XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

TÊMIS LIMBERGER

VALTER MOURA DO CARMO

AIRES JOSE ROVER

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI/ UNISINOS
Coordenadores: Têmis Limberger; Valter Moura do Carmo; Aires Jose Rover. – Florianópolis: CONPEDI, 2018.

Inclui bibliografia
ISBN: 978-85-5505-725-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Tecnologia, Comunicação e Inovação no Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. XXVII Encontro Nacional do CONPEDI (27 : 2018 : Porto Alegre, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

Universidade do Vale do Rio dos Sinos
Porto Alegre – Rio Grande do Sul - Brasil
http://unisinos.br/novocampuspoa/

XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Os encontros nacionais do Conselho Nacional de Pesquisa e Pós-graduação em Direito (Conpedi) têm se consolidado como referência na disseminação de pesquisas que abordam os novos fenômenos envolvendo o direito e o Grupo de Trabalho Direito, Governança e Novas Tecnologias é exemplo de pesquisas desse tipo.

Como na última edição, houve uma diversidade grande de temas e tópicos. Numa tentativa de dar certa unidade temática, ainda assim podemos organizar os artigos em alguns grupos.

O primeiro e mais presente em termos numéricos de artigos foi o tema da Inteligência Artificial. Isso mostra o interesse que hoje está presente em toda comunidade jurídica, com o avanço de diversas técnicas e experimentos no judiciário e nos escritórios de advocacia. Um dos artigos literalmente afirmava que o direito não está imune a essa transformação e outro que é preciso estar atentos aos desafios regulatórios na advocacia. Também foi discutida a disponibilização de dados para que a inteligência artificial avance.

Outro grupo de artigos envolve o tema que sempre está presente de alguma forma, os dados pessoais e sua proteção. O direito à privacidade, a internet das coisas, a proteção dos dados pessoais e big data, o regulamento europeu de proteção de dados e dados personalíssimos na internet foram tópicos tratados.

Outro tema importante sempre presente neste gt foi o processo judicial eletrônico. Uma análise dos tribunais de justiça estaduais e o website do tribunal regional eleitoral do Paraná foram dois artigos que trataram o judiciário neste contexto de uso intensivo de tecnologia.

A internet foi outra temática bem discutida, como sempre. Os temas do discurso de ódio, liberdade de expressão, fake news e a pós-verdade não podiam deixar de estar presentes tendo em vista o seu grau de novidade. Já o acesso à internet, o (cyber)bullying, as redes sociais e a necessidade de coregulação na internet, já bastante discutidos, também foram tratados.

Fechando, os temas da responsabilidade civil, governança e anticorrupção foram bem representados. Temas afins como a política de comunicação e a política de segurança, o papel

das empresas sob a perspectiva ética, a política de governança do youtube e a herança e transmissão de bens virtuais podem ser aqui agrupados.

Enfim, os coordenadores do GT convidam os leitores para desfrutarem do teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Prof. Dr. Aires José Rover – UFSC

Profa. Dra. Têmis Limberger – UNISINOS

Prof. Dr. Valter Moura do Carmo – UNIMAR

Nota Técnica: Os artigos que não constam nestes Anais foram selecionados para publicação na Plataforma Index Law Journals, conforme previsto no artigo 8.1 do edital do evento. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

O NOVO REGULAMENTO EUROPEU DE PROTEÇÃO DE DADOS

THE NEW EUROPEAN DATA PROTECTION REGULATION

Caroline de Melo Lima Gularte
Gabriela Pandolfo Coelho Glitz [1]

Resumo

O presente artigo propõe o estudo comparativo da Diretiva 95/46/CE e do RGPD. Para tanto, analisa-se o histórico e evoluções conceituais trazidas por este novo regulamento, que busca superar as dificuldades de uniformização vivenciados durante a vigência da Diretiva 95/46 /CE. Posteriormente, passa-se para uma análise comparativa entre as legislações. Nesse ponto focar-se-á nas principais alterações identificadas e na ampliação ao direito fundamental de proteção de dados. Fixadas estas premissas, se discutirá o compliance digital e os elementos deste programa, concluindo-se o trabalho com as implicações do Novo Regulamento nas empresas brasileiras.

Palavras-chave: Diretiva 95/46/ce, Novo regulamento europeu de proteção de dados pessoais, Principais alterações, Lei 13.709, Compliance digital

Abstract/Resumen/Résumé

This article proposes the comparative study of Directive 95/46 / EC and the RGPD. We analyze the history and conceptual evolutions brought by this new regulation, which seeks to overcome the difficulties of standardization experienced during the validity of Directive 95 /46 / EC. Subsequently, a comparative analysis is made between legislations. This will focus on the main changes identified and on the extension of the fundamental right to data protection. Based on these premises, the digital compliance and the elements of this program will be discussed, concluding the work with the implications of the New Regulation in Brazilian companies.

Keywords/Palabras-claves/Mots-clés: Directive 95/46 / ec, New european regulation on the protection of personal data, Main changes, Law 13.709, Digital compliance

[1] Mestranda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Bolsista vinculada ao Capes. Pós-graduada em Ciências Penais pela PUCRS. MBA em Gestão Empresarial pela FGV.

