PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

LEI GERAL DE PROTEÇÃO DE DADOS

ASPECTOS DA TITULARIDADE DE DADOS E A IMPORTÂNCIA DE UM *DATA PROTECTION OFFICER* EM UMA INSTITUIÇÃO DE ENSINO

ORIENTANDO: SÉRGIO LOPES DE SOUSA

ORIENTADOR - PROF. Dr. JOSÉ QUERINO TAVARES NETO

GOIÂNIA

2020

SÉRGIO LOPES DE SOUSA

LEI GERAL DE PROTEÇÃO DE DADOS:

ASPECTOS DA TITULARIDADE DE DADOS E A IMPORTÂNCIA DE UM *DATA PROTECTION OFFICER* EM UMA INSTITUIÇÃO DE ENSINO

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).
Prof. Orientador: Dr. José Querino Tavares Neto

GOIÂNIA

2020

SÉRGIO LOPES DE SOUSA

LEI GERAL DE PROTEÇÃO DE DADOS

ASPECTOS DA TITULARIDADE DE DADOS E A IMPORTÂNCIA DE UM *DATA PROTECTION OFFICER* EM UMA INSTITUIÇÃO DE ENSINO

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador: Prof. Dr. José Querino Tavares Neto Nota

_____

Examinador Convidado: Prof. Ms. Elias Batista Ferreira Nota

Dedico este breve estudo a minha querida família, em especial aos meus pais, Francisco Lopes e Antônia Nogueira.

A minha esposa Irene Teixeira de Moura e as minhas filhas Anna Clara e Yasmim.

Aos meus irmãos Cesár, Calebe, Mariele, Marivone e Josué.

A minha avó Dona Chaguinha “in memorian’

Ao meu orientado Professor Doutor, José Querino Tavares Neto, por toda sua dedicação no auxílio prestado a produção deste artigo, assim como pela sua paciência na correção e empenho nas orientações.

Aos amigos que fiz no ambiente acadêmico, os quais jamais sairão do meu ciclo de amizade.

A todos os professores que tive o privilégio em conhecer, os quais contribuíram para elevar meu conhecimento ao longo desses cinco anos de curso, em especial ao professor Elísio Miranda, que me fez acreditar nas ferramentas que temos no Direito.

Agradeço a Deus pelo sopro de vida, por ter me guiado em todos os meus caminhos e dado provimento a todas as minhas necessidades.

SUMÁRIO

LEI GERAL DE PROTEÇÃO DE DADOS

ASPECTOS DA TITULARIDADE DE DADOS E A IMPORTÂNCIA DE UM *DATA PROTECTION OFFICER* EM UMA INSTITUIÇÃO DE ENSINO

Sérgio Lopes de Sousa[1]

RESUMO

O presente estudo trouxe, em primeiro plano, uma visão ampla, porém sucinta da Lei Geral de Proteção de Dados no Brasil, realçando a figura do *Data Protection Officer – DPO* no processo de tratamento e fiscalização de dados pessoais. Após apresentação da LGPD, com destaque para seu processo histórico, o qual passa pelo Marco Civil da Internet, Lei 12.965/2014, foi pontuado os principais princípios a serem tutelados pelo Estado, no âmbito do direito digital, sendo estes a intimidade e a privacidade. Ainda foi pontuada a classificação dada pela aludida Lei referente a dados sensíveis e não sensíveis. Recortou-se no contexto apresentado o enfrentamento a violação de dados pessoais, sendo destacado um caso concreto referente a um vazamento de dados de uma Instituição de Ensino Superior no Brasil. Sem a pretensão de esgotamento do tema, deu-se enfoque ao papel do DPO e sua atuação como encarregado de efetivar as normas impostas pela Lei, ou seja, buscando a garantia que dados pessoais de clientes não sejam expostos indevidamente, bem como prestar informação a Autoridade Nacional de Proteção de Dados – ANPD, órgão federal responsável pela fiscalização de empresas, no que se refere aos dados de terceiros. Para tanto, recorremos à metodologia diversificada, materializada na pesquisa bibliográfica, documental e jurisprudencial para que, ao final, a partir desta análise doutrinária apresentada fosse possível reconhecer a importância de um profissional especializado para a segurança tanto da empresa, quanto do cliente.

Palavras-chave: Segurança. Dados Pessoais. *Data Protection Officer*. Privacidade. Intimidade.

[1] Acadêmico do Curso de Direito da Pontifícia Universidade Católica de Goiás, sergiaogyn@gmail.com

INTRODUÇÃO

Durante o processo evolutivo da sociedade contemporânea os direitos individuais se vincularam a proteção da pessoa ou de seus bens, estes derivados do direito a propriedade. Todavia, a dimensão da proteção pessoal de um cidadão se altera ou se alarga no transcurso do tempo, devido às mudanças ocorridas no cenário político, social e econômico.

Quando tais transformações acontecem se faz necessário reavaliar o bloco de direitos tutelados pelo Estado, a fim de garantir a proteção integral de seus cidadãos. Nesta esteira, considerando o avanço tecnológico da atualidade, o Direito se vê ante a uma nova fronteira, a Era Digital.

Nesse contexto, a partir de uma análise da mudança de paradigma jurídico-social, o presente estudo tratará da Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais - LGPD e suas implicações no cenário atual, no que se refere à segurança de dados pessoais de terceiros quando estes são entregues a empresas.

Objetivando detalhar a importância de se regulamentar as novas práticas do mundo digital, a LGPD instituiu uma série de medidas e sanções a serem aplicadas aquelas empresas que infringirem seu regulamento. Criando, inclusive, uma nova profissão, o *Data Protection Officer- DPO,* responsável pelo tratamento de dados pessoais e fiscalização da correta aplicabilidade da LGPD nas empresas, tanto públicas, quanto privadas, entre outros pontos relevantes.

Nesse sentido, visando apontar os benefícios e a importância de se ter um profissional DPO em seu quadro de funcionário, o presente estudo avaliará algumas das possibilidades apresentadas pela doutrina na construção desta nova função, a fim de priorizar o interesse do cidadão e garantir a efetividade dos princípios constitucionais da intimidade e privacidade da pessoa.

Nesta feita, na primeira seção deste estudo será apresentado o contexto legal onde se amparou a elaboração da LGPD, bem como suas principais diretrizes, em especial os limites e responsabilidades de cada ator garantidor da segurança de dados pessoais. Para tanto, será apresentado o processo evolutivo até a vigência da aludida Lei, passando pelo Marco Civil da Internet, instituído em 2014.

Na segunda seção serão tratados os riscos e as preocupações naturais que se deve ter ao se utilizar a rede de computadores, destacando a importância do fator ‘consentimento’ para a utilização de dados pessoais por terceiros, bem como a classificação de dados como sensíveis e não sensíveis, a fim de se garantir maior proteção

Na última seção se apresentará especificamente a função de um *Data Protection Officer -DPO* e sua relevância dentro de uma Instituição de ensino. Objetivando trazer a experiência para o campo da realidade será apresentado um caso concreto, onde a não observância de leis protetivas de dados levou ao prejuízo milhares de pessoas.

