A TUTELA DOS DADOS PESSOAIS SENSÍVEIS PELO ORDENAMENTO JURÍDICO: UMA ANÁLISE DO DEVER DE SEGURANÇA INSTITUCIONAL NO SETOR PÚBLICO SOB A ÓTICA DA LGPD

Juliomar de Paula Neto[1]

Karlos Alves Barbosa[2]

RESUMO

O presente artigo tem por finalidade investigar as diretrizes da LGPD (Lei Geral de Proteção de Dados), especialmente no que diz respeito ao tratamento de dados pessoais sensíveis na administração pública, uma vez que o tratamento de dados nesse setor obteve diretivas relevantes na Lei nº 13.709/18, arts. 23 e 46 ss., sobretudo, devido à crescente exploração da tecnologia da informação e dos procedimentos de tratamento de dados na gestão pública. Em síntese, o presente estudo buscou examinar formas de ampliação de proteção da existência eletrônica da pessoa física, ou seja, "dados pessoais sensíveis", em respeito ao dever de segurança institucional aplicado ao setor público diante dos ciberataques, bem como as eventuais penalidades, multas e sanções aplicadas aos agentes envolvidos. Para este estudo, foi utilizado o método dedutivo, empregando-se a técnica de pesquisa bibliográfica, alicerçado em doutrinas, artigos, legislação e jurisprudência acerca do tema.

Palavras-chave: dados pessoais; direito à privacidade; ciberataques;

[1] Graduando em Direito pela Universidade Federal de Uberlândia, Av. João Naves de Ávila, 2121, *Campus* Santa Mônica, bloco 3D, Uberlândia – MG, 38400-902. Contato: juliomar.neto@ufu.br

[2] Professor da Faculdade de Direito "Prof. Jacy de Assis" da Universidade Federal de Uberlândia, Av. João Naves de Ávila, 2121, *Campus* Santa Mônica, bloco 3D, Uberlândia – MG, 38400-902. Contato: karlosalves@gmail.com

THE PROTECTION OF SENSITIVE PERSONAL DATA BY THE LEGAL ORDINANCE: AN ANALYSIS OF THE INSTITUCIONAL SECURITY DUTY IN THE PUBLIC SECTOR FROM THE VIEWPOINT OF THE LGPD

ABSTRACT

The purpose of this article is to investigate the LGPD guidelines (General Data Protection Law), especially with regard to the processing of sensitive personal data in the public administration, since the processing of data in this sector has obtained relevant directives in Law no. 13,709/18, arts. 23 and 46 ff., above all, due to the growing exploitation of information technology and data processing procedures in public management. In summary, this study sought to examine ways to expand the protection of the electronic existence of the individual "sensitive personal data", in respect of the institutional security duty applied to the public sector in the face of cyber attacks, as well as any penalties, fines and sanctions applied to the agents involved. For this study, the deductive method was used, using the technique of bibliographic research, based on doctrines, articles, legislation and jurisprudence on the subject.

Keywords: personal data; right to privacy; cyber attacks;

1. INTRODUÇÃO

No âmbito jurídico ainda há muito que se analisar os mecanismos de tutela dos dados pessoais sensíveis[3], bem como sua segurança institucional, haja vista a crescente importância da tecnologia da informação e dos procedimentos de tratamento de dados pessoais tanto na esfera das pessoas jurídicas de direito público, seja interno, ou externo, quanto no âmbito das pessoas jurídicas de direito privado.

Ocorre que os fatores negativos intimamente ligados ao ambiente virtual se ampliaram, a exemplo dos ciberataques e tentativas de infecção de computadores e dispositivos móveis por meio de fraudes on-line que objetivam a captação de dados dos usuários. Não é nada forçoso constatar que através de uma "engenharia digital ilícita", "hackers" aplicam golpes nos internautas com a finalidade de subtrair dados pessoais, em especial informações sobre dados bancários para que possivelmente consigam realizar atividades ilícitas em nome do titular.

Os dados pessoais são informações relativas à uma pessoa que, eventualmente, será identificada com seus dados específicos, tais como: nome, RG, CPF, endereço, telefone, cartão ou dados bancários e, para além destes dados pessoais simples, os mais complexos denominados dados pessoais sensíveis, quais sejam: "convicção religiosa, opinião política, dado referente à saúde ou à vida sexual, entre outros".

A identificação do indivíduo é algo relevante para nossa vida em sociedade. É através da análise desses dados que o setor público consegue traçar perfis e formular políticas públicas, ampliando até mesmo a qualidade de vida de sua população. Eis a relevância da aplicação da LGPD em prol do bom tratamento de dados pessoais e da criação de mecanismos de proteção e garantia do consentimento e ciência do internauta.

Objetivando enriquecer ainda mais a presente discussão, urge trazer à baila para fins de fundamentação do tema a Teoria Tridimensional do jusfilósofo Miguel Reale[4], haja vista a presença de três concepções unilaterais do direito, quais sejam: o aspecto fático (fato), sendo seu nicho social e histórico; o aspecto axiológico (valor), ou seja, os valores buscados pela sociedade, bem como o aspecto normativo (norma) proveniente do ordenamento jurídico. (REALE, 1994, p. 117).