INTRODUÇÃO

Nossa sociedade está passando por uma acelerada alteração nas estruturas de interações pessoais. A popularização da internet e dos computadores vem revolucionando a forma de comunicação e transmissão de conhecimento, gerando um impacto tão expressivo que a sociedade passou a adotar uma nova lógica de organização, na qual a posse de dados é vista como detenção de poder (RUARO; SOUZA, 2017, p. 210). Seguindo nesta perspectiva, dados e informações pessoais passaram a ter o papel de matéria prima básica para este novo formato de capitalismo, no qual toda utilização feita na rede deixa um rastro oculto de informações, permitindo que terceiros tenham acesso indiscriminado a dados do usuário, trazendo a consequente mitigação do direto à privacidade (RUARO; SOUZA, 2017, p. 198).

Na era do Facebook, Instagram, Linkedin e de tantos outros aplicativos que surgem aos milhares diariamente, as tecnologias da comunicação e informação caminham no sentido oposto à esfera privada, entendida como autodeterminação informativa, como poder de controlar a circulação das próprias informações. Ou seja, este seria o "preço" a ser pago para usufruir desta sociedade da informação (RODOTÁ, 2008, p. 113).

Neste sentido, menciona Stefano Rodotá:

> A contrapartida necessária para se obter um bem ou um serviço não se limita mais à soma de dinheiro solicitada, mas é necessariamente acompanhada por uma cessão de informações. Nessa troca, então, não é mais somente o patrimônio de uma pessoa que está envolvido. A pessoa é obrigada a expor seu próprio eu, sua própria persona, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito (RODOTÁ, 2008, P. 113).

A proteção da pessoa humana é o ideal máximo do ordenamento jurídico norteado pela Constituição Federal, e o Direito Fundamental à Privacidade é uma das facetas da Dignidade da Pessoa Humana, reconhecido inclusive na Declaração Universal da ONU em seu artigo 1º (SARLET, 2015, p. 50). Canotilho descreve a noção nuclear da dignidade da pessoa humana como sendo *"indivíduo conformador de si próprio e da sua vida segundo o seu próprio projecto espiritual (plastes et fictor)"* (CANOTILHO, 2003, p. 225).

Esta importante definição serve como norteador da problemática hoje vivenciada, onde a tecnologia e as mudanças sociais traçam um novo cenário no qual a informação pessoal e a privacidade dividem uma tênue linha. O direito fundamental à

privacidade se vê diante dos mais variados desafios para a sua tutela, ainda mais quando analisado sob a ótica da proteção de dados pessoais.

Nesta perspectiva, um instituto fundamental é o consentimento para o tratamento de dados pessoais. Segundo Danilo Doneda, em sua obra *Da Privacidade à Proteção de Dados Pessoais*:

> Através do consentimento, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos deste consentimento à natureza dos interesses em questão (DONEDA, 2006, p. 371).

Ocorre que não podemos desconsiderar que estamos diante de um sistema patrimonialista, no qual os dados pessoais podem se transformar em uma *commodity* nesta nova sociedade digital. Saber usar do consentimento e dar a este as vestes de um ato unilateral, não podem ser pressupostos de uma ausência de interesse na proteção de dados pessoais.

Os atuais avanços tecnológicos trazem consigo inquestionáveis ganhos e benefícios para toda a sociedade. Porém, em contrapartida, também implicam em grandes riscos para os direitos fundamentais e para a proteção de dados pessoais. O acesso à internet tornou-se, nos dias de hoje, um direito fundamental a liberdade de expressão e informação. A vida sem internet não seria mais possível (PIÑAR MAÑAS, 2017, p. 60).

Por outro lado, o que também parece inquestionável, seria o direito de viver sem internet, estando certo que quem opta por exercer este direito, também deve estar ciente do que está abrindo mão e das possibilidades que não terá acesso.

Ocorre que, cada vez estamos mais conectados e transmitindo mais dados na rede e não se pode desconsiderar o grande ganho que estas trocas podem trazer para a sociedade como um todo. Quem não gostaria de viver em uma cidade mais segura, mais acessível, mais inteligente e conectada com as suas necessidades?

Exatamente neste sentido, José Luis Piñar Mañas menciona que as cidades inteligentes são aquelas que se valem da inovação tecnológica para oferecer um entorno mais habitável à população. E mais, salienta que *"las ciudades inteligentes no son viables sin el tratamento massivo de información, tanto publica como la que afecta a las personas em particular."* (PIÑAR MAÑAS, 2017, p. 69).

Buscando viabilizar e regularizar esta situação que, diga-se de passagem, é inevitável, o Parlamento Europeu e o Conselho emitiram o Regulamento 2016/679 que

entrou em vigor desde de 25 de maio de 2018. Tal norma incorpora a evolução tecnológica e a globalização como pontos de partida e introduz um novo modelo de proteção de dados, trazendo uma gestão e uso responsável da informação (RUARO; MOLINARO, 2017, p. 30).

O avanço trazido por esta norma para o modelo europeu de gestão e proteção de dados é inquestionável e coloca a União Europeia em um novo patamar em relação a este assunto.