Nesse diapasão, em razão da complexidade do tema exposto, principalmente por sua recente vigência e muitos pontos ainda a serem esclarecidos, bem como as consequentes e inevitáveis discussões a respeito de sua eventual funcionalidade, a Lei 13.709/2018 se tornou objeto relevante de estudo para o Direito.

1- LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS Nº 13.709/18

A Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais, foi sancionada pelo então presidente Michel Temer, em agosto de 2018, com o objetivo de regulamentar a proteção e o uso de dados pessoais em todo o território nacional, seja no âmbito público ou privado. Já em seu primeiro artigo a referida Lei preconiza:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018).

A temática da proteção de dados pessoais se moldou em meio ao avanço da tecnologia digital a qual é responsável pela alteração das relações sociais no mundo moderno. A tecnologia suprimiu distâncias com a implementação de cabos ópticos e a informação se encontra no espaço de um click.

A Era Digital trouxe ao homem possibilidades exponenciais de crescimento e de desenvolvimento, fomentando a economia, gerando novas profissões e revolucionando a noção de tempo e espaço.

Não obstante, a rapidez e a evolução tecnológica vieram acompanhadas de inúmeros problemas e consequências pejorativas aos indivíduos, principalmente no âmbito dos direitos referentes a personalidade, sendo que muitas dessas demandas ainda não foram solucionadas pela sociedade contemporânea.

O uso indevido da internet para fins criminosos, por exemplo, fez nascer uma legislação específica para punir eventuais transgressores. Mas, mesmo quando o uso impróprio da tecnologia digital não incorra em crimes passiveis de sanção penal, tem-se presente outros prejuízos como, por exemplo, a exposição excessiva da vida íntima por meio das redes sociais, o que leva a pensar que para muitos a internet virou um grande reality show.

1.1 Contexto Legal

Cabe destacar em breve síntese histórica a evolução do Direito pátrio até a implementação de normas legais protetivas e regulamentadoras do uso de dados pessoais. Nessa linha, o Marco Civil da Internet no Brasil se deu a partir da Lei nº 12.965/2014, contudo, em que pese tenha sido a referida Lei reconhecida como pioneira no mundo no que tange a proteção de dados, sua principal função foi estabelecer diretrizes para a elaboração de uma lei de proteção específica, o que somente veio a ocorrer em julho de 2018, com a Lei Geral de Proteção de Dados – LGPD.

> A LGPD se originou do Projeto de Lei da Câmara de Deputados de nº 53, de 2018, de iniciativa do Deputado Federal Milton Monti (PR/SP). Durante o período de trâmite, foram realizadas duas consultas públicas em que houve mais de 2.500 contribuições de atores nacionais e internacionais (AGÊNCIA SENADO, 2018).

A LGPD, originalmente, previa uma *vacatio legis* de 18 meses, sendo adiada sua efetividade por seis meses, por força da Medida Provisória nº 869/2018.

Atualmente ainda espera por sanção ou veto presidencial, após sua aprovação pelo Senado Federal, o que ocorreu no dia 26 de agosto de 2020.

Ressalta-se que as sanções impostas pela Lei às empresas que a descumprirem somente passarão a ser aplicadas a partir de 1º de agosto de 2021, devido ao período de adequação imposto no texto legal.

Um dos principais problemas a ser enfrentado pelo LGPD se converge para a constante violação da privacidade e intimidade do outro, em razão do uso indevido de dados pessoais alheios por diferentes espectros sociais, o que inclui até mesmo corporações e órgãos governamentais. Nesse sentido, analisa Santos e Araújo (2017, p 171):

> O ambiente da internet trouxe inúmeros desafios como a preservação da liberdade de expressão, a proteção da personalidade, a dificuldade de armazenamento de dados privados disponíveis na web, como fotos, textos, vídeos, a regulação das relações comerciais, a proteção dos direitos autorais, o anonimato para causar danos ou prejuízos a outros, as inúmeras fraudes para obtenção de vantagem, os danos causados pelos vírus, furto de dados mediante fraude.

A falta de uma legislação específica que tratasse da matéria e a ocorrência constante de casos de violação à intimidade e a privacidade das pessoas impulsionou legislativo, muito em razão da pressão popular, a criar normas reguladoras.

Recorda-se que quando surgiu internet havia uma grande preocupação em impor limites ao fluxo e ao conteúdo das informações que iriam circular na rede de computadores, bem como a não obstrução da liberdade de expressão.

Entretanto, ante a ausência de normas estatais, a iniciativa privada passou a disponibilizar e a recorrer a protocolos como os TCP/IP[2] e os Comitês Gestores da Internet a fim de garantirem segurança na circulação de dados.

Quando ocorria afronta no âmbito virtual a algum direito tutelado pelo Estado, o ordenamento jurídico interno se valia das legislações esparsas já existentes, como o Código de Defesa do Consumidor e o Código Civil para julgar esses casos específicos. As autoras Santos e Araújo (2017, p 171) destacam que:

[2]É um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem de dois protocolos: o TCP (*Transmission Control Protocol*) e o IP (*Internet Protocol*). Pode ser visto como um modelo de camadas, onde cada uma é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas estão mais perto do usuário, chamada camada de aplicação e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração

> As problemáticas ocorridas nesse ambiente, como a violação de dados, privacidade e as tentativas de limitação da liberdade de expressão recebiam críticas e tentativas de solução alicerçadas na ideia de direitos civis do indivíduo da sociedade liberal, ignorando totalmente a dimensão coletiva da sociedade de redes.

Por certo, a conexão virtual desencadeou uma gama de desafios a sociedade moderna e escancarou a urgência de um direito positivado garantidor de regras e princípios para a atuação no ambiente digital preservando a liberdade de expressão, tanto quanto a intimidade e a privacidade de seus usuários. Além, é claro, de impor sanções aqueles que se apropriassem de dados disponíveis na rede para realizarem fraudes ou qualquer tipo de dano ou prejuízo.

1.2 Princípios pertinentes: Intimidade e Privacidade

No Brasil, o Marco Civil da Internet ocorrido em 2014 foi festejado por muitos que acreditaram que se estaria construindo uma nova Constituição da internet ou, ainda, a Carta de Direitos dos internautas, ao assegurar direitos e liberdades dos usuários, proteger a liberdade de expressão, a privacidade, a proteção dos dados e a cidadania e a participação no mundo digital. (SANTOS, ARAÚJO, 2017, p 168).

