I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

DIREITO CIVIL E TECNOLOGIA

D598
Direito civil e tecnologia [Recurso eletrônico on-line] organização I Congresso de Tecnologias Aplicadas ao Direito – Belo Horizonte;

Coordenadores: Renato Campos Andrade, Priscila Ladeira Alves de Brito e Jayro Boy de Vasconcelos Júnior – Belo Horizonte, 2017.

Inclui bibliografia
ISBN: 978-85-5505-658-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: O problema do acesso à justiça e a tecnologia no século XXI

1. Direito. 2. Tecnologia. 3. Direito civil. I. I Congresso de Tecnologias Aplicadas ao Direito (1:2018 : Belo Horizonte, BH).

CDU: 34

I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

DIREITO CIVIL E TECNOLOGIA

Apresentação

É com imensa satisfação que apresentamos os trabalhos científicos incluídos nesta publicação, que foram apresentados durante o I Congresso de Tecnologias Aplicadas ao Direito nos dias 14 e 15 de junho de 2018. As atividades ocorreram nas dependências da Escola Superior Dom Helder Câmara, em Belo Horizonte-MG, e tiveram inspiração no tema geral "O problema do acesso à justiça e a tecnologia no século XXI".

O evento foi uma realização do Programa RECAJ-UFMG – Solução de Conflitos e Acesso à Justiça da Faculdade de Direito da UFMG em parceria com o Direito Integral da Escola Superior Dom Helder Câmara. Foram apoiadores: o Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, EMGE – Escola de Engenharia, a Escola Judicial do Tribunal Regional do Trabalho da 3ª Região, a Federação Nacional dos Pós-graduandos em Direito – FEPODI e o Projeto Startup Dom.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito, oriundos de dez Estados diferentes da Federação, puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central do grupo. Foram debatidos os desafios que as linhas de pesquisa enfrentam no tocante ao estudo do Direito e sua relação com a tecnologia nas mais diversas searas jurídicas.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, e, principalmente, pesquisas oriundas dos programas de iniciação científica, isto é, trabalhos realizados por graduandos em Direito e seus orientadores. Os trabalhos foram rigorosamente selecionados, por meio de dupla avaliação cega por pares no sistema eletrônico desenvolvido pelo CONPEDI. Desta forma, estão inseridos no universo das 350 (trezentas e cinquenta) pesquisas do evento ora publicadas, que guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

A RESPONSABILIDADE CIVIL NA PROTEÇÃO DE DADOS: UM ESTUDO COMPARADO ENTRE BRASIL E UNIÃO EUROPEIA

RESPONSABILIDAD EN LA PROTECCIÓN DE DATOS: UN ESTUDIO COMPARADO ENTRE BRASIL Y LA UNIÓN EUROPEA

Sílvia Gabriel Teixeira
Carolina Rodrigues de Freitas

Resumo

Diante da velocidade de circulação de dados pessoais entre diversos estados, verifica-se uma necessidade de reforço do direito dos titulares dos dados pessoais e na harmonização de um elevado nível de proteção. Para isso, é analisada a responsabilização civil dos provedores de internet perante a normatização brasileira acerca do uso da internet como a Lei 12.965/2014 e destaca as principais alterações introduzidas pelo Regulamento Geral de Proteção de Dados na União Européia. Ao longo do artigo, é destacada a natureza da exposição da responsabilidade dos controladores e processadores, o ônus da prova e as defesas disponíveis para controladores e processadores.

Palavras-chave: Responsabilidade civil, Dados pessoais, Direitos fundamentais, Harmonização, Proteção

Abstract/Resumen/Résumé

Ante la velocidad de circulación de datos personales entre diversos estados, se observa una necesidad de reforzar el derecho de los titulares de datos personales y la armonización de un alto nivel de protección. Se analizará la responsabilización civil de proveedores de internet ante la normatización brasileña sobre el uso de internet como la Ley 12.965/2014 y destaca las principales alteraciones introducidas por el Reglamento General de Protección de Datos en la UE. Se destaca la naturaleza de la exposición de la responsabilidad de los controladores y procesadores, la carga de la prueba y defensas disponibles para controladores y procesadores.