1.O NOVO REGULAMENTO EUROPEU

1.1. Histórico e evoluções conceituais até a publicação do RGPD

O novo regulamento geral de proteção de dados pessoais passou a ser aplicável no dia 25 de maio de 2018, sendo obrigatório todos os seus elementos e diretamente aplicável a cada Estado membro da União Europeia. Como diz José Luis Piñar Mañas, passa-se de uma gestão de dados ao uso responsável da informação e tal afirmativa vai muito mais além. Passará a se apreciar as questões através do princípio de accountability (art. 24 do RGPD)[1], ou seja, uma responsabilidade proativa, com princípios que vão desde a privacidade por desenho e padrão (artigo 25 do RGPD)[2] até a figura de um Delegado de proteção de dados (PIÑAR MAÑAS, 2016, p. 16).

[1] Artigo 24. Responsabilidade do responsável pelo tratamento
1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.
2 Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.o 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.
3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40.o ou de procedimentos de certificação aprovados conforme referido no artigo 42.o pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

[2] Artigo 25. Proteção de dados desde a concepção e por padrão
1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por padrão, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento.

A rápida evolução tecnológica e a globalização trouxeram novos paradigmas para a proteção de dados pessoais, transformando tanto a economia, como a vida social, sendo imprescindível que para isso haja uma circulação de dados pessoais entre os países membros, assim como entre outros países e organizações internacionais, sem que para isso se perca o nível de proteção destes dados (PIÑAR MAÑAS, 2016, p. 51).

A base e avanço de toda a legislação europeia está calcada no artigo 8º da Carta Europeia de Direitos Humanos, o qual reconhece o direito fundamental a proteção de dados. Este direito foi elevado a categoria de direito fundamental autônomo, separado, inclusive, do direito à intimidade, que está previsto no artigo 7º. Este grande avanço ocorrido nos anos 2000, fundamentou e embasou o Novo Regulamento Europeu de Proteção de Dados, que busca superar as dificuldades de uniformização e aplicação vividos durante a vigência da Diretiva 95/46/CE.

A visão trazida pelo RGPD reforça que o tratamento de dados pessoais deve servir à humanidade, porém tal direito não é um direito absoluto e, portanto, deve ser considerado em relação a sua função com a sociedade e manter sempre o equilíbrio com os demais direitos fundamentais, baseado no princípio da proporcionalidade (PIÑAR MAÑAS, 2016, p. 57).

Outro ponto importante a ser considerado como conceito e fundamento do Novo Regulamento, diz respeito a qual seria a definição do direito a proteção de dados. Tal definição não está prevista no Regulamento, mas segundo Piñar Mañas, poderia ser entendida como o controle que as pessoas físicas devem ter sobre seus dados pessoais, sendo este controle, o elemento central do direito (PIÑAR MAÑAS, 2016, p. 57).

Assim, o objetivo final do Novo Regulamento está em regular o direito fundamental a proteção de dados reconhecido no artigo 8º da Carta Europeia de Direitos Humanos e garantir a livre circulação destes dados dentro da união Europeia.

1.2.Principais Alterações do Regulamento 2016/679 da UE

Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por padrão, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.os 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.o.

Um dos principais conceitos para estudar esta legislação está no que são **dados pessoais**. O conceito trazido pela Diretiva 95/46/CE foi mantido pelo Novo Regulamento, porém agregaram-se novos elementos e exemplos, pertinentes ao desenvolvimento de novos aplicativos e da internet das coisas. Assim, pode-se definir como dados pessoais toda informação sobre uma pessoa física identificada ou identificável, devendo considerar-se pessoa física identificável toda aquela que puder ser determinada, direta ou indiretamente. O RGPD especificou ainda mais tal conceito, mencionando que seriam considerados como dados identificáveis o nome, o número de identidade, dados de localização, dados em linha ou ainda vários elementos próprios de sua identidade física, fisiológica, genética, psíquica, econômica, cultural ou social (POU, 2016, p. 117).

O regulamento também clarifica esta informação sobre pessoa identificável, deixando evidente que não se considera identificável uma pessoa que tal identificação necessite de prazos ou atividades desproporcionais. A identificação deve ser algo mais imediato e que não requeira grandes esforços (POU, 2016, p. 119).

Contudo, como há muito já vem sendo dito, o problema não está nos dados em si, mas no seu tratamento. O conceito de **tratamento** foi mantido o mesmo já tido pela Diretiva 95/46/CE, porém agregou o conceito de limitação, que faz referência a dados pessoais que são coletados, porém possuem uma limitação de tratamento.

Outra significativa alteração feita pelo Regulamento está no ato do **consentimento,** que incorporou ao seu conceito de livre manifestação de vontade, específica e informada a manifestação de vontade inequívoca. Aqui altera-se um parâmetro de consentimento "padrão", que por muitas vezes era dado sem que o usuário tivesse de fato consentido, já que uma simples marcação em uma janela de sítio era tida como consentimento.

Agora exige-se um consentimento claro, inequívoco, com uma linguagem fácil e acessível, de compreensão rápida, não podendo conter cláusulas abusivas. Ainda, tendo o tratamento de dados mais de um fim, o consentimento deve ser dado de forma separada, para cada um dos fins projetados e o responsável do tratamento deve ser capaz de demonstrar que foi dado o consentimento por determinada pessoa para determinado fim.