Entretanto, percebe-se que a tão sonhada proteção não foi eficaz ante aos exponenciais casos de violação a privacidade e a intimidade e as inúmeras fraudes realizadas na rede e, mais uma vez, o ordenamento jurídico apresenta por meio da LGPD uma resposta no sentido de regular o uso, restringir e punir aqueles que violarem direito de terceiros no ambiente virtual.

A LGPD estabelece de modo claro as atribuições, as responsabilidades e as penalidades para aqueles que infringirem a Lei, aplicando multas que pode chegar a 50 milhões de reais por incidente, como dita o artigo 52, II, da LGPD.

De fato a Era Digital trouxe consigo a preocupação em manter garantias fundamentais estabelecidas no artigo 5º, inciso X, CRFB/88, o qual preleciona que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas,

assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Observa-se que tais direitos não estão expressos apenas na Constituição Federal brasileira, mas, também em leis infraconstitucionais, assim como em tratados internacionais dos quais o Brasil é signatário, como leciona Gonçalves (2018, p. 79):

> O princípio do respeito pela vida privada e familiar encontra-se consagrado, desde logo, no art. XII da Declaração Universal dos Direitos do Homem, segundo o qual 'ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação' (sic). Este artigo remata dizendo que 'toda a pessoa tem direito à proteção da lei contra as interferências ou ataques' (sic). Em termos similares, o art. 8.º, n. 1, da Convenção Europeia dos Direitos do Homem (CEDH) dispõe que 'qualquer pessoa tem direito ao respeito pela sua vida privada e familiar, do seu domicílio e da sua correspondência' (sic), acrescentando no n. 2 que 'não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros' (sic).

Quando se trata do direito à intimidade, normalmente, se tem a ideia de que algumas ações individuais devem ficar longe do conhecimento público, resguardando o autor o seu direito de realizar escolhas e estabelecer comportamentos sem que outras pessoas interfiram. Assim, a intimidade se relaciona a esfera particular, a qual deve ser protegida para que terceiros não opinem, repreenda ou intervenha a respeito de qualquer atitude do outro.Com relação à privacidade, Silva (2009, p.206) afirma se tratar do:

> Conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito. Embarca todas as manifestações das esferas íntimas, privadas e da personalidade, que o texto constitucional consagrou. A esfera de inviolabilidade, assim, é ampla, abrange modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo.

Ocorre que o mundo tecnológico escancarou a vida íntima e privada das pessoas, fato este, em certa medida, reforçado pelo mercado de produtos midiáticos, incentivador da alta exposição pessoal. De um lado o mercado em busca de usuários, de outro uma sociedade carente de exposição, disposta a apresentar uma imagem

virtual que, por vezes em nada condiz com a realidade vivida. É neste paradoxo que se apresenta uma das grandes dificuldades da atualidade, o limite para se verificar uma violação a privacidade e a intimidade de alguém e a mera exposição pessoal.

As informações disponíveis em bancos de dados conectados a uma rede de computadores se tornaram um espaço fragilizado justamente por conter informações de todos os níveis de conhecimento. De acordo com Santos e Araújo (2017, p. 174) “com as novas ferramentas tecnológicas, seja na Internet ou nos espaços físicos, as condutas passam a ser registradas com mais facilidade e os registros divulgados rapidamente.”

Parte desta reflexão a importância de compreender o direito à privacidade e a intimidade na era digital, uma vez que o desenvolvimento tecnológico e o acesso descontrolado às mídias virtuais em nível global tornaram os conceitos e as soluções aplicadas até então, obsoletos, configurando-se indispensável à realização de estudos e ponderações que levem em considerações tais mudanças.

Assim, faz-se latente a necessidade de conformação do uso de dados na internet com a proteção dos direitos fundamentais presentes em documentos jurídicos internacionais, bem como na Constituição brasileira.

Essa tênue linha que separa o acesso a dados de terceiros da violação ao bloco de direitos ligado a personalidade já foi objeto de debate jurídico interno. A Suprema Corte brasileira ao se manifestar a respeito atestou que a proteção à intimidade e à vida privada não tem caráter absoluto. Por meio da ADIn 2937/2012, o Tribunal Pleno, tendo como relator o Ministro Cézar Peluso, dispôs que “De todo modo, no que concerne ao alegado desrespeito a direitos e garantias individuais, anoto que, sobre não se revestirem de caráter absoluto, como já afirmado (…)”.

Destaca-se que a maioria dos acórdãos que envolvem a questão da intimidade e da vida privada são relativos a uma colisão entre o direito à intimidade e outro direito constitucional fundamental, como o direito a liberdade de expressão, por exemplo, tendo, em regra, o princípio da proporcionalidade como medida de ponderação.

A Constituição brasileira assegura reparação indenizatória pelo dano material ou moral causado pela violação do espaço privado. O Superior Tribunal Federal ao tratar do tema fundamentou na ADPF 130, de relatoria do Ministro Carlos Britto da seguinte forma:

> Com efeito, de um lado, a Constituição, nos arts. 5.º, incs. IV e IX, e 220 garante o direito coletivo à manifestação do pensamento, à expressão e à informação, sob qualquer forma, processo ou veículo, independentemente de licença e a salvo de toda restrição ou censura. De outro, nos art. 5.º, incs. V e X, a Carta Magna garante o direito individual de resposta, declarando, ainda, inviolável a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização por dano moral ou material decorrente de sua violação.

Para Silva (2015, p. 210) o direito a reparação respalda o indivíduo, pois: "(...) é a condição de expansão da personalidade. Para tanto, é indispensável que a pessoa tenha ampla liberdade de realizar sua vida privada, sem perturbação de terceiros."

Por certo a Lei nº 13.709/18 virá para definir limites e responsabilidades acerca de direitos fundamentais, como a liberdade de expressão, a privacidade e a intimidade, em razão do tráfego crescente e dos riscos de ataques e vazamentos de dados que afetam praticamente toda a iniciativa pública e privada, assim como todos os usuários particulares da internet.

A partir de sua vigência o direito interno deixará, em regra, de recorrer às normas esparsas para punir quem se utilizar de maneira irregular da rede de computadores. A Lei nº 13.709/18, também regulamentará uma gama de serviços disponibilizados por servidores e empresas do ramo, ainda carentes de disposições legais. Observa-se que a complexidade e a rapidez da internet são um desafio para ordenamento jurídico pátrio, contudo disciplinar permite maior proteção a todos os usuários.

Em face do exposto, é de primordial importância uma maneira lícita e eficaz de garantir, proteger e, principalmente, manter sobre controle a inviolabilidade à privacidade das pessoas para evitar a ocorrência de danos que muitas vezes se tornam irreparáveis.

2- CONSENTIMENTO DO USO DE DADOS: LIMITES E OBRIGAÇÕES

Consentimento, a principal palavra da Lei Geral de Proteção de Dados Pessoais. Nas palavras de Santos e Araújo (2017, p. 174) “a LGPD, entre outras disposições, exige consentimento explícito para coleta e uso dos dados e obriga a oferta de opções para o usuário visualizar, corrigir e excluir esses dados.”