Keywords/Palabras-claves/Mots-clés: Responsabilidad civil, Datos personales, Derechos fundamentales, Armonización, Protección

INTRODUÇÃO

O rápido desenvolvimento tecnológico vem mudando a nossa vida em diversos aspectos, trazendo benefícios e também desafios, principalmente para o direito. A proteção de dados e a regulação jurídica está na pauta de diversos países, principalmente após o escândalo do uso de dados dos usuários do *Facebook* pela firma *Cambridge Analytica* em campanhas eleitorais[1]. Reabre-se assim, o debate sobre como a informação na *social network* é compartilhada e com quem.

Entretanto, não é fácil tratar desses temas em um mundo formado por interações cada vez mais velozes e complexas, que partem da conectividade e do caráter transfronteiriço da internet, potencializando-se a partir de inúmeros aplicativos, websites e plataformas. Neste contexto, questão fundamental é a quem atribuir a eventual responsabilidade por dano pelo conteúdo das informações transmitidas pela Internet (Sousa, 2013, p. 681).

A questão deve ser visualizada sob dois espectros. Pelo campo da responsabilidade extracontratual visto que "estamos, na verdade, e conforme se constata a partir da identificação de uma relação de interioridade constitutiva entre a proteção de dados e diversos direitos de personalidade[2], num domínio onde se lida com direitos absolutos" (BARBOSA, 2018, p. 443). Por outro lado, a violação dos dados também ocorre pela preterição de determinados deveres que oneram o responsável pelo tratamento, numa relação contratual firmada entre ele e o titular daqueles. Ainda que o contrato não tenha como objeto essa proteção dos dados, a boa-fé pode impor determinados deveres de cuidado que, quando violados, geram responsabilidade contratual (p. 445).

Sendo assim, o objetivo deste artigo é esclarecer a responsabilidade civil dos controladores e processadores sob a lei de proteção de dados da UE e no Brasil. O artigo começa analisando o RGDP, atraves do texto da diretiva em si, seus trabalhos preparatórios e a orientação emitidas. Em seguida, tece breves considerações sobre os instrumentos normativos oferecidos quanto à proteção de dados pessoais nas relações de consumo no Brasil e a perspectiva da instituição de marco regulatório na matéria. Procura-se ainda identificar o conceito de responsável, analisando em que medida a lesão que ocorre se liga funcionalmente ao dever preterido e compreender que podem ser estabelecidas relações entre o responsável

[1] A empresa de propaganda Cambridge Analytica, que participou da campanha eleitoral do presidente americano Donald Trump, recebeu dados pessoais dos usuários do Facebook a partir de um aplicativo usado na rede social, violando as políticas de privacidade da empresa.

[2] A civilística portuguesa tem tratado do problema da proteção de dados a propósito da privacidade seja a concretização ou refração do conteúdo da privacidade, enquanto elemento integrador do objeto do direito geral de personalidade (BARBOSA, 2018, p. 476).

pelo tratamento de dados e outros responsáveis pelo tratamento de dados ou entre o responsável pelo tratamento de dados e os subcontratantes ou interferência de terceiros.

METODOLOGIA

A metodologia utilizada será dedutiva e de abordagem qualitativa, tendo em vista que o critério para a identificação dos resultados é valorativo. Relativamente quanto ao procedimento utilizaremos o método histórico-comparativo. A técnica escolhida para a recolha de dados será a pesquisa bibliográfica e legislativa, com a análise do Regulamento da União Europeia e almeja-se evidenciar a tratativa que possui a matéria na legislação brasileira e se a instituição de uma nova dinâmica normativa será eficiente nos objetivos a que se destina.