O Novo Regulamento ainda traz conceitos como a "pseudonimização", baseado no princípio da minimização dos dados; a violação de segurança dos dados e a necessidade de informação à autoridade de controle com o objetivo de preservar maiores danos e prejuízos às pessoas físicas donas destas informações; e o conceito de

estabelecimento principal, que decide sobre a finalidade e meios de tratamento destes dados, devendo este local ser considerado o principal.

Outro assunto de grande importância está na **transferência de dados pessoais a terceiros países (fora da comunidade europeia) e organizações internacionais,** matéria esta regulada pelo Capítulo V, artigos 44 a 50 do RGPD. O principal ponto em relação a esta matéria é que as transferências de dados para fora do da União Europeia não podem colocar em risco o nível de proteção já garantido às pessoas físicas em relação aos seus dados pessoais.

Para viabilizarmos a transferência internacional a um terceiro país ou organização internacional, deverá basear-se em uma decisão de adequação, com garantias efetivas e notórias aos dados ou, que esteja enquadrado em uma das exceções previstas no artigo 49 do RGPD (PIÑAR MAÑAS, 2016, p. 450).

O Novo Regulamento atribui a competência para declarar adequado o grau de proteção dado por determinado país fora da União Europeia ou organização internacional sobre o controle de dados pessoais, a uma Comissão. Porém, com o objetivo de auxiliar o trabalho desta Comissão, o Regulamento prevê em seu artigo 70.1 que o Comitê facilitará o trabalho da Comissão, emitindo um parecer para avaliar o nível de proteção de onde se pretende autorizar a transferência internacional de dados.

A consequência mais importante sobre esta decisão de adequação está na autorização para que a transferência seja feita a quem solicitou, não necessitando de nenhuma autorização específica. Além disso, tal decisão obriga, de outra parte, o acompanhamento e supervisão por parte da Comissão de maneira contínua sobre os acontecimentos e desdobramentos de tal decisão. Haverá uma revisão sobre a decisão a cada quatro anos, pelo menos, com o objetivo de constatar se os níveis de proteção seguem estando adequados aos parâmetros estabelecidos pela Comissão (PIÑAR MAÑAS, 2016, p. 444).

Não sendo constatada a manutenção da proteção dos dados pessoais nestes critérios, a Comissão revogará, modificará ou suspenderá a decisão anterior, proibindo a transferência de dados pessoais, não havendo efeito retroativo desta decisão.

Na falta de uma decisão de adequação, de acordo com o artigo 46.1, o responsável ou o encarregado do tratamento só poderá transmitir dados pessoais a um terceiro país ou organização internacional se estes oferecerem garantias adequadas e uma condição de que os interessados contem com direitos exigidos e ações legais efetivas (PIÑAR MAÑAS, 2016, p. 447). O artigo 46.2 segue nesta linha e esclarece o que seriam

garantias adequadas: instrumento juridicamente vinculante e exigível entre as autoridades e organismos públicos, normas corporativas vinculantes, cláusulas de proteção de dados adotadas pela Comissão, cláusulas de proteção de dados adotadas por uma autoridade de controle e aprovadas pela comissão, código de conduta e um mecanismo de certificação associado a compromissos vinculantes e exigíveis nos mesmos termos que os códigos de conduta.

Todas estas alternativas possibilitam a transferência de dados pessoais para países fora da Comunidade Europeia sem a necessidade de uma decisão de adequação expressa, responsabilizando o encarregado e o responsável do tratamento de dados por tudo que envolva esta transferência.

Ainda sobre este tema, as **normas corporativas vinculantes,** também conhecidas como Binding Corporate Rules (BCR's) requerem uma atenção especial. Estas normas são um elemento legitimador das transferências internacionais de dados dentro de um grupo empresarial, ou uma união de empresas, embasando políticas de proteção de dados pessoais sob a responsabilidade do encarregado de tratamento, que permitam sua proteção para além das fronteiras Europeias (POU, 2016, p. 131).

As BCR's são consideradas fontes de obrigação para os responsáveis e encarregados da proteção de dados pessoais e possuem caráter vinculante enquanto declaração unilateral de vontade. Contudo, justamente ciente de que tais regras poderiam gerar problemas de aplicação, o RGPD reconhece esta regulação e prevê em seu artigo 47.1 os seus requisitos, garantindo que a autoridade de controle competente aprovará normas corporativas vinculantes sempre que forem juridicamente vinculantes e se apliquem e sejam cumpridas por todos os membros do grupo empresarial, inclusive seus empregados; confiram expressamente aos interessados direitos exigíveis em relação ao tratamento de seus dados pessoais e cumpram o apartado 2, que regula o que é considerado conteúdo mínimo para as BCR's (PIÑAR MAÑAS, 2016, p. 452).

O grande objetivo do legislador europeu foi de que as BCR's de fato garantissem o direito a proteção de dados pessoais, considerando o complicado e complexo panorama mundial que a cada dia realiza mais transferências internacionais. Exatamente em virtude disso, o legislador traz no artigo 47.2 o que deve contar nestas normas corporativas vinculantes, não deixando espaço para subjetividade. Após elaboradas pelo responsável de dados do grupo econômico, este deve submeter a aprovação à autoridade de controle competente.