É o titular, ou seja, a pessoa a quem se referem os dados que deve, caso queira, ao ser questionado, de forma explícita e inequívoca, autorizar que suas informações sejam usadas, por empresas e órgãos públicos, na hora da oferta de produtos e serviços, gratuitos ou não.

Assim sendo, com a nova lei, fica inteligível que quem é o verdadeiro dono do dado não é aquele que o utiliza, nem aquele que o salvaguarda em bancos de dados, mas unicamente a pessoa a quem ele diz respeito. Na teoria isso parece algo óbvio, mas na prática não é bem assim, muitos usuários têm seus dados utilizados para fins diversos, inclusive ilícitos.

Vale enfatizar que a Lei endossa que o consentimento deve ser para finalidades determinadas. Isso denota que não se pode solicitar dados de terceiros para fins genéricos, sem especificações, o pedido e sua posterior autorização não podem deixar margens para dubiedades. A Lei 13.709/18 em seu artigo 9º preconiza que:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Autorizações genéricas, sem menção à finalidade específica do tratamento, conforme se recomenda acima, serão nulas, por força do parágrafo 4º, do artigo 8º, da Lei 13.709/2018.

Em uma situação hipotética em que o detentor do dado autorizou que seus dados fossem empregados por uma organização ou empresa qualquer essa deverá pedir nova permissão caso queira empregar os dados para um novo fim.

Ademais, a hipótese de compartilhamento de dados pessoais com outros controladores também demandará consentimento específico do titular, nos termos do parágrafo 5º, do artigo 7º da Lei 13.709/2018 quando “necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.”

Ressalta-se que a revogação pode acontecera qualquer momento após o consentimento cedido anteriormente, como, por exemplo, nos casos em que a organização altere informações no decorrer do tratamento dos dados e o titular dos dados não concorde com a alteração.

O consentimento também poderá ser fornecido por qualquer outro meio que demonstre a manifestação de vontade do titular, quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual o titular seja parte e a pedido do titular destes dados.

Ao longo de toda a Lei nº 13.709/2018 se percebe a preocupação constante com a autorização dada pelo titular dos dados para que este seja tratado, compartilhado ou controlado por terceiros.

Inclui-se o tratamento de dados para o cumprimento de obrigação legal ou regulatória pelo controlador, caso em que o titular deverá ser informado das hipóteses em que poderá ocorrer o tratamento de seus dados pessoais, nos termos do artigo 7º da LGPD.

Ainda, de acordo com o supramencionado artigo o tratamento de dados pessoais somente poderá ser realizado quando necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou incolumidade física do titular ou de terceiro; para proteção do crédito; quando necessário para atender aos legítimos interesses do controlador ou de terceiro, sendo que por interesse legítimo do controlador entende-se o tratamento de dados pessoais para finalidades legítimas consideradas a partir de situações concretas que incluiriam, mas não se limitariam a apoio e promoção de atividades do controlador e proteção,

em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem.

Importante esclarecer que dado pessoal, de acordo com o estabelecido no anteprojeto que deu ensejo a Lei 13.709/2018, significa:

> Qualquer informação sobre uma pessoa física que seja capaz de identificá-la, podendo ser o número de documentos, biometria, fotos, digitais, endereço, exames, localização ou outro documento idôneo, e que é tido como tratamento toda operação realizada com esses dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Nessa perspectiva, infere-se que o objetivo maior da LGPD é assegurar que o indivíduo que disponibiliza seus dados pessoais a terceiros seja capaz de identificar o responsável pela segurança da informação passada, assim como, o que estão fazendo com os referidos dados, ou seja, a Lei se preocupa com a transparência, o acesso à informação e a garantia de que a pessoa física ou jurídica que está na posse de dados do outro tenha o controle sobre estes. Mas, principalmente a Lei determina que para esse procedimento ocorrer, deverá haver, explicitamente, o consentimento para que dados pessoais sejam entregues a terceiros ou até mesmo compartilhados.

2.1Os riscos e as preocupações ao usar a internet

Contudo, em que pese o consentimento seja o principal requisito para o manuseio de dados alheios, nos dias atuais o avanço da tecnologia e dos meios de comunicação, apesar dos benefícios, também tem gerado inúmeros transtornos e, princípios como da intimidade e da privacidade têm sido quebrados, resultando em danos materiais e, singularmente morais, trazendo em quase sua totalidade consequências irreparáveis e imensuráveis em virtude da repercussão social de certos atos.Cabe ressaltar que, em muitos casos, tais situações ganham repercussão mundial.

Por certo o acesso à internet permite ao usuário, em rápida pesquisa conhecer da vida de outra pessoa e até mesmo se apropriar de dados pessoais, incorrendo, eventualmente, em algum delito.

Além do que, é possível que violações ocorram propositadamente, por meio de fraudes criadas por hackers e de sites que depositam *cookies* nos computadores dos usuários e, ao compilar dados, mesmo autorizados pelos donos passam a compartilhar com outras pessoas. Santos e Araújo (2017, p. 175) destacam que “a principal empresa de busca da Internet, a Google, faz associações das buscas dos usuários a contas de e-mails destes, registrando sempre as buscas“, o que facilita o acesso ilegal e a disseminação indevida de dados.

Conhecido popularmente como “vazamento” de informações digitais essa conduta pode desencadear consequências irreparáveis a vítima, refletindo no quanto é importante questões relativas a regulação do uso de dados pessoais e o quanto eles estão vulneráveis. O autor Blum (2018, p. 7) destaca que:

> Nos dias de hoje, quase não se fala em expansão digital sem que sejam considerados eventuais atos criminosos, que são cada vez mais propagados por meio do uso dessas novas fontes. É por isso mesmo que a crescente disponibilidade de dados nas redes e a facilidade de acesso a tais informações tornou-se um chamariz para agentes mal-intencionados. Os motivos para isso são inúmeros. Os setores afetados pelos *cybercriminosos*, na sua maioria, guardam relação direta com ativos financeiros, mas a violação à privacidade, inclusive de cunho sexual, vazamento de dados sensíveis, *cyberbullying* e determinadas modalidades de *fake news*, também ocupam a lista dos principais ilícitos da atualidade, cujo resultado depende diretamente das ferramentas digitais.

Outro ponto a se observar é o amplo acesso as mídias digitais por meio do aparelho celular. Cabe destacar que com o avanço tecnológico o telefone móvel não se presta somente a fazer e receber ligações. Os modernos aparelhos são verdadeiros computadores portáteis, por onde se pode acessar e-mail, redes sociais, fotografar, além de armazenar uma infinita quantidade de informações íntimas e de cunho privado.