DISCUSSÃO E RESULTADOS

Os dados pessoais abrangem as informações respeitantes à vida privada de uma pessoa, bem como informações sobre a sua vida profissional ou pública. Atualmente, na ordem jurídica portuguesa, a tutela geral da personalidade está prevista no artigo 70º do Código Civil, no qual estabelece que a lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça à sua personalidade física ou moral, igualmente previsto na Constituição, no artigo 26º, nº 1, quando se refere ao direito "ao desenvolvimento da personalidade". No Brasil, a proteção se mantém em termos semelhantes, encontrando amparo nos artigos 11 a 20 do Código Civil e no art. 5º, X, c/c o art. 5º, LXXII, da Constituição Federal (CF/88).

Com o avanço da sociedade da informação, especialmente com o crescimento da internet, as legislações atuais restaram ineficazes para o tratamento daquela matéria, dando abertura à regulamentação do uso da Internet[3] e estabelecendo princípios, garantias, direitos e deveres. No âmbito da União Europeia, o Regulamento Geral de Proteção de Dados (RGPD) mais recente é o Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de

[3] Sobre a necessidade de regulação da Internet, Sousa (2013, p. 682-683) lembra que existem quatro soluções teóricas para a questão proposta. A Corrente Liberatória surgiu nos Estados Unidos no início da década de 90 e entende que a Internet é um ambiente que não deveria estar sujeito à regulamentação jurídica tradicional, haja vista a própria impossibilidade de adequação da normatização legal às hipóteses surgidas no âmbito virtual. Contemporaneamente, a teoria da Escola da Arquitetura, sustenta que a arquitetura técnica criada pelo código dos programas de computador que controlam a internet seria a chave para a aplicação do direito no ambiente virtual. A terceira posição, advinda dos EUA, sustenta que há a necessidade de tratados internacionais estabelecerem o direito da Internet e a corrente tradicionalista defende que a norma interna deve ser a principal fonte do direito regulamentador da Internet, mediante o uso da analogia.

Abril de 2016. E em seu artigo 4º/1 conceitua dados pessoais como toda a informação relativa a uma pessoa singular identificada ou identificável, sendo considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador.

No que tange à identificação do responsável, importante a discussão sobre as noções de *data controller* (responsável pelo tratamento de dados) e de *data processor* (subcontratante)[4], pois com isso, é possível elencar critérios de determinação do responsável em caso de violação do direito à proteção de dados pessoais. É a responsabilidade pelo tratamento de dados que, ao desenhar uma esfera de controle associada a especiais deveres de cuidado que têm de ser assumidos, nos permite, a posteriori, determinar quem é o civilmente responsável. Logo, é 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, assim como os eventuais comportamentos de terceiros que possam surgir.

O regulamento vem, igualmente, reforçar alguns dos deveres que recaem sobre os responsáveis (*controllers*) pelo tratamento dos dados, incrementando a segurança na matéria. Estes deveres são extensíveis aos subcontratantes (*processors*) e aplicam-se mesmo que estes sujeitos estejam sediados fora da União Europeia. Um exemplo interessante é fornecido pelo artigo 13 do GDPR, que diz respeito ao dever de fornecer informações à pessoa em causa no caso de um controlador quem coletou informações do assunto dos dados pretende continuar a processar dados para um outro propósito do que aquele para o qual os dados foram coletados (ALSENOY, 2016, p. 282). Entretanto, a identificação do responsável enfrenta obstáculos como o sigilo profissional por parte dos respectivos fornecedores de acesso, utilização de falsa identidade, utilização de um IP falso, prática do Mirror, etc.

O regulamento europeu prevê, no artigo 82º[5], que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do referido regulamento tem direito a

---

[4] O *data controler* é definido como a entidade que sozinha ou em conjunto com outras pessoas "determina os fins e os meios" do processamento. Por outro lado, o *data processor* é definido como uma entidade que processa dados pessoais "em nome de" um controlador. Juntos, esses conceitos fornecem a base sobre a qual a responsabilidade pela conformidade é alocada. Como resultado, ambos os conceitos desempenham um papel decisivo na determinação da exposição de responsabilidade de uma organização ao abrigo da lei de proteção de dados da UE (ALSENOY, 2016, p. 271).

[5] Art. 82 GDPR - *Right to compensation and liability*

1. *Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*
2. *[1]Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. [2]A processor shall be liable for the damage caused by processing only where*

receber uma indenização 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.