---

[3] Considera-se dados pessoais "sensíveis" aqueles que possuem características particulares e íntimas do titular, a exemplo da convicção religiosa ou opinião política, que revelam origem racial ou étnica, filiação sindical, questões genéticas, biométricas, sobre saúde e orientação sexual.

[4] Reale, Miguel. Teoria tridimensional do direito/ Miguel Reale - 5 ed. - São Paulo: Saraiva, 1994.

Em diálogo com a teoria tridimensional do direito supramencionada, entende-se instrumentalizada no "valor" atribuído ao direito à privacidade em sociedade, sendo por sua vez o bem juridicamente tutelado pelo texto normativo, bem como a "norma" apresentada, qual seja: Lei nº 13.709/18, em seu art. 23[5] e 46[6] ss., que dispõe sobre o tratamento de dados no setor público e a promoção da segurança e das boas práticas e, por fim, o "fato" de que empresas privadas e hackers se apropriam dos dados pessoais dos internautas indiscriminadamente, utilizando de má-fé, impulsionando *deepfakes*, fraudes e diversos outros cibercrimes.

Mediante ao exposto, medidas são necessárias para ampliar a defesa da existência eletrônica da pessoa, a ponto de identificar as falhas e eventuais desconformidades à LGPD no setor público, em respeito aos dados sensíveis da população e, para além disso, no objetivo de ampliar à adequação das pessoas jurídicas de direito público às exigências legais, gerando maior credibilidade, como também crescimento econômico para um ambiente digital mais seguro e atrativo.

Dessa maneira, o presente trabalho objetiva analisar os conceitos e as características dos dados pessoais em suas ramificações mais singelas, em especial na esfera dos dados sensíveis que por sua vez obteve uma atenção especial pelo ordenamento jurídico. Ademais, foi examinado, aspectos sobre a governança de dados e acesso à informação no setor público, em prol de boas considerações acerca dos elementos essenciais para construção de um sistema público de dados de excelência, com direcionamento estratégico de dados e incentivo nos investimentos em infraestrutura digital de qualidade, bem como estratégias para um bom gerenciamento do banco de dados.

Nessa senda, foi observado o dever de segurança institucional por parte do ente público, em conformidade com as diretrizes da Lei nº 13.709/18 (LGPD) e as eventuais vulnerabilidades das extensões digitais.

---

[5] Art. 23º - O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (...) <www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>

[6] Art. 46º - Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. <www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>

2. DADOS PESSOAIS

Cumpre demonstrar que um dado pode ser definido como uma informação em potencial, que não passou por um procedimento de refinamento, ou seja, um dado seria o conjunto de conteúdos relativos a uma pessoa desprovidos de estrutura organizada e, portanto, não cognoscitivo.

Infere-se que os dados pessoais determinam informações relativas a uma pessoa, identificada ou identificável, podendo ser até mesmo a configuração de um conjunto de informações que identifica uma pessoa viva. Sob o ponto de vista técnico à luz da Lei Geral de Proteção de Dados, estes dados podem ser anônimos ou sensíveis. O primeiro refere-se a um indivíduo que não possa ser identificado, sendo portanto um dado descaracterizado que inclusive não é considerado "pessoal". Já o segundo alcança características particulares e íntimas do titular, a exemplo da convicção religiosa ou opinião política.

Os dados pessoais são uma autodeterminação informacional vinculada diretamente com a normativa do consentimento. Este é o pilar para concessão do referido tratamento pelo qual um indivíduo apresenta dados pessoais identificados ou identificáveis para em seguida autorizar o fluxo dos seus dados.

Nota-se que os dados pessoais se tornaram uma ferramenta crucial no âmbito mercadológico, em que a publicidade sendo uma potente ferramenta para movimentação informacional de dados realiza seu papel no mundo do marketing. Cabe ressaltar ainda que é nessa seara da publicidade onde empresas, marcas, aplicativos e todas as segmentações do tipo fazem a solicitação dos dados pessoais dos usuários em troca de alguma ferramenta, informação ou serviços na rede informacional. (BIONI, 2019, p. 106).

Hodiernamente, o internauta ingressa na chamada "economia de vigilância", sendo apenas um espectador de seus dados, esperando por uma governança de dados segura que receba um tratamento adequado.

Ao longo dos anos diversas legislações objetivando a regulamentação de dados dos usuários foram criadas, a exemplo da GDPR na União Europeia em 2012, que estabeleceu um tratamento rígido quanto a coleta, processamento, compartilhamento e guarda dos dados, em conformidade com as seguintes diretrizes: informação ao usuário quanto a forma que os dados seriam tratados; necessidade de autorização dos internautas (consentimento); restou demonstrado a importância de se ter a opção de exclusão e interrupção da coleta de dados; utilização de linguagem clara e concisa nos termos; Necessidade de se comunicar às

autoridades dentro de prazo específico o vazamento/violação de dados, dentre outras diretrizes.