Nessa feita, questão relevante no mundo jurídico se apresenta em razão de se ter a vida privada registrada em um celular, pois, embora não possa ser considerado um local físico, permite a realização de atividades pertinentes à intimidade e à vida pessoal do indivíduo, características próprias de um domicílio.

Foi nessa linha de pensamento que tanto doutrina, quanto jurisprudência expandiu o conceito do termo domicílio. Para muitos juristas se faz necessária uma leitura ontológica a fim de atender a questão da tecnologia em relação a vida privada. Dezem elenca que (2018, p.36): “o conceito de casa como sendo o espaço físico onde se exerce a intimidade e a vida privada não é mais condizente com a realidade tecnológica que invade a sociedade moderna.”

Outros autores debatem sobre a extensão do conceito de domicílio a fim de estender a proteção pessoal de cada um, como o autor Amaral (2012, p.158):

> A moradia, conceitualmente, é um bem da personalidade, com proteção constitucional e civil. É, portanto, um bem irrenunciável da pessoa natural, indissociável da sua vontade e indisponível, exercendo-se de forma definitiva pelo indivíduo; secundariamente, recai o seu exercício em qualquer pouso ou local, mas é objeto de direito e protegido juridicamente. O bem da ‘moradia’ (sic) é inerente à pessoa e independe de objeto físico para a sua existência e proteção jurídica. Existe independentemente de lei, porque também tem substrato no direito natural. Atualmente, é uma situação de direito reconhecida pelo ordenamento jurídico, é uma qualificação legal reconhecida como direito inerente a todo o ser humano, notadamente, em face da natureza de direito essencial referente à personalidade humana.

Além do que, as câmeras fotográficas, hoje ao alcance da mão, tornando a captura de qualquer momento, seja ele íntimo ou não, facilmente registrável, também são capazes de, ao passo de um *click,* enviar uma imagem para milhares de pessoas, atacando o direito fundamental da dignidade da pessoa humana, muitas vezes de maneira irreparável.

Assim, a facilidade e a rapidez com que qualquer tipo de dados são compartilhados pelo celular, abrem espaço para outra discussão da sociedade moderna, a invasão de privacidade digital. Sobre tal situação, Paulo e Alexandrino apontam (2011, p. 135):

> No entendimento da Corte Suprema, a mera publicação não consentida de fotografias gera o direito à indenização por dano moral, independentemente da ocorrência de ofensa à reputação da pessoa, porquanto o uso indevido da imagem, de regra, causa desconforto, aborrecimento ou constrangimento ao fotografado, que deve ser reparado

Essa preocupação na busca de proteção digital nos dias atuais se apresenta em proporcionalidade com os grandes avanços tecnológicos. Nesse caminho, se faz imprescindível observar o princípio da dignidade humana para uma

melhor relação interpessoal e a eficácia da proteção, destacando a garantia da inviolabilidade à privacidade das pessoas.

Ante ao exposto se percebe a urgência de um posicionamento de ordenação e proteção proporcionada pelo Estado, sobretudo em relação às questões de segurança ou no combate a crimes como a pedofilia, pornografia, racismos, homofobias, machismos, entre outras violências.

2.2Dados pessoais sensíveis e não sensíveis

Atendendo a demanda de controle de dados a Lei 13.709/2018 estabelece e delimita os tipos de dados que poderão ser ou não compartilhados e o grau de segurança que cada um deve ser submetido. Denominando-os de dados sensíveis e não sensíveis a depender de suas especificidades.

Nesse sentido, já em seu artigo 5º, inciso I, a LGPD elenca que dado pessoal é toda “informação relacionada a pessoa natural identificada ou identificável”, regulamentando no inciso II que dado pessoal sensível deve ser entendido como aquele que revela a “origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural.”

Sabe-se que no atual cenário digital, as pessoas estão extremamente vulneráveis, informações privadas como fotos, vídeos íntimos, emails, senhas bancárias, entre tantos outros dados pessoais podem, sem autorização, serem expostos na internet violando a intimidade e a vida privada de alguém.

Na medida em que o acesso não autorizado cresce se torna urgente a criação de meios para barrar tais violações. Desse modo, ao estabelecer os denominados dados sensíveis a LGPD cria mecanismos para operacionalizar a proteção de direitos no âmbito digital, ampliando a tutela do Estado aos direitos da personalidade.

Influenciada pelo conjunto de regulações a respeito de proteção de dados na União Europeia, a *General Data Protection Regulation*– GPDR, a Lei 13.709/2018,

trás em seu bojo uma série de bases legais que definem os tipos de dados que devem ser classificados como sensíveis em razão de seu potencial grau de prejudicialidade, caso seja usado para fins criminosos ou discriminatórios.

Assim, qualquer dado que possa identificar uma pessoa de maneira singular, de forma 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 eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa deve ser inserido na classificação de sensível.

> Portanto, verifica-se que os dados pessoais sensíveis, seriam aqueles dados que podem identificar uma pessoa, demonstrando as características da sua personalidade, podendo, ainda, servir de base para uma discriminação, ao passo que, os dados pessoais não sensíveis não possuem essa propensão. (GRESSLER. BACHINSKI. SILVA, 2019, p. 08)

Pode-se inferir que dados pessoais sensíveis, além de serem utilizados para fins discriminatórios ou criminosos, também podem ser usados para controlar pessoas ou até mesmo um grupo social, caso usados de maneira indevida.

A título de exemplo, tem-se o uso destes dados em eleições recentes por todo o mundo. De posse de informações pessoais, criaram-se softwares, mediante o uso de algoritmos, a fim de divulgação de notícias específicas que privilegiava determinado candidato, adequando tais informações ao perfil ou a identidade digital do usuário. Assim, dados sensíveis possuem valor político e, sobretudo, econômico, uma vez que podem ser vendidos para o controle social.

É interessante destacar que, de acordo com o §2º, do artigo 12, da LGPD qualquer dado pessoal, ou seja, qualquer informação usada para formação do perfil comportamental de uma pessoa, que torne esta pessoa identificada ou identificável, está sujeita a se tornar sensível ou, ainda, uma informação anônima, a depender do poder de prejudicialidade.

Desse modo, a proteção de dados deve ser observada como uma proteção a dignidade da pessoa humana e o direito de cada indivíduo à convivência social pacífica, sem interferências exteriores, resguardando o livre desenvolvimento de sua personalidade e, em particular, garantindo a sua autodeterminação informacional.