A doutrina aponta dois célebres casos jurisprudenciais, dos quais se extrai que o fornecedor de hospedagem, em regra, não é responsável pelos conteúdos ilícitos transmitidos, com exceção das situações de dever de controle ou de fiscalização destes (CASIMIRO, 2000, p. 82). Sendo esta, a tese recepcionada pela jurisprudência brasileira. Embora o GDPR não preveja qualquer responsabilidade específica para o Diretor de Proteção de Dados, as Diretrizes sobre DPO (*data protection officer*), de 13 de dezembro de 2016, abordam essa questão, ao declarar que cabe ao controlador ou processador demonstrar conformidade de atuação. Nesse sentido, entende Luís Menezes Leitão (2002, p. 165) que, a irresponsabilização do prestador de serviços depende do desconhecimento da ilegalidade do material ou atividade, da não atribuição pecuniária pela atividade ilegal e da remoção imediata do material armazenado caso seja notificado da existência de infração.

Em conformidade aos relatórios da União Europeia, o reforço do controlo dos indivíduos sobre os seus dados pessoais deve assentar sobre quatro pilares fundamentais. O direito a ser esquecido, o que significa que as pessoas têm o direito de retirar o seu consentimento (art. 7º, inciso 3 do GDPR) para o processamento dos seus dados. A transparência, fundamental para a construção de confiança na internet e para uma maior clareza no âmbito dos registos em redes sociais. A privacidade por defeito, isto porque as configurações de privacidade exigem, na maior parte dos casos, um esforço operacional

---

it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. *A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.*
4. *Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.*
5. *Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.*
6. *Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).*

considerável. A proteção, independentemente do local dos dados, o que significa que os padrões de privacidade devem respeitar as normas da União Europeia e ser aplicados independentemente da localização geográfica do prestador de serviço (REGENTE, 2015, p. 121).

Relativamente ao ônus da prova, de acordo com o artigo 5 do GDPR, os controladores possuem obrigação geral de demonstrar sua conformidade com os princípios básicos de dados proteção. Além disso, um número de outras disposições estipula adicionalmente que o controlador deve ser capaz de demonstrar conformidade, como as disposições relativas às condições para consentimento (artigo 7), ao processamento que não permitir a identificação (artigos 11 e 12), e à obrigação geral de adotar medidas técnicas adequadas e medidas organizacionais para garantir a conformidade (artigo 24) (ALSENOY, 2016, p. 282).

No Brasil, são oferecidas proteção em legislações esparsas, mas não concede medida profilática para o uso indevido de dados pessoais. Enquanto o Projeto de Lei 5.276/2016 ou o PLS 330/2013 não sejam finalizados e aprovados, o tratamento da problemática é pautado no Código Civil, no Código de Defesa do Consumidor e na Lei 12.965, de 23 de abril de 2014, que institui o denominado "marco civil da internet". Redigido como um verdadeiro tratado, estabelece princípios, garantias, deveres e direitos para o seu uso no país, com a intenção de regular todo o arcabouço jurídico sobre o tema. O texto é dividido em cinco capítulos, sendo reservado ao terceiro, as previsões sobre a neutralidade da rede, a proteção e guarda dos registros, dados pessoais e das comunicações privadas, a responsabilidade pelos danos decorrentes de conteúdo gerado por terceiros, além da requisição judicial de registros.

Conforme o art. 19 do Marco Civil, com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

Seja o Regulamento Europeu, sejam as Leis Brasileiras, além de constituírem norma principiológica, observamos que o texto e sua interpretação guardam consonância com as principais diretrizes de direitos humanos e, consequentemente, orienta o uso da Internet a luz dos direitos personalíssimos e fundamentais do indivíduo. Tais regramentos tratam-se de manifesta incidência dos direitos personalíssimos, eis que garantem ao usuário garantias essenciais, principalmente no plano da integridade moral e intelectual.