Essas são determinações que previnem violações aos dados dos usuários e que por sua vez estão intimamente ligadas com a rede global, ou seja, caso uma empresa brasileira pretenda realizar um negócio com a União Europeia seus termos e contratos eletrônicos sobre tratamento de dados deverão estar em conformidade com sua legislação.

Em solo brasileiro, tivemos a inauguração do Marco Civil da Internet[7] (Lei 12.965/2014) onde se promoveu uma normativa específica acerca dos direitos dos usuários nas relações da internet. De forma principiológica, houve a ampliação da proteção da privacidade e dos dados pessoais, bem como a ratificação de garantia de um ambiente virtual de neutralidade e de liberdade de expressão. Nessa perspectiva, ainda se normatizou em alguns de seus dispositivos a orientação quanto ao consentimento expresso e informado.

São essas as diretrizes apresentadas pelo Marco Civil da Internet e, eventualmente, ilustradas sobre uma autodeterminação informacional apresentada pelos cidadãos-usuários da rede global de internet.

2.1. DADOS PESSOAIS SENSÍVEIS E SUAS VULNERABILIDADES

Insta esclarecer que os dados pessoais sensíveis recebem um tratamento diferenciado pelo ordenamento jurídico, haja vista sua maior vulnerabilidade em razão do seu teor personalíssimo. Esses dados possuem um papel fundamental para que o sujeito de direitos se realize e se relacione na sociedade.

Quando se pensa nesses dados estaremos diante de informações bem específicas do indivíduo, a exemplo de questões como orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical.

A grande questão está presente no âmbito tecnológico, *(e.g., Big Data),* em que se permite incluir essas informações em um sistema de cruzamento de dados cujo objetivo seja relacionar uma série de dados e prever comportamentos e acontecimentos, a exemplo, de uma empresa que tenha acesso aos resultados de pesquisas de mulheres sobre período de gestação

[7] O Marco Civil da Internet, oficialmente chamado de Lei n° 12 965/2014, é a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

e, eventualmente, tenha oferecido produtos e serviços para mulheres que queiram engravidar ou que já estejam grávidas, ou seja, uma “publicidade direcionada”. Nesse sentido, o objetivo se volta para a captura dos dados e posterior revenda às empresas interessadas no mercado, por intermédio da coleta de dados das individualidades sigilosas dos usuários através de formulários e contratos eletrônicos ou até mesmo de ferramentas com vírus e programas maliciosos.

Em continuidade ao tema, se faz de suma importância entender que a proteção de dados pessoais se apresenta como um novo direito da personalidade, cabendo ressaltar que essa proteção não é direcionada apenas aos dados existentes na rede global da internet, ou seja, também se aplica a dados obtidos por meio físicos, a exemplo da proteção de dados contidos em um prontuário médico de informações relevantes acerca da saúde do paciente. (GUIMARÃES, 2020, p. 7).

Nota-se que em muitos casos de subtração de dados o “modus operandi” a ser realizado após a coleta desses dados dos usuários seria, a rigor, a venda aos interessados no mercado para seja possível determinar perfis comportamentais com a finalidade de influenciar de alguma forma a vida dos usuários, seja na oferta de um produto ou serviço, ou de qualquer questão que venha a ser de interesse do internauta que disponibiliza estes dados pessoais. Portanto, medidas são necessárias para ampliar a proteção dessa existência eletrônica da pessoa humana, uma vez que a proteção de dados pessoais pelo ordenamento jurídico como nos apresentou um novo direito da personalidade, entendendo alguns juristas especialistas da área como uma evolução do direito à privacidade.

2.2. CONSENTIMENTO E GOVERNANÇA DE DADOS NO SETOR PÚBLICO

O consentimento nas relações de fornecimento de dados possui bastante relevância para autorização do fluxo de informações pessoais, sendo considerado pelo ordenamento jurídico uma hipótese de base legal para o tratamento de dados. Um consentimento livre, informado e inequívoco, em conformidade com uma contraprestação da parte que irá coletar esses dados de transparência, especificação de propósitos e permissão de livre acesso ao usuário.

É de fundamental importância que o setor público observe essas diretrizes e promova investimentos na infra-estrutura de rede para que seja possível coletar as informações necessárias e, eventualmente, desenvolver os projetos de políticas públicas.

Nessa senda, infere-se a elevada responsabilidade por parte do setor público em efetivar uma boa administração dos dados pessoais do cidadão-usuário, uma vez que a boa administração ou até mesmo a ingerência resulta em impacto direto na vida dessas pessoas e na esfera do direito à privacidade e à intimidade dos indivíduos.