3- ATUAÇÃO DE UM *DATA PROTECTION OFFICER –DPO*

Importante acordar que a questão da proteção de dados ultrapassa a esfera governamental, devendo ser entendida como um assunto de toda a sociedade. Compete também ao cidadão usuário a responsabilidade em avaliar se um determinado site é de fato seguro para inserção de seus dados pessoais, a fim de se evitar danos pela simples má-utilização no uso da ferramenta (PAESANI, 2012). Informa Blum (2018, p. 7) que:

> A *Norton Cyber Security*[3] chegou a reportar recentemente que o Brasil se destaca em seu radar como um dos países com maior índice de cometimento de crimes cibernéticos no mundo, concorrendo com países tais como China, Estados Unidos e Rússia. Também é relevante pontuar que a Microsoft chegou à conclusão, após um estudo promovido em 23 países, de que cerca de 30% dos “crimes online” (sic) estão ligados a amigos ou mesmo parentes das vítimas.

Objetivando uma maior proteção de dados nas redes de computadores, a Lei 13.709/2018 estipulou limites e prerrogativas a serem seguidas por aqueles responsáveis por guardar informações de terceiros, dentre essas medidas de segurança e atendendo uma demanda do mercado, surgiu o profissional *Data Protection Office* – DPO, o qual seria o responsável por garantir a segurança das empresas e de seus clientes.

Atualmente, a Lei Geral de Proteção de Dados determina que, em regra, toda empresa, seja ela pública ou privada, que processe um número significativo de registros de dados, precisa do apontamento de um profissional responsável pela proteção de tais informações, no caso um encarregado, como determinado no artigo 5ª da aludida Lei.

Sua função seria proteger dados da empresa, sendo o encarregado, termo aplicado na LGPD para designar o DPO, o principal canal de comunicação entre o controlador, ou seja, a empresa que está na posse dos dados de terceiros, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD, de

[3]Empresa responsável por examinar comportamentos, as atitudes e os hábitos de segurança online dos consumidores, as preocupações e os perigos associados á privacidade e segurança online.

responsabilidade do governo federal, já devidamente estruturada, conforme o Decreto nº 10.474, de 26 de Agosto de 2020.

De acordo com o supramencionado Decreto, a ANPD é um órgão do governo federal, dotado de autonomia técnica e decisória, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pelo disposto na LGPD

Ressalta-se que a ANPD, diferentemente das demais agências setoriais, será responsável por fiscalizar todas as empresas atuantes no mercado, como informa o artigo 2º do referido Decreto:

> Art. 2º Compete à ANPD:
> [...]
> IV - fiscalizar e aplicar sanções na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

Assim, antes de adentrar na aplicabilidade e nos benefícios de se ter um especialista em proteção de dados dentro de uma empresa, seja ela pública ou privada, cabe esclarecer quem é este profissional que surgiu no mercado de trabalho nos últimos anos, se destacando como imprescindível para o bom funcionamento de um banco de dados.

Conhecido como *Data Protection Officer*, ou simplesmente DPO, este profissional tem como uma de suas principais funções cuidar para que informações de clientes entregues a uma organização não sejam expostas ou caiam nas mãos de terceiros. Na Lei de Proteção de Dados o DPO é descrito no artigo 5º, VII como:

> Art. 5º Para os fins desta Lei, considera-se:
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Percebe-se que, em que pese tenha recebido a denominação de encarregado sua função é responsável por adaptar e estruturar todo o processo de *compliance*, a fim de garantir a segurança das informações tuteladas de uma empresa ao garantir que a esta cumpra os requisitos dispostos no artigo 39 da LGPD frente aos órgãos fiscalizadores.

Ocorre que a Lei de Proteção apenas aponta diretrizes para a função estabelecida, deixando que a regulamentação posterior aprofunde suas atribuições em normas complementares. Assim as funções pré-estabelecidas na LGPD acerca de seu trabalho foram delimitadas no artigo 41, *in verbis:*

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Infere-se deste artigo que o DPO pode ser uma pessoa natural ou jurídica, de direito público ou privado, o que dá liberdade de escolha aos controladores, mas, também, ressalta a imprescindibilidade deste "canal de comunicação entre o controlador, a quem cabe a decisão do tratamento dos dados pessoais, os titulares desses dados e a ANPD, órgãos normatizador, orientador e fiscalizador das ações de tratamento." (SABATT, 2019, p. 5).

Destaca-se que o DPO como um encarregado da proteção de dados, não necessariamente deve ser um funcionário da empresa controladora. De acordo com a lei brasileira, em tese, toda empresa terá de contar com esse profissional, independentemente de seu porte ou segmento de atuação. Na prática, seu trabalho consiste em estruturar um programa de segurança da informação em conformidade com a legislação, que estabelece diretrizes para tratamento de dados.

Por certo uma nova lei necessita de um período de adaptação, principalmente se tratando de um assunto que a maioria da população não domina ou, ainda, não percebeu a importância.

Contudo, assim como ocorreu há algumas décadas ante a vigência do Código do Consumidor, a LGPD trará conscientização maior e a exigência da

população para que suas informações pessoais sejam respeitadas passará a ser uma constante.

3.1A importância de um DPO em uma Instituição de Ensino

Por certo, a necessidade de adequação de qualquer empresa que retém dados pessoais de terceiros se fará obrigatória e a função de um profissional DPO será determinante nesse novo cenário. Sabatt (2019, p. 6) ao analisar esse novo mercado de trabalho e seus efeitos futuros descreve que:

> Tem-se que o trabalho do DPO ainda está em estágio inicial tanto para as organizações sujeitas ao cumprimento do GDPR e, mais ainda, para as que deverão estar em conformidade com a LGPD. Timidamente, as empresas estão buscando investir e lidar com a conformidade com o GDPR. Entretanto, o GDPR exige um DPO em situações específicas, enquanto a LGPD não define especificidades. Desse modo, diante da obrigatoriedade, é preocupante o fato de poucas empresas ainda terem iniciado, ao menos grupos de trabalho para tratarem internamente do tema.

Desse modo, para que uma empresa se resguarde no cuidado com dados de clientes, garantindo aos titulares o direito à informação segura, com identificação do controlador e de todos aqueles que compõem a cadeia de acesso a seus dados pessoais, respeitando os direitos do titular trazidos pelo artigo 18 da LGPD, a função de um DPO se faz essencial, sendo sua função proporcional a confiança depositada.

Destaca-se que o profissional DPO ainda se apresenta de maneira tímida no mercado, em que pese tenha um valor enorme, garantindo que o elo de confiança entre o cliente, a empresa e os órgãos normatizadores não se desfaçam.

Assim, com base em todas as informações e inovações trazidas pela LGPD, pode-se inferir possíveis situações onde se requer imprescindível um DPO, como uma instituição de ensino, tanto superior, quanto fundamental, haja vista o fato de receber semestralmente centenas de alunos e, em decorrência, informações pessoais de todos eles.

Mesmo que se acredite ser capaz de ter o controle de tais informações, por já ter uma rotina de anos no manuseio de matrículas, o autor Blum (2020, p. 4) alerta que “a conformidade com a legislação de proteção de dados não é estática, e a empresa deve estar atenta para já prever a adequação de novos produtos, áreas ou negócios.”