Tendo a sensibilidade para o reconhecer, a proteção de dados "deve ser integrada num direito de maior latitude", o direito à identidade informacional. Este seria um "direito de personalidade, na medida em que protege um bem da personalidade composto por várias posições jurídicas" (PINHEIRO apud BARBOSA, 2018, p. 473). No entanto, entendemos que o direito à proteção de dados ultrapassa o direito à privacidade, quanto ao seu âmbito de relevância e a proteção de dados pessoais afigura-se fundamental a diversos níveis.

Em primeiro lugar, ela é vital para salvaguarda da identidade do sujeito, já que a divulgação de dados pessoais pode levar a que outros se apropriem daquela ou que haja dela uma deturpação, levando a que a pessoa seja confundida com outra ou que seja desvirtuada a verdade pessoal do sujeito. Em segundo lugar, torna-se essencial para garantir que não se divulgam determinados elementos que, dizendo respeito ao sujeito, podem ser motivo de discriminação, sendo por isso determinante para a defesa da igualdade.

Por fim, ela é fulcral para a defesa da privacidade do sujeito, bem como para outros direitos de personalidade como a honra. Isto significa que a proteção de dados não tem como objeto último um direito de personalidade, mas vários direitos de personalidade do titular dos dados. E, por outro lado, significa que, e fazendo apelo a uma classificação jus-subjetiva muito cara ao constitucionalismo, estamos diante de um direito-garantia, uma guarda-avançada de certas posições jurídicas ativas.

CONSIDERAÇÕES FINAIS

A proteção dos dados pessoais e o respeito pela vida privada são direitos fundamentais. Neste quadro, o Parlamento Europeu propõe salvaguardar os dados pessoais na União Europeia, aumentando o controle dos utilizadores sobre os seus próprios dados e reduzindo os custos para as empresas. A harmonização do quadro legislativo é essencial dado o caráter global das transferências de dados pessoais na internet.

O GDPR manteve o princípio geral de que o controlador detem a responsabilidade principal sob qualquer atividade de seu controle, mas reconhece também, que os processadores devem ser diretamente responsáveis em relação aos titulares de dados. O Brasil, embora ainda não possua uma legislação específica sobre a proteção de dados pessoais, deveria seguir o exemplo europeu e concretizar o projeto de lei que pretende preencher esse vazio jurídico.

A relevância e a urgência do tratamento da matéria são inegáveis, tanto para os titulares como para aqueles que utilizam dados pessoais de terceiros. Para os titulares, é

importante saberem seus direitos e como exercê-los. Para as empresas, quanto antes iniciarem o processo de adaptação à legislação de proteção de dados, menor será o impacto sentido, do ponto de vista operacional e no relacionamento com titulares de dados pessoais, minimizando o risco de sofrerem penalidades ou outras sanções decorrentes da falta de conhecimento no assunto.

REFERÊNCIAS

FERRETT, Federico. Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? In: **Common Market Law Review**, nº 51, p. 1–26, 2014.

BARBOSA, Mafalda Miranda. Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. In: **Revista de Direito Comercial**, Lisboa, 2018, p. 416-486.

REGENTE, Diuliane Ellen Ribeiro. **A proteção de dados pessoais e privacidade do utilizador no âmbito das comunicações eletrónicas**. Dissertação de mestrado apresentada na Universidade Autónoma de Lisboa, 2015.

SOUSA, Marcos Rogério de. Responsabilidade civil pelo conteúdo das informações transmitidas pela Internet. In: LOPEZ, Teresa Ancona; LEMOS, Patricia Faga Iglecias; Rodrigues Junior, Otávio Luiz (coord.). **Sociedade de Risco e direito privado: desafios normativos, consumeristas e ambientais**. São Paulo: Atlas, 2013.

CASIMIRO, Sofia de Vasconcelos. **A Responsabilidade civil pelo conteúdo da informação transmitida pela Internet**. Coimbra: Almedina, 2000.

LEITÃO, Luís Menezes. **A Responsabilidade civil na Internet. In Direito da sociedade da informação**. Coimbra: Coimbra Editora, 2002, v. III.

ALSENOY, Brendan Van. Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation. In: **Journal of Intellectual Property, Information Technology and E-Commerce Law.** nº 7, 2016, p. 271-288.