Nota-se que a referida ingerência pelo poder público resulta em um protocolo negativo ao sistema e à existência eletrônica dos usuários, cabendo demonstrar ainda que essa falta de administração do todo, se justificada, ou seja, uma vez constatada a efetivação do princípio do dever de segurança institucional por parte do setor público, possivelmente afastaria qualquer tipo de responsabilidade ao ente. Obviamente, isso deveria ser demonstrado em situações envolvendo motivo de força maior ou caso fortuito que, eventualmente, poderia excluir o nexo causal.

Ora, não é nada forçoso constatar que a simples prova de se ter agido com a devida cautela, em respeito ao dever de segurança e com o princípio da segurança, mantendo constantemente atualizados e protegidos os sistemas de proteção de dados, bem como com uma boa política de privacidade, acarretaria no afastamento de qualquer imputação de responsabilidade ao setor público. Basta analisar a hipótese de que se com todas as técnicas de proteção (hardware e software), bem como medidas de seguranças atualizadas não foi possível impedir um ciberataque ao banco de dados do sistema público, logo estaríamos diante de uma hipótese inevitável, ou seja, lastreada em um caso fortuito ou força maior que por sua vez já afastaria o nexo causal.

De toda sorte, inúmeros casos são constatados relativo à ações judiciais que se arrastam na Justiça por parte dos usuários lesados em busca de reparação civil, em razão do mau uso dos dados pessoais e da ingerência dos administradores, cabendo demonstrar ainda que a maioria das discussões estão centralizadas sobre o setor privado.

Tanto o setor público quanto o privado armazenam elevada quantidade de dados e informações, importando apresentar um fato de bastante interesse ao presente trabalho, qual seja: relativo à venda de dados pessoais por empresas ligadas ao Governo.

Dessa maneira, empresas com contratos junto ao sistema do Governo possuem livre acesso aos dados pessoais obtidos a título de políticas públicas, que em muitos casos são utilizados para alcançar alguma vantagem ao seu detentor, a exemplo de vantagens auferidas nas eleições dos Estados Unidos.

Nessa perspectiva, é possível identificar uma realçada dicotomia entre a "melhoria das políticas públicas" e à "privacidade dos indivíduos", uma vez que o Governo precisa coletar dados das pessoas para efetivar seus programas e projetos e, ao mesmo tempo, devido a sua ingerência, instaura uma margem para que pessoas da administração pública de má-fé tenha acesso à esses dados com a finalidade de obter vantagens. (GONÇALVES, 2019, p. 20).

O poder público encontra diversas dificuldades para trabalhar a presente discussão, uma vez que uma regulamentação restritiva acerca da abordagem sobre os dados pessoais traria uma blindagem ao setor público que impossibilitaria o setor da inovação, impedindo que a máquina pública tenha uma atualização na forma de trabalho. Nota-se a necessidade de se trabalhar o tema nos órgãos públicos com firmeza, atentando-se para a importância do equilíbrio entre a obtenção desses dados e sua concessão lastreada pelo consentimento do internauta, acompanhada de uma boa fiscalização e investimento em infraestrutura que possibilite a ampliação de proteção mínima aos bancos de dados.

Em discussão parece prático solucionar o problema, todavia, essas propostas de melhorias apresentadas são desafiadoras ao âmbito governamental na atual sociedade da informação[8]. O setor público precisa aprimorar novas práticas e implementar políticas capazes de usufruir todas as possibilidades que os recursos tecnológicos nos permite. Eis a necessidade de investimento na máquina pública para se ter um bom desempenho em sua atividade, superando aquele velho estigma de que na administração pública faltam recursos tecnológicos de qualidade e que as falhas só acontecem por falta de investimento.

Não é nada forçoso constatar que hodiernamente vivemos em uma sociedade pautada na informação, cabendo demonstrar que a entrega de bons resultados neste âmbito em que a tecnologia dita as regras vai depender diretamente de um bom aparato legislativo, bem como de um maquinário e recursos humanos de qualidade para que seja possível um gerenciamento preventivo e, diante das eventualidades, se ter uma boa capacidade de resposta ao solucionar qualquer problema que venha surgir na esfera de tratamento de dados pela administração pública.

Mediante ao exposto, no que diz respeito à atuação do Poder Público, nota-se a necessidade de ampliação de sua capacidade de atualização e adaptação de sistemas tecnológicos para que seja possível aproveitar os recursos disponíveis e atender as demandas de políticas públicas sem colocar em xeque o direito à privacidade do cidadão-usuário da rede global de internet.

O mau uso ou a divulgação indevida dos dados pessoais sensíveis e não sensíveis causa sérios prejuízos políticos, ações de danos morais, bem como a perda da credibilidade de um governo que realiza a captação de dados da população.

Por isso, urge trazer à baila a necessidade de inclusão da administração pública nos novos conceitos, terminologias e regras disciplinadas pela LGDP.

3. DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO - LEI Nº 13.709/18

A Lei Geral de Proteção de Dados destinou os arts. 23 ss. do Capítulo IV especialmente para regular o tratamento de dados pessoais pela administração pública, cuja inteligência dos artigos possibilita a interpretação de que seria mais fácil o tratamento e compartilhamento de dados pessoais e sensíveis pelos órgãos e entidades públicas.