A temática da proteção de dados pessoais tornou-se relevante nas últimas décadas muito em razão do grande número de casos de violação e o avanço da tecnologia utilizada para a prática de crimes digitais.

Sabe-se que um cidadão comum se torna vulnerável ao se expor na internet, o que gera uma série de protocolos de segurança, mas quando se trata da realização de um cadastro em alguma empresa ou da informação pessoal repassada em algum órgão público, normalmente a precaução não é observada.

Nesse contexto, importante destacar que muitos dos transtornos causados por violação dos direitos inseridos no bloco da personalidade, como intimidade e privacidade podem surgir a partir de vazamento de dados por empresas privadas, levando a aplicação do instituto da responsabilidade civil como forma de reparação a eventuais ofensas e com a vigente da LGPD o pagamento de multa, sem prejuízo de outras sanções legais administrativas, dispostas nos artigos 52, 53 e 54 da aludida Lei.

Em razão de tudo isso, a figura do encarregado dentro da empresa foi imposta, justamente para que tanto a empresa, quanto o cliente se protejam de vazamentos indesejados. Blum, (2020, p.3) ainda ressalta que “cabe ainda ao encarregado garantir a implementação das políticas internas criadas e a adaptação destas aos novos produtos e necessidades que forem surgindo com o decorrer do tempo.”

Enfatizando que um DPO deve ter seu conhecimento voltado para a área de proteção de dados, mas não se esquecendo do campo jurídico ou técnico e áreas de *compliance,* razão pela qual, muitas instituições privadas estão contratando não uma pessoa jurídica, mas sim um escritório para atuarem nesta área em especifico.

3.2 Caso Concreto: como se proteger

A título de exemplo da importância em se ter um controle de informações em uma Instituição de ensino, cabe trazer o caso ocorrido em uma Universidade do Rio Grande do Sul, a Unisinos, o qual gerou uma ação coletiva pleiteando indenização por danos morais, após a Universidade expor dados pessoais de mais de 23.300 alunos, em janeiro de 2012.

Com o intuito de divulgar vagas para estágio para alunos do curso de Arquitetura e Urbanismo, a Universidade, equivocadamente, encaminhou email contendo os dados pessoais de aproximadamente 900 alunos, provocando uma série de transtornos para aqueles que tiveram seus dados vazados, alguns, inclusive, prejuízos financeiros, pois de posse de dados de terceiros golpistas realizaram compras via internet.

O email continha um arquivo anexo onde informava o número de telefone celular, residencial e comercial, e-mail, RG, CPF, nome completo, data de nascimento e várias informações acadêmicas, como login no sistema da Universidade, tipo de ingresso e etapa da graduação de outros milhares de alunos. (Nº CNJ: 0296615-34.2018.8.21.7000/RS/2012)

A ação coletiva movida pelos estudantes prejudicados se amparou na responsabilidade civil prevista no Código Civil, em seu artigo 186, bem como no artigo 187 pelo abuso de direito, a fim de pleitear indenização pelos danos patrimonial e moral causados, em razão de não haver na época lei específica para regular a demanda.

Neste caso a responsabilidade surgiu em razão do contrato estabelecido entre as partes, assim, como leciona Tartuce (2018, p. 60) “o dano pode surgir tanto em atividade disciplinada por um contrato, daí a chamada responsabilidade contratual, como em atividade independente de qualquer ajuste com o ofendido, sendo esta a denominada responsabilidade extracontratual.”

> No caso em análise, havia um contrato entre as partes, o qual impunha o dever de cuidado e observância da boa-fé objetiva no tratamento dos dados. Por outro lado, a ação de publicar os dados não estava relacionada com o escopo contratual e atingiu direitos de personalidade dos contratados. Na época não havia previsão legal específica para a tutela de dados pessoais nestes casos, no entanto, havia o dever de guarda e de cuidado, decorrentes da boa-fé objetiva. Esta situação se altera com a novel legislação, pois ela se destaca pela previsão de princípios que regem a proteção de dados pessoais, especialmente quanto ao consentimento, que possui um importante papel para a efetivação de autodeterminação informativa, um dos fundamentos da LGPD. (GRESSLER. BACHINSKI. SILVA, 2019, p. 11)

Na ocasião tanto o tribunal *a quo,* quanto o de apelação entendeu pela não condenação da Universidade ao pagamento de indenização por danos morais, embora tenham reconhecido o ato ilícito, fundamentando que os dados pessoais divulgados eram tidos como não sensíveis, sendo estes rotineiramente expostos para

fins cadastrais em qualquer estabelecimento social, não comportando nenhum teor vexatório ou moral.

> Isso porque as informações divulgadas não configuram os chamados "dados sensíveis" (sic), tais como orientação ideológica, religiosa, sexual, etc. Friso, não houve a divulgação de dados bancários, financeiros, creditícios e/ou senhas. Tampouco de informações que atingissem a dignidade da pessoa humana, tais como, convicção política, religiosa, partidária, sindical, racial e sexual. Essas, sim, resguardadas pelo art. 5º, x, da constituição federal. (Apelação nº 70079314035/ Des. Relator: Eugênio Facchini Neto, RS/2018).

Ocorre que nos dias atuais, uma questão semelhante provavelmente terá um desfecho diferente. No caso em comento a Universidade certamente teria que arcar com uma sanção financeira, sem prejuízo de medidas administrativas impostas pelo órgão regulamentador, inclusive sofrendo restrições legais.

Analisando por meio das normas impostas pela LGPD, princípios e garantias fundamentais foram violados, pois não houve a manifestação da vontade expressa dos alunos para que seus dados tivessem fim diverso do acordado no momento de seu depósito na Universidade, embora estes não constituíssem dados sensíveis.

Instituído pela primeira vez pela Organização para a Cooperação e Desenvolvimento Econômico- OCDE, o princípio da finalidade trata do propósito a que se destina a coleta de dados pessoais, devendo ser o titular dos dados sempre informado caso qualquer utilização tenha finalidade diversa da declarada no ato de entrega.

Este princípio incorporado pela Lei 12.965/2014, em seu artigo 7º, VIII, assegura o direito ao "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei".

Assim, como no Marco regulatório da internet a finalidade, também, se encontra respaldada pela LGPD, em seu artigo 6º, I, onde se lê que:

> Art. 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

Nestes termos, percebe-se que a LGPD veio para estabelecer diretrizes e assentar princípios a serem observados ao se manipular dados pessoais de terceiros. Apontando condutas e normas a serem atendidas na mesma medida, seja por empresas públicas ou privadas, a fim de que não padeça qualquer violação a direitos individuais de leis infra legais ou de fundamentação discricionárias de tribunais.

Infere-se que deverá ser observada em toda a cadeia de proteção de dados, a finalidade a que estes se destinam, bem como respeitada a vontade de seu titular, pois é o consentimento deste que dita o caminho a ser seguido pelo controlador dos dados.