Em um mundo globalizado como vivemos hoje em dia, imprescindível que toda e qualquer empresa que mantenha relações, ou pense em manter, com cidadãos ou empresas europeias, busque adequar-se de forma antecipada ao que diz o presente regulamento, pois do contrário pode estar sujeito a altas multas que podem chegar até 20.000.000,00 de euros ou 4% do volume de negócios total anual da empresa.

Por fim, e não menos importante, imprescindível tecermos algumas considerações sobre o direito de retificação, cancelamento, oposição e decisões individuais automatizadas; direito ao esquecimento e ao direito da portabilidade dos dados. Tais direitos apenas reforçam o controle do indivíduo sobre os seus próprios dados pessoais, modificando os tradicionais direitos ARCO do cidadão (acesso, retificação, cancelamento e oposição) e agregando os novos direitos acima mencionados.

O direito de retificação constou no RGPD de forma muito similar ao que já estava previsto na Diretiva 95/46/CE. Já o direito ao cancelamento passou a ter a denominação de direito à supressão, com um contexto mais amplo que o tradicional direito ao cancelamento, incluindo inclusive a supressão em buscadores de internet, o qual veio a denominar-se direito ao esquecimento.

O direito ao esquecimento nada mais seria que um avanço ao direito de supressão e oposição, sendo a manifestação destes direitos já existentes. Este direito permitirá na prática, por exemplo, que usuários de rede sociais ou qualquer outro serviço da sociedade da informação, como sites de compras online, suprimam os seus dados pessoais quando do encerramento da conta (ÁLVARES CARO, 2016, p. 255).

Com o direito ao esquecimento, o RGPD reforça, mais uma vez, a sua posição sobre o maior controle do cidadão sobre seus próprios dados, fortalecendo o princípio da finalidade, qualidade e minimização de dados, os quais estavam em aberto desde a Diretiva 95/46/CE.

Outro importante avanço está em relação às decisões automatizadas individuais. De acordo com o novo regulamento, o interessado deve ter o direito de não ser objeto deste tipo de decisão. Um exemplo disso seria a negativa de crédito automática, baseada exclusivamente em informações da rede, sem qualquer intervenção humana.

O RGPD permite decisões deste tipo, inclusive elaboração de perfis, desde que sejam necessárias para a celebração ou execução de um contrato entre interessado e o responsável do tratamento de dados, ou se houver consentimento específico do interessado. Porém, mesmo assim serão necessárias várias garantias, dentre elas o direito de receber intervenção humana por parte do responsável, direito que o interessado

expresse seu ponto de vista ou ainda direito a impugnar a decisão, sendo vedada este tipo de decisão quando envolver menores.

Por fim, o RGPD trouxe um novo direito consigo, o direito à portabilidade. Este direito reforça mais uma vez o poder de disposição de dados dos cidadãos e também fomenta a competência do mercado digital. Através da portabilidade será possível receber os dados pessoais armazenados em formato estruturado, de uso comum e de leitura mecânica, possibilitando sua transferência para outro responsável. O RGPD reforça que isso só será possível quando for tecnicamente viável e coloca que o prazo para atendimento será de um mês, a partir do pedido, podendo ser prorrogado em certos casos. Este direito será exercido a título gratuito, excetuando-se os pedidos manifestamente infundados ou excessivos (FERNÁNDEZ-SAMANIEGO; FERNÁNDES-LONGORIA, 2016, p. 262).

As alterações acima trazidas sugerem o grande reforço à proteção de dados que o Regulamento Geral de Proteção de Dados Pessoais 2016/679 trouxe para o mundo digital. Os princípios basilares da Diretiva 45/96/CE foram todos mantidos e ampliados neste grande avanço legislativo sobre o tema, enaltecendo o poder do cidadão sobre a gestão efetiva, clara e transparente de seus dados pessoais.

2.COMPLIANCE DIGITAL E RGPD

2.1 Elementos do Programa de *Compliance*

Os programas de *compliance* são utilizados para transmitir aos dirigentes e aos funcionários o conhecimento sobre as leis e demais normas regulamentares, sendo comum a utilização de uma monitoração sistêmica, baseada em padrões pré-definidos, utilizando-se de investigações internas e privadas para avaliação de eventuais irregularidades praticadas no âmbito empresarial.

A modernidade avançada e a produção social de riquezas vieram acompanhadas da produção social de riscos, coincidindo num novo paradigma: como se poderia evitar/minimizar riscos e/ou perigos produzidos por um processo avançado de modernização, sem ultrapassar os limites do sustentável (BECK, 1998, 25)?

A ruptura paradigmática com ideia de dano, mediante uma concepção preventiva e do papel do Direito na prevenção de ilícitos, reclama a participação dos operadores

jurídicos em um novo horizonte de sentido, a partir de uma ética da responsabilidade (JONAS, 2006, p. 160).

A palavra *compliance* vem do verbo em inglês *to comply*, que significa "cumprir", "estar de acordo". É uma prática empresarial que impõe padrões internos para o cumprimento de normas, observância de leis e diretrizes nacionais e internacionais. O sistema de autorregulação adotado por organizações empresariais, normalmente, é composto por um programa de *compliance* para detectar operações suspeitas e encaminhá-las à supervisão da empresa.

