FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

MATHEUS CORONA PATRICIO

PROTEÇÃO DO SEGREDO COMERCIAL E INDUSTRIAL À LUZ DA TUTELA DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

VITÓRIA/ ES
2023

MATHEUS CORONA PATRICIO

PROTEÇÃO DO SEGREDO COMERCIAL E INDUSTRIAL À LUZ DA TUTELA DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Monografia escrita e apresentada ao curso de Graduação em Direito da Faculdade de Direito de Vitória (FDV), como requisito parcial para obtenção do grau de bacharel em Direito, sob a orientação do Professor Me. Bruno Costa Teixeira.

VITÓRIA/ ES

2023

MATHEUS CORONA PATRICIO

PROTEÇÃO DO SEGREDO COMERCIAL E INDUSTRIAL E A TUTELA DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Monografia escrita e apresentada ao curso de Direito da Faculdade de Direito de Vitória (FDV), como requisito parcial para obtenção do grau de bacharel em Direito, sob a orientação do Professor Me. Bruno Costa Teixeira.

Aprovada em ___ de junho de 2023.

COMISSÃO EXAMINADORA

_____

Professor Me. Bruno Costa Teixeira.
Faculdade de Direito de Vitória
Orientador

_____

Professor(a)
Faculdade de Direito de Vitória

_____

Professor(a)
Faculdade de Direito de Vitória

AGRADECIMENTOS

Em primeiro lugar, a Deus, que fez com que meus objetivos fossem alcançados, durante todos os meus anos de estudos.

Aos meus pais Solange Corona e Carlos Patricio e meus irmãos por todo apoio e pela ajuda, especialmente nos momentos difíceis, que muito contribuíram para minha formação, assim como para a realização deste trabalho.

Agradeço ao professor Mestre Bruno Costa Teixeira, por ter sido meu orientador e ter desempenhado tal função com dedicação e empenho. Bem como aos professores Doutor Adriano Sant'Ana Pedra e