados, crimes.

A não preceituação da possibilidade de impugnação das decisões da CNPD nacional claramente grave, por que deixa a descoberto ações vitais do titular de dados, ou mesmos do próprio responsável pelo tratamento em ter o direito de ver revisto (por exemplo) a decisão da comissão. Sem prejuízo de legislações subsidiárias, considera-se que seria uma tutela maiormente, que essa possibilidade estiver na lei de proteção de dados, como o faz a legislação

Portuguesa e a Angolana, se bem que a nossa Lei estivesse mais próxima da primeira que a da segunda, existindo entre a legislação de Cabo verde e de Angola diferenças substanciais em termos de regulamentação da proteção social, mas todos têm uma linha orientadora semelhantes. Sendo de realçar que a nossa lei de proteção de dados data de 2001 e já está na sua segunda alteração, sendo a última de 2021. Sendo conduto importante ainda importar melhorias não só de países considerados mais avançados mais também daqueles que, dada a proximidade cultural e outras, nos permitiria reforçar a proteção de dados ao nível de transferências e de comunicabilidade de dados entre indivíduos, dentro da lusofonia, por exemplo. Em termos da relação de consumo, seria pertinente a sua análise.

Cabo-Verde, Setembro de 2021.

Bibliografia

Bruno Ricardo Bioni, *Proteção de dados pessoais : a função e os limites do consentimento*, editora forense 2019. (ISBN 978-8530981686)

Dov Seidman, *Como. Por que o Como Fazer Algo Significa Tudo*. 2011 (978-8588329690).

Fernando Antonio Tasso (org.), *A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor - Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020*. (ISSN 1806-5449)

Freitas Valle Dresch | Lílian Brandt Stein, *Direito Fundamental à proteção de dados e Responsabilidade Civil*, *in* <https://revistadireitoresponsabilidade.pt/2021/direito-fundamental-a-protecao-de-dados-e-responsabilidade-civil-rafael-de-freitas-valle-dresch-lilian-brandt-stein/>

José Faria da Costa – *Direito Penal da Comunicação, alguns escritos*, Coimbra editora 1998 (ISBN 972-32-0850-4)

Joel Timóteo Ramos Pereira, *Compêndio Jurídico da Sociedade da Informação, notas Práticas, legislações, jurisprudências, Quid Juris -2004*. (ISBN 9789727242252)

Manuel A. Carneiro da Frada, *Direito e Internet (Liberdade de Informação, Privacidade e Responsabilidade Civil)*, 6ª ed. Atlas, 2013 (e-ISBN 978-85-224-7892- 7).

Mafalda Miranda Barbosa, *Revista de Direito Comercial - Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil*, <https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5b2b4f0b575d1f53ad7ad45e/1529564942011/2018-10.pdf>

Orides Mezzaroba e Fernando Galindo (eds.), *DEMOCRACIA eletrônica — Zaragoza*, Prensas Universitárias de Zaragoza, 2010, Página 20, 21. (LEFIS Series ; 11) ISBN 978-84-15031-74-1

Patrícia Peck, *Direito digital — 5. ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 — São Paulo : Saraiva, 2013* (ISBN: 9788502635616)

Walter Aranha Capanema, *Responsabilidade civil na Lei Geral de Proteção de Dados*, Cadernos Jurídicos - Ano 21 - Número 53 - Janeiro-Março/2020.

Warren and Brandeis, *The Right to Privacy - Harvard Law Review*, Vol. IV December 15, 1890, No. 5.

Sites

https://apd.ao/fotos/frontend_1/editor2/110617_lei_22-11_de_17_junho-proteccao_dados_pessoais.pdf

https://www.uc.pt/protecao-de-dados/perguntas_frequentes#q4_2.

<https://static1.squarespace.com/static/58596f8a29687fe710cf45cd/t/5b2b4f0b575d1f53ad7ad45e/1529564942011/2018-10.pdf>

(http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)

<https://carneirocunha.adv.br/artigos> (Lei Nº 13.709, de 14 de agosto de 2018).

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/e922d7c5a0ca56aa8025851200533efd?OpenDocument>

<https://dre.pt/legislacao-consolidada/-/lc/74901117/201704032057/diploma/1?rp=indice>

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis&so_miolo=

https://www.apd.ao/fotos/frontend_1/editor2/190709_resolucao_33-19_de_9_julho-convencao_ciberseguranca_proteccao_dados.pdf

https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

https://www.uc.pt/protecao-de-dados/perguntas_frequentes#q4_2.

https://apd.ao/fotos/frontend_1/editor2/110617_Lei_22-11_de_17_junho-proteccao_dados_pessoais.pdf

Legislações

Constituição da República de Cabo Verde DE 1992

Código Civil de Cabo verde de 1997

Lei Cabo Verdiana de proteção de dados (Lei n.º 121/IX/2021, de 17 de março, procede à segunda alteração da Lei n.º 133/V/2001, do Regime Jurídico Geral de proteção de dados pessoais de pessoas singulares – RJGPD de 22 de janeiro, alterada pela Lei n.º 41/VII/2013, de 17 de setembro)

Lei Brasileira de proteção de dados (Lei Nº 13.709, de 14 de agosto de 2018)

Lei português de proteção de dados (Lei n.º 67/98 - Diário da República n.º 247/1998, Série A de 1998-10-26 (que transpõe para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995)

Lei Angolana de proteção de dados (Lei n.º 22/11 de 17 de junho)

Lei Santomense de proteção de dados (Lei n.º 03/2016)