Nesse passo, as principais normas sobre *compliance* são as seguintes :

FCPA - FOREIGN CORRUPT PRACTICE ACT- 1977: Os EUA foram o primeiro país a se comprometer com o combate à corrupção. A FCPA é fruto do escândalo do pagamento de propina pela Empresa de Aeronaves Lockheed Aircraft Corporation a funcionários públicos de vários países, na época da Guerra Fria. A FCPA é aplicável às Empresas americanas e Empresas que queiram se relacionar com os EUA.

LEI SARBANES-OXLEY (Sarbanes-Oxley Act - SOX ou SARBOX) - 2002: Lei americana que define práticas de boa governança corporativa e transparência na condução dos negócios.

UK BRIBERY ACT - 2011: Responsabiliza a Empresa pela falha ao prevenir atos de corrupção, praticados por qualquer pessoa a ela associada, em qualquer lugar do mundo, tanto no setor público, quanto no privado. Há a possibilidade de isentar a empresa de responsabilidade pela existência de procedimentos adequados anteriores ao cometimento do ato ilícito (compliance). A lei inglesa é considerada mais agressiva que a lei americana, por possuir um caráter extraterritorial ainda mais amplo.

CONVENÇÃO DA ONU DE MÉRIDA – 2003 e Decreto 5.687 - 2006: Tem por finalidade promover, facilitar e apoiar, em nível internacional, o controle da corrupção.

A implantação de um programa de integridade impõe a observância de deveres de prevenção e análise de riscos, mediante uma cultura corporativa de transparência nas atividades empresariais.

Para a implementação de um programa de integridade, utilizam-se alguns elementos, tais como: a) criação e informação de um código de conduta, que defina a postura ética empresarial; b) canal de denúncias, que possibilite aos *stakeholders* denunciar atos ilícitos, de forma anônima; c) contratação de um *compliance officer*, o

profissional que será responsável pela informação e fiscalização no cumprimento do programa de integridade.

O *compliance officer* é o responsável pela supervisão e gerenciamento do *compliance* na empresa, ou na administração pública. Pode ser contratado pela própria organização, ou ser profissional terceirizado, ou até mesmo empresa terceirizada para desempenhar tais funções.

A exemplo da figura do *data protection officer* (encarregado pela proteção de dados), conforme se verá adiante, tem a difícil missão de garantir que todos os procedimentos realizados estejam de acordo com o ordenamento jurídico nacional e internacional, bem como, em conformidade com o código de ética e conduta implementado na organização.

Nesta seara, tornou-se imprescindível, tanto para as empresas quanto para a própria Administração Pública, a implantação de um programa de integridade, o *compliance*, para que se adequassem às exigências de mercado nacional e internacional, criando boas práticas de governança corporativa, com impactos na gestão empresarial, sendo mister o estudo do impacto do programa de compliance no âmbito do direito à proteção de dados pessoais.

Conforme vimos acima, as organizações empresariais que não estiverem em conformidade com o RGPD podem sujeitar-se a multas no valor de até 20.000.000,00 de euros, ou 4% do volume de negócios total anual da empresa.

Essas sanções não trazem um impacto negativo apenas financeiro para as empresas. Sem dúvida, atuar em desconformidade com as normas sobre *compliance* e o Regulamento Europeu mancham sua imagem a nível internacional.

Essa situação foi vivenciada, recentemente, pela Empresa Facebook, no escândalo de vazamento de dados para uso político, que fez com que a Empresa perdesse 50 bilhões de dólares em valor de mercado, em apenas dois dias (JORNAL O GLOBO, 2018).

Nas palavras de Aristóteles (ARISTÓTELES, 2009, p. 200), a escolha de nossas ações não será correta sem prudência, nem sem virtude moral, pois a virtude moral nos capacita a atingir o fim desejado e a prudência é o que nos permite adotar o meio certo para atingi-lo. Vale lembrar: a prática da justiça requer o senso da medida.

No âmbito administrativo, a eficácia dos programas de *compliance* está vinculada à governança pública, na perspectiva do princípio da condução responsável dos assuntos do Estado, o que pressupõe "*accountability* (dever de cuidado dos poderes

públicos e o dever de prestar contas) e a *responsiveness* (sintonia profunda da actuação dos poderes públicos com as aspirações dos cidadãos)", no horizonte de uma concepção de "cidadania activa e participativa, e não apenas da cidadania representativa" (CANOTILHO, 2008, p. 327).

Nesse sentido, demanda-se a construção de uma cultura de transparência e *accountability*, com o devido acesso à informação e prestação de contas por parte dos gestores públicos.

Partindo da ideia de mudança de paradigma do dano para o paradigma da prevenção de ilícitos, deve-se considerar a atuação do Direito a frente das contradições sociais, potencializando o acompanhamento das inovações tecnológicas, com a devida segurança jurídica.

2.2 Encarregado pela Proteção de Dados: *data protection officer*

O Regulamento Geral de Proteção de Dados Europeu impacta profundamente o direito digital e o setor da inovação, prevendo direitos e deveres a usuários e prestadores de serviços.

A exemplo do *compliance officer*, o *data protection officer*, que é o encarregado pela proteção de dados, é o responsável por supervisionar o cumprimento por quem trata dados pessoais, servindo, inclusive, para fomentar a efetivação do direito fundamental à proteção de dados. Para sua atuação, é de extrema importância que possua independência, seja no setor público, como no setor privado, para o exercício de suas funções. Pode ser tanto um empregado interno, quanto um consultor externo.