O referido privilégio concedido ao setor público é identificado em várias passagens da LGPD, a exemplo do art. 7º c/c a al. "b" do inc. II do art. 11., acerca do tratamento de dados pessoais sensíveis, onde se é possível identificar a dispensa do consentimento por parte do titular na hipótese da administração pública solicitar os dados pessoais para efetivação de políticas públicas quando estas estiverem previstas em leis e regulamentos ou quando respaldadas em contratos, convênios ou instrumentos jurídicos semelhantes.

Vale dizer ainda que as diretrizes do art. 23 da LGPD obriga os órgãos públicos e entidades a darem a devida e ampla publicidade à dispensa de consentimento.

Essa autorização ao setor público se não feito com a devida gerência acarreta a diversos riscos aos agentes envolvidos, e por isso, vários aspectos precisam de observância a LGPD, a exemplo dos riscos de segurança na disponibilização dos dados; aspectos sobre a avaliação dos mecanismos de controle de divulgação das informações provenientes dos dados acessados; a responsabilização da Administração do gestor ou do usuário no caso de eventual vazamento de informações ou de revelação indevida, além de questões específicas relacionadas à tecnologia da informação e à disponibilidade de recursos humanos especializados.

Portanto, as diretrizes para o tratamento de dados pessoais no setor público foram inseridas no art. 23 da Lei nº 13.709/18, que dispõe:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
>
> (...)
>
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019)
>
> (...)
>
> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
>
> § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
>
> § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
>
> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
>
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Em continuidade, afirma-se com elevada certeza que a tutela dos direitos pessoais e sensíveis pela Administração Pública se apresenta de modo insatisfatório, pois, em se tratando de base de dados geridas pelo governo é notória a deficiência quanto à blindagem do sistema, bem como a publicidade e transparência quanto a gestão, tratamento e disponibilização de dados pessoais e sensíveis mesmo com todas as regras e diretrizes apresentadas pelo art. 23 da LGPD.

Como o próprio caput prevê, deverá ser realizado o tratamento de dados para o atendimento de sua finalidade pública, na percepção do interesse público, com o objetivo de executar as competências legais das atribuições legais do serviço público, podendo-se assim compreender que o poder público atuará como controlador e operador do tratamento de dados. E para que esse tratamento seja lícito, deverá obedecer aos princípios e à boa-fé previstos no art. 6º desta lei, e o poder público deverá ainda indicar um encarregado, que poderá ser pessoa física ou jurídica, quando realizarem o tratamento de dados, que atue como canal de comunicação para as relações entre o controlador, o titular e a autoridade nacional (GUIMARÃES, 2020, p. 37).

Na sociedade do conhecimento em que vivemos marcados pelo avanço tecnológico, os dados estão em constante circulação pela maior facilidade em seu acesso, sendo a todo momento por diversos agentes, coletados, armazenados, tratados e geridos no âmbito público e privado. A linguagem própria do mecanismo digital, a complexidade e técnicas próprias da tecnologia, com algoritmos e códigos que só programadores entendem, engloba questões de segurança da informação a nível mundial e evidentemente inovações que os operadores jurídicos não compreendem em sua totalidade. Ademais, cumpre demonstrar alguns exemplos das inovações que o profissional do direito possui elevada dificuldade em manusear e que demonstra a necessidade do setor público identificar profissionais de excelência para as questões, quais sejam: mecanismos de processamento nas tecnologias do e-commerce, gestão de patente e direitos autorais, *blockchain*, *cloud computing*, realidade aumentada, inteligência artificial, dentre outros.

Por isso, a regulação desses meios acaba por ser demasiadamente complexa, pelo fato do jurista não compreender as fases desses processos e sua aplicação na dinâmica do órgão público. Eis a necessidade de um trabalho conjunto do profissional da área e os operadores do direito.

4. ANÁLISE DE CASE: ATAQUE CIBERNÉTICO À BASE DE DADOS DE PROCESSOS DO SUPERIOR TRIBUNAL DE JUSTIÇA

Em novembro de 2020 ocorreu um marcante ataque cibernético realizado contra o sistema de tecnologia da informação do Superior Tribunal de Justiça, instituição pública de renome que armazena milhares de dados pessoais sensíveis acerca de processos judiciais físicos e eletrônicos.

O referido ataque foi apresentado como uma invasão à rede informática do órgão público, cuja atividade criminosa desencadeou a suspensão do funcionamento de diversas funções do Superior Tribunal de Justiça, a exemplo da suspensão de julgamentos por videoconferências, sessões virtuais e audiências. Vale dizer ainda que houve mudança no calendário forense haja vista a instauração da suspensão supramencionada.

De forma prática, o ataque cibernético configurou o bloqueio de processos e endereços de e-mails do STJ, o que eventualmente levou à suspensão das sessões de julgamento uma vez que essas audiências são agendadas e disponibilizadas no e-mail e no processo judicial eletrônico.