Para tanto, a função de um *Data Protection Officer* é de extrema relevância nesta nova relação empresa/cliente, haja vista ser ele o responsável por acompanhar todos os fluxos de processos realizados dentro da empresa controladora, bem como a elaboração de termos de consentimento e o processo de anonimização dos dados armazenados, entre outros tantos pontos imprescindíveis para a certificação correta de todas as práticas de tratamento de dados, dentro do ideal de *compliance* imposto pela Lei Geral de Proteção de Dados.

Resguardar-se e preservar clientes seria, nos dias atuais, com a Era digital, um dos principais objetivos de uma empresa, independente de quantos dados retém, basta somente um dado em mãos erradas para gerar prejuízos. Assim, uma boa estrutura empresarial deve levar em conta a figura de um *DPO* em seu quadro de funcionários.

CONCLUSÃO

O que antes era regulamentando por Leis diversas agora possui um assentamento próprio dentro do ordenamento jurídico pátrio. Com o advento da LGPD rompe-se o paradigma cultural de que, sem prejuízos efetivos ao terceiro prejudicado não se havia responsabilidade direta daquele responsável por guardar a informação. Inaugura-se, assim, uma nova etapa em que se impõe a tutela material dos dados pessoais tratados em ambiente digital.

Considerando que o Marco Civil da Internet, vigente a partir de 2014, estabeleceu diretrizes e regulamentou temas específicos no que se refere a proteção de dados, contudo, sem impor sanções condenatórias, tão pouco detalhar o procedimento a ser aplicado no que tange a segurança da informação pessoal de terceiros, a Lei 13.709/2018, de fato, marca o início de uma nova era para a coleta, o tratamento e a exploração de dados pessoais.

Sendo a tutela jurídica de dados pessoais o ponto central do direito à privacidade e a intimidade do cidadão no campo do direito digital, ressalta-se que dentre as alterações mais relevantes da LGPD está o reconhecimento da autodeterminação informativa, a qual veda o tratamento de dados sem o consentimento expresso do titular.

Nesse contexto apresentado, a figura de um profissional responsável para garantir o tratamento correto de dados em empresas públicas e privadas, se faz essencial, principalmente, naquelas com grande fluxo de dados, como ocorre em uma Instituição de ensino.

Tendo em vista que quanto maior o número de informações a ser controlada, maior a probabilidade de apresentar-se um problema, desse modo, a garantia de segurança no tratamento de dados em grande escala requer um profissional específico, materializado na função do DPO.

Desse modo, conclui-se que, o recolhimento de dados pessoais para as atividades regulares de uma Universidade e o tratamento destes dados em tempo real, faz com que a função de um DPO, com autonomia e imparcialidade dentro das organizações, seja imprescindível ao quadro funcional.

REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL. Cláudio do Prado. Inviolabilidade do domicílio e flagrante de crime permanente.**Revista Brasileira de Ciências Criminais**. vol. 95. p. 137/165. São Paulo: Ed. RT, mar. /2012. Disponível em https://repositorio.usp.br/item/002302878. Acessado em 06/05/2020.

BLUM. Renato Opice. **LGPD – Lei Geral de Proteção de Dados**. 1ª Ed. Revista dos Tribunais. 2018

BRASIL**. ADIn 2937**, Tribunal Pleno, j. 23.02.2012, rel. Min. Cezar Peluso, DJe 104, divulg. 28.05.2012, public. 29.05.2012, RT 922/542-567, 2012.

_____. **ADPF 130**, Tribunal Pleno, j. 30.04.2009, rel. Min. Carlos Britto, DJe 208, divulg. 05.11.2009, public. 06.11.2009, ement. vol. 02381-01, p. 00001, RTJ 213/20.

_____. Tribunal de Justiça do Estado do Rio Grande do Sul.**Apelação cível n. 70079314035.**Relator: Des. Eugênio Facchini Neto, 18 de dezembro de 2018. Disponível em: http://www.tjrs.jus.br/site/busca-solr/index.html?aba=jurisprudencia. Acesso em: 03/set/ 2020.

_____. **Lei 12.965/2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 02/set/2020.

_____. **Lei 13709/2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acessado em: 02/set/2020.

DEZEM. Guilherme Madeira. **Prática Jurídica Penal**. 13ª ed. São Paulo. Saraiva. 2018.

FONSECA, Fernando. O Caminho **do DPO (Data Protection Officer).** Rio de Janeiro. 2018. Disponível em:https://www.exin.com/br-pt/o-caminho-do-dpo-data-rotection-officer/. Acessado em 10/Set./2019.

GONÇALVES. Pedro Correia. **O direito ao respeito pela vida privada e familiar dos doentes mentais à luz da jurisprudência do Tribunal Europeu de Direitos Humanos**. RBCCrim. São Paulo. 2006.

GRESSLER. Igor Costa. BACHINSKI. Fabiane Leitemberger. SILVA. Rosane Leal da. **A divulgação indevida de informações pessoais em site de Universidade gaúcha: resposta jurisdicional entre a óptica constitucional e os princípios da lei n.13.709/2018.** 5º Congresso Internacional de Direito e Contemporaneidade. UFSM – Universidade Federal de Santa Maria. Set. 2019.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. 5. ed. São Paulo: Atlas, 2012.

PAULO, Vicente. ALEXANDRINO, Marcelo. **Direito Constitucional Descomplicado**. Grupo Gen. Goiânia. Ed. Método. 2011.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD).** São Paulo: Saraiva Educação. 2018.

RIVERO. Jean Moutouh Hugues. **Liberdades públicas**. São Paulo: Martins Fontes. 2006.

SABBAT. Arthur. **O papel do 'Encarregado' ou 'Data Protection Officer' na LGPD** Disponível em: https://www.securityreport.com.br/destaques/o-papel-do-encarregado-ou-data-protection-officer-na-lgpd/#.X3uNwPZKjIU. Acessado em 18/set.2020.
SANTOS, Maria Celeste Cordeiro Leite dos. ARAÚJO, Marilene. O tempo e o espaço. Fragmentos do marco civil da internet: paradigmas de proteção da dignidade humana. **Revista Bras. Políticas Públicas**, Brasília. Vol. 7, nº 3. 2017.

SILVA.José Afonso da. **Curso de direito constitucional positivo**. 19. ed. São Paulo: Malheiros, 2009.

SOMADOSSI, Henrique. **O que muda com a Lei Geral de Proteção de Dados (LGPD).** São Paulo. 2018.Disponível no Link: https://medium.com/@marcellomullerteive/o-que-vai-mudar-nas-nossas-vidas-com-a-lgpd-a8b83192a629. Acessado em 14/10/2019.

TARTUCE, Flávio. **Manual de responsabilidade civil: volume único**. São Paulo: Método, 2018.