A Diretiva 95/46/CE já previa, de forma limitada, a figura do encarregado pelo proteção de dados. Entretanto, o RGPD oferece uma exposição muito mais detalhada das funções do EPD (encarregado pela proteção de dados), incrementando suas obrigações (GARCÍA, 2016, p. 322).

De acordo com o artigo 37 do RGPD, o "delegado de proteção de dados" será designado atendendo a suas qualidades profissionais e, em particular, os seus conhecimentos especializados em Direito e a prática em matéria de proteção de dados e a sua capacidade para desempenhar as funções (REGULAMENTO (UE) 2016/679, 2018).

Além de ter de cumprir com os critérios previstos no RGPD, é essencial que se trate de uma pessoa com alto nível de experiência profissional, com profundo

conhecimento em direito nacional e europeu sobre proteçao de dados pessoais, que conheça o setor do negócio ou atividade da organização na qual desempenhe suas funções, conheça as operações e tecnologia para tratamento e segurança dos dados (GAYO, 2016, p. 377).

De acordo com o previsto no Regulamento Europeu, é importante considerar os seguintes itens para a designação do encarregado pela proteção de dados: 1) designação obrigatória quando se cumpram os critérios estabelecidos no Regulamento, nos setores público e privado; 2) designação obrigatória em virtude do Direito da União Europeia, como por exemplo, a Diretiva sobre proteção de dados pessoais tratados com fins policiais e judiciais; 3) designação voluntária, sendo necessário neste caso, que o encarregado pela proteção de dados cumpra os requisitos e critérios do regulamento (GAYO, 2016, p. 377).

Portanto, os encarregados de proteção de dados deverão conscientizar, de forma precisa, o que representa o RGPD, os seus contornos e o espírito das suas normas, estabelecendo as condições ideais para a conformidade com o Regulamento.

2.3 Da Proteção de Dados desde o Desenho e por padrão: *privacy by design and by default*

O novo Regulamento Europeu prevê que, desde a concepção (*privacy by design*), de construção de bens, serviços, produtos, sistemas, sejam obedecidos os critérios de privacidade.

De acordo com o artigo 25 do RGPD, o responsável pelo tratamento de dados necessita aplicar, tanto no momento de definição dos meios de tratamento, como no momento do próprio tratamento, medidas técnicas e organizativas adequadas, como a pseudonimização e a minimização (REGULAMENTO (UE) 2016/679, 2018).

A pseudominimização é compreendida como o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico e medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável. A minimização é compreendida como a limitação ao que é necessário, relativamente às finalidades para as quais são tratados os dados.

Essas técnicas são utilizadas para a aplicação e eficiência das garantias necessárias no tratamento, para cumprir os requisitos do RGPD, protegendo os direitos dos titulares dos dados.

Ainda, informa o Regulamento que, por padrão (*privacy by default*), só sejam tratados os dados pessoais que forem necessários para finalidade específica de tratamento. Essa obrigação aplica-se, em especial, para assegurar que os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

2.4 Implicações do RGPD nas Empresas Brasileiras

Visto que o RGPD prevê a necessidade de que todas as Empresas envolvidas com manipulação de dados pessoais dos cidadãos da comunidade europeia tenham de cumprir requisitos, a fim de estarem em *compliance* com o prescrito no Regulamento, é de fundamental importância abordarmos a ressonância do RGPD nas Empresas Brasileiras.

Empresas brasileiras que armazenem e/ou tratem dados pessoais de titulares europeus deverão atentar-se ao RGPD, uma vez que ela se aplica a entidades que processam dados pessoais, mesmo quando o tratamento se dá fora da limitação geográfica da União Europeia, desde que sejam oferecidos bens ou serviços a titulares de dados que sejam cidadãos da comunidade europeia. É o que preceitua o artigo 3º do presente Regulamento (REGULAMENTO (UE) 2016/679, 2018).

Além disso, é válido lembrar que foi sancionada em agosto a Lei 13.709, Lei Geral de Proteção de Dados Pessoais, inspirada no RGPD, que regulamenta o tratamento e a proteção de dados pessoais no Brasil (BRASIL, 2018).

A atual Lei Geral de Proteção de Dados Pessoais exige que os dados só sejam usados e manipulados com autorização, além de estabelecer uma série de restrições em relação a informações consideradas sensíveis, como opção sexual e posição política. O texto também menciona a autoridade nacional de proteção de dados, a qual foi vetada pelo presidente da república quando sancionou a Lei, estando pendente a forma de fiscalização, sanção e orientação à população enquanto não instituída tal autoridade.

Nesse sentido, torna-se imprescindível a implementação de um programa de *compliance* digital, direcionado às questões referentes ao tratamento de dados pessoais no Brasil, em consonância com o RGPD, bem como com o ordenamento jurídico pátrio e demais normas e regulamentos referentes ao tema.

CONCLUSÃO

O Regulamento Europeu de Proteção de Dados influencia não apenas a Comunidade Europeia, como também, ressona em todos os países que tratarem e/ou manipularem dados pessoais de cidadãos europeus.

A atual quadra vivida exige o acompanhamento das empresas para que possam implementar padrões éticos em suas atividades, não apenas por uma questão moral, mas sim, legal.