Nessa perspectiva, configurou-se a infecção de um *malware*, com similaridade ao ransomware, cuja finalidade é a efetivação do sequestro do sistema da vítima, com eventual bloqueio e criptografia dos dados. Dessa forma, o hacker realiza a cobrança de um valor pecuniário em prol da devolução do acesso aos dados.

Não é nada forçoso constatar que um ataque dessa magnitude poderia causar danos irreversíveis à sistemática eletrônica do Superior Tribunal de Justiça, bem como aos dados pessoais presentes no banco de dados da referida administração pública.

Os dados presentes nesse ataque em sua maioria são considerados informações confidenciais e de conteúdo sensível e, restou claro que o agente causador deste ataque obteve acesso aos "dados sensíveis", a depender da forma e quantidade obtida, poderia compartilhar esses dados a terceiros afetando diretamente o bem juridicamente tutelado pela Lei Geral de Proteção de Dados, qual seja: o direito à privacidade[8] garantido no art. 5º, inciso X da Constituição Federal, bem como no art. 21 do Código Civil.

O referido ataque cibernético foi objeto de investigação em inquérito instaurado pela Polícia Federal. Muito se discute sobre a necessidade do malware ingressar no sistema pela atitude de algum facilitador, ou seja, um servidor público, ministro, estagiário que, por sua vez, tem acesso ao maquinário da instituição e, eventualmente, ingressa em um link/formulário que permite a invasão. Em se tratando de tecnologia da informação todos os pontos são relevantes para análise.

---

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

5. DO TRIDIMENSIONALISMO JURÍDICO DO JUSFILÓSOFO MIGUEL REALE

Em princípio, antes de ingressar na esfera das eventuais penalidades sobre a violação da privacidade do internauta em casos de vazamento de dados pessoais, façamos uma reflexão quanto à teoria tridimensional do direito.

A esse propósito, faz-se mister trazer à colação o entendimento do ilustre Miguel Reale que assevera:

(...)

"o Direito é uma integração normativa de fatos segundo valores". (REALE, 1994, p. 119)

O presente autor nos ensina que o Direito inicia-se no fato até o valor que, eventualmente, culmina na norma. Significa dizer que sobre um fato incidirá um complexo de interesses ou valorações que exigem uma disciplina normativa.

Em conformidade com o caso em tela, aplica-se ao aspecto fático (fato) a violação ao bem juridicamente tutelado na presente discussão, qual seja: (direito à privacidade) que por sua vez, é o (valor) buscado pela sociedade, necessitando dessa forma de tutela pelo ordenamento jurídico através da (norma), Lei nº 13.709/18 - LGPD (Lei Geral de Proteção de Dados). (REALE, 1994, p. 89)

A partir dessa leitura é possível identificar todos elementos para a boa interpretação do direito como fenômeno jurídico, entendendo melhor o fato social, a valoração atribuída pela sociedade a um determinado direito e, por fim, a norma reguladora da relação jurídica.

6. EVENTUAIS PENALIDADES, SANÇÕES E MULTAS

Os dados pessoais sensíveis possuem grande relevância para o ordenamento jurídico, sendo de fundamental importância que agentes de tratamentos observem as diretrizes legais sob pena de sanções nos casos de violação de direitos e liberdades individuais.

A exposição indevida de um dado pessoal sensível pode resultar em uma triste repercussão ao titular, tanto na vida social quanto profissional.

Na hipótese de violação da liberdade individual ou até mesmo da privacidade do titular, nos casos em que um agente delituoso invade um dispositivo informático, tem-se o delito previsto no art. 154-A do Código Penal Brasileiro, com especial aplicação do §3º e §4º do referido artigo para presente discussão.

Senão vejamos:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
>
> (...)
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012)
>
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

Nessa perspectiva, nota-se que o presente artigo esboça implicações relevantes acerca do delito de crimes cibernéticos, tendo como elementos objetivos do tipo invadir dispositivo informático alheio, conectado ou desconectado da internet, causando violação indevida ao titular daqueles determinados dados pessoais (sensíveis ou não sensíveis), através de mecanismo que consiga burlar o sistema.

O elemento subjetivo está lastreado no dolo que se vincula à referida prática delituosa, com a finalidade de invadir, adulterar ou destruir dados ou informações, sem autorização do titular, com esteio no elemento subjetivo específico de auferir vantagem ilícita.

Ademais, ocorrendo a promoção de controle remoto por parte do agente delituoso, será aplicada a qualificação do teto da sanção penal de pena privativa de liberdade de até 2 (dois) anos, em conformidade com o parágrafo terceiro do referido artigo.

De outro lado, restando comprovada a mera transmissão a qualquer título, o parágrafo quarto supracitado configura uma majoração de pena na ordem de ⅓ (um terço) a ⅔ (dois terços) na terceira fase da dosimetria da pena.