A gestão de compliance empresarial abarca diversas áreas jurídicas, sendo o objetivo deste trabalho a análise da ressonância do *compliance* no direito digital, mais precisamente, referente ao tratamento de dados pessoais, com a devida observância aos direitos e garantias fundamentais, em suas múltiplas dimensões.

Vale ressaltar que a inobservância dos direitos fundamentais implica na ruptura das legítimas expectativas dos cidadãos e das empresas que pretendem agir com a devida eticidade, exigida no mercado atual.

A eficácia dos direitos fundamentais, tanto nas relações públicas quanto privadas, atua como limite objetivo. O conteúdo da dignidade enuncia a compreensão de que o indivíduo é um fim em si mesmo, vedando-se a sua instrumentalização, o qual não pode ser tratado como meio para a consecução de objetivos ou metas de natureza coletiva.

Por todo exposto, é imprescindível que as organizações empresariais e a administração pública se atentem ao Regulamento Europeu de Proteção de Dados Pessoais, que começou a viger em maio de 2018, de forma a estarem em *compliance* com o que fora ali previsto, evitando riscos e possíveis danos que possam culminar na aplicação de multas gravíssimas e, principalmente, situações que possam ferir a reputação dessas organizações.

REFERÊNCIAS BIBLIOGRÁFICAS

ARISTÓTELES. **Ética a Nicômaco**. 3ª edição. Bauru, SP: Edipro, 2009.

BECK, Ulrich. **La sociedad del riesgo hacia una nueva modernidad.** Barcelona: Paidós, 1998.

BRASIL. Câmara dos Deputados. **Lei 13.709**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 07 setembro 2018.

CANOTILHO, J. J. Gomes. **Direito Constitucional e Teoria da Constituição**. 5. ed., Coimbra: Almedina, 1991.

_____. **Direito Constitucional e Teoria da Constituição**. 7. ed., Coimbra: Almedina, 2003.

_____. **"Brancosos" e interconstitucionalidade: itinerários dos discursos sobre a historicidade constitucional.** 2. ed. Coimbra: Almedina, 2008.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

_____. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico. Joaçaba, v. 12, n. 2, jul/dez. 2011.

GAYO, Miguel Recio. El Delegado de Protección de Datos. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos: hacia um nuevo modelo europeo de privacidade.** Madrid: Editoral Reus, 2016.

GARCÍA, José Leandro Núñez. El Encargado del Tratamiento. In: PIÑAR MAÑAS, José Luis (Dir.). **Reglamento General de Protección de Datos: hacia um nuevo modelo europeo de privacidade.** Madrid: Editoral Reus, 2016.

JONAS, Hans. **O princípio responsabilidade: ensaio de uma ética para a civilização tecnológica.** Tradução Marijane Lisboa, Luiz Barros Montez. Rio de Janeiro: Contraponto: Ed. Puc-Rio, 2006.

JORNAL O GLOBO. **Em dois dias, Facebook perde quase US$ 50 bilhões em valor de mercado.** Disponível em: <https://g1.globo.com/economia/noticia/em-dois-dias-facebook-perde-quase-us-50-bilhoes-em-valor-de-mercado.ghtml>. Acesso em: 20 abril 2018.

PINAR MANAS, Jose Luis. Introducción. Hacia un Nuevo Moledo Europeo de Protección de Datos. **Reglamento General de Protección de Datos – Hacia un nuevo modelo de privacidade.** Editora Reus: Madrid.2016.

RODOTÀ, Stefano. **A vida da sociedade de vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; SOUZA, Fernando Inglez de. **Cenários de regulação da proteção de dados pessoais e os desafios de uma tutela efetiva no ordenamento jurídico brasileiro: a internet e suas implicações na privacidade e na proteção de dados pessoais.** Interesse Público – IP, Belo Horizonte, ano 19, n. 103, p. 197-216, maio/jun. 2017.

_____. **O direito à proteção dos dados pessoais na sociedade da informação.** Revista Direito, Estado e Sociedade. n. 36, jan/jun 2010, p. 178-199.

_____. **Responsabilidade civil do Estado por dano moral em caso de má utilização de dados pessoais.** Direitos Fundamentais e Justiça. Porto Alegre: PUCRS, 2007. Vol.1.

_____; RODRIGUEZ, Daniel P.; FINGER, Brunize. **O direito à proteção de dados pessoais e à privacidade.** Revista da Faculdade de Direito da UFPR. Curitiba: UFPR, 2011.Vol. 53.

_____; MAÑAS, José Luis Piñar, Molinaro, Carlos Alberto (Orgs.). **Privacidade e proteção de dados pessoais na sociedade digital.** [recurso eletrônico] / Regina Linden Ruaro; José Luis Piñar Mañas; Carlos Alberto Molinaro (Orgs.) -- Porto Alegre, RS: Editora Fi, 2017.

PIÑAR MAÑAS, José Luis (Dir.). **Reclamento General de Protección de Datos: hacia um nuevo modelo europeo de privacidade.** Madrid: Reus, 2016.

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. **Regulamento Geral sobre a Proteção de Dados.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679>. Acesso em: 20 abril 2018.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.** 12 ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2015.

_____. **Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988.** 10 ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2004.