Nesse diapasão, infere-se que a ação penal dos crimes de invasão de dispositivo informático com eventual subtração de informações sigilosas e dados pessoais sensíveis do

titular, necessariamente terá de observar o art. 154-B do Código Penal, relativo à ação penal pública condicionada à representação, cabendo a vítima manifestar a sua vontade. Nota-se que o legislador acertadamente vinculou o impulso da referida ação penal ao interesse da vítima, uma vez que nesses casos ocorre ofensa à vítima em sua intimidade, cabendo a esta promover a referida ação caso entenda necessário.

Por outro lado, acerca da responsabilidade dos administradores da empresa controladora dos dados, para imputação de uma responsabilidade deverá ser observado o nexo de causalidade e resultado. Ao passo que as sanções administrativas decorrentes da falta de adequação à LGPD resultaria em multas de até 2% do faturamento, com limite de R$ 50 milhões, com bloqueio ou eliminação de dados tratados irregularmente e, até mesmo, a suspensão ou proibição do banco de dados ou da atividade de tratamento.

7. CONCLUSÃO

Mediante ao exposto, restou comprovada a necessidade do poder público tratar e processar os dados pessoais na estrita forma descrita em lei, em conformidade com as boas práticas e infraestrutura tecnológica adequada, respeitando o consentimento do titular, classificado pela lei como a manifestação livre, informada e inequívoca do sujeito que autoriza para finalidade específica, salvo nas hipóteses em que são utilizados dados anonimizados para efetivação de políticas públicas.

A busca por um maior padrão de segurança gera mais confiança no desenvolvimento da economia digital no conjunto do mercado interno do Brasil e permite que o ente público consiga cumprir com seu dever de manutenção da segurança institucional. (LECIO, P. 103)

O direito à privacidade se apresentou no presente estudo como um bem juridicamente tutelado de grande relevância, sendo de fundamental importância que os operadores do direito e estudiosos continuem ampliando os conhecimentos acerca do tema para que exclua eventuais formas de violação de dados pessoais relativo à pessoa e possíveis injustiças quanto exposição da intimidade e honra dos usuários, levando a sociedade informação quanto ao presente tema.

A observância desses elementos permite ao setor público a possibilidade de ampliação da proteção da existência eletrônica da pessoa “dados pessoais sensíveis”, resultando em uma evolução tecnológica que permite o estabelecimento de um padrão de sistema com regras sólidas e coerentes com a realidade.

Em conclusão, infere-se que o Direito é uma ciência autocorretiva e, eventualmente, está sempre um passo atrás da sociedade e sua dinâmica de desenvolvimento. Dessa forma, o campo jurídico tem procurado suprir as necessidades de adaptação aos ambientes virtuais. A sociedade identificou a necessidade de regulamentação, resultando na criação da Lei de Acesso à Informação, no Marco Civil da Internet, no Código de Defesa do Consumidor, bem como na Lei Geral de Proteção de Dados. Diante disso, é necessário entender o ingresso da sociedade em um novo patamar de produção de bens e serviços. Hodiernamente, vivemos em uma sociedade da informação, onde constantemente ocorre a geração, o armazenamento e a transferência das informações instantaneamente, sendo que as novas tecnologias agregam valor à informação.

Conforme já apresentado no decorrer do estudo, a identificação do indivíduo é algo relevante para nossa vida em sociedade. Os elementos de identificação do indivíduo devem ser protegidos pela legislação vigente e fiscalizada pelo setor público, pelo qual tem o dever de agir em prol da segurança institucional e do direito à privacidade que por sua vez está lastreado na Constituição Federal de 1988.

É nosso entendimento que os órgãos públicos devem funcionar na sociedade como "garante" na proteção dos dados pessoais sensíveis, por se tratar de uma extensão do Estado, uma organização centrada no ser humano, e não qualquer outro referencial. A razão de ser do Estado brasileiro não se funda na propriedade, em classes, em corporações, em organizações religiosas ou tampouco no próprio Estado, mas sim na pessoa humana. Os direitos fundamentais foram inseridos na Constituição de 1988, sob essa perspectiva, a serem realizados, mediante ou imediatamente, pela forma do Estado Democrático de Direito.

8. REFERÊNCIAS

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: <Constituição (planalto.gov.br)> Acesso em: 01 nov. 2021.

Reale, Miguel. **Teoria tridimensional do direito/ Miguel Reale** - 5 ed. - São Paulo: Saraiva, 1994. Disponível em: <https://doi.org/10.11606/issn.2318-8235.v88i0p301-312> Acesso em: 01 nov. 2021.

GUIMARÃES, João; MACHADO, Lecio; **Comentários à Lei Geral de Proteção de Dados**. Lei 13.709/2018 com alterações da MPV 869/2020. Rio de Janeiro: Lumen Juris, 2020.

BRASIL. Lei 12.965/14 (**Marco civil da internet**). 2014. in <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 01 nov. 2021.

BRASIL. CÓDIGO CIVIL. LEI Nº 10.406 DE 10 DE JANEIRO DE 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm>. Acesso em: 01 nov. 2021.

BRASIL. CÓDIGO PENAL. LEI Nº 2.848 DE 7 DE DEZEMBRO DE 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 01 nov. 2021.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor. Brasília**, DF, setembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm>. Acesso em: 01 nov. 2021.

GONÇALVES, Tânia Carolina Nunes Machado. **Gestão de Dados Pessoais e Sensíveis pela Administração Pública Federal: desafios, modelos e principais impactos com a nova Lei**. Orientador Prof. Dr. Marcelo Dias Varella. - Brasília, 2019. in <https://www.uniceub.br/arquivo/144ng_20190730051313*pdf?AID=3007> Acesso em: 01 nov. 2021.

MENDONÇA, Suzana. **A boa fé na atividade administrativa**. e-Pública. 2018, vol. 5, n.1,pp.175-209.ISSN2183-184Xin<http://www.scielo.mec.pt/scielo.php?script=sci_artte xt&pid=S2183-184X2018000100010> Acesso em: 01 nov. 2021.

RUDZIT, Gunther. NOGAMI, Otto. **Segurança e defesa nacionais: conceitos básicos para uma análise**. Rev. bras. polit. Int. vol.53, Brasília. Jan/July, 2010, in <https://doi.org/10.1590/S0034-73292010000100001> Acesso em: 01 nov. 2021.

CONJUR. **TRF-3 sofre ataque hacker nesta sexta-feira, 2021**. Disponível em: <https://www.conjur.com.br/2021-jan-15/trf-sofre-ataque-hacker-nesta-sexta-feira>

CASTRO, Luiz Fernando Martins. **Proteção de dados pessoais-panorama internacional e brasileiro**. Revista CEJ, v. 6, n. 19, p. 40-45, 2002.

D´AQUINO, Fernando. **A história das redes sociais: como tudo começou**. Disponível em: <www.tecmundo.com.br>. Acesso em: 01 nov. 2021.

O que são dados pessoais? Comissão Européia. Disponível em: <Proteção de dados | Comissão Europeia (europa.eu)> Acesso em: 01 nov. 2021.

TOSTES, Marcelo. **Segurança de dados na Internet: como proteger a sua empresa?**2019. Equipe Marcelo Tostes. Disponível em: <https://transformacaodigital.com/juridico/segurancade-dados-na-internet-como-protege r-a-sua-empresa/.> Acesso em: 01 nov. 2021.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2018.

CAVALIERI FILHO, Sérgio. **Programa de responsabilidade civil**. 11. ed. São Paulo: Atlas, 2014.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies**. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal de Uberlândia, Minas Gerais, 2018.

LANCHESTER, John. **Você é o produto:** Mark Zuckerberber e a colonização das redes pelo Facebook. Revista Piauí, 2017. Disponível em: <https://piaui.folha.uol.com.br/materia/voce-e-o-produto/>. Acesso em: 01 nov. 2021.

ANCELIER, Mikhail Vieira de Lorenzi. **Infinito particular: Privacidade no século XXI e a manutenção do direito de estar só**. Florianópolis, 2016.

NETWORKS, Telium. **Confidencialidade, integridade e disponibilidade: os três pilares da segurança da informação**. 2018. Disponível em: <https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres pilares-da-seguranca-da-informacao.> Acesso em: 01 nov. 2021.

STJ Notícias destaca reforço na segurança de informações digitais do tribunal após o ataque hacker. Disponível em: <STJ Notícias destaca reforço na segurança de informações digitais do tribunal após o ataque hacker> Acesso em: 01 nov. 2021.

39 dias após o ataque cibernético ao STJ: reflexões e desafios - Migalhas. Disponível em: <39 dias após o ataque cibernético ao STJ: reflexões e desafios - Migalhas> Acesso em: 01 nov. 2021.

Possíveis reflexos penais da Lei Geral de Proteção de Dados - Migalhas. Disponível em: <Possíveis reflexos penais da Lei Geral de Proteção de Dados (migalhas.com.br)> Acesso em: 01 nov. 2021.

O tridimensionalismo de Miguel Reale. Jus.com.br. Disponível em:<O tridimensionalismo de Miguel Reale - Jus.com.br | Jus Navigandi> Acesso em: 01 nov. 2021.

BIONI e Ricardo, B, Proteção de Dados Pessoais - **A Função e os Limites do Consentimento**, Rio de Janeiro, 2019.

PINHEIRO e Peck, P. Proteção de dados pessoais - **comentários à Lei n. 13.709/2018** LGPD, São Paulo, 2018.

BOTELHO, Marcos César. **A LGPD e a Proteção ao Tratamento de Dados Pessoais de Crianças e Adolescentes**. Revista Direitos Sociais e Políticas Públicas, [S.l.], v. 8, n. 2, 2020. Disponível em: <https://doi.org/10.25245/rdspp.v8i2.705>. Acesso em: 01 nov. 2021.

BRASIL. Lei 13.709, de 14 de agosto de 2018 (LGL\2018\7222). **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm]. Acesso em: 01 nov. 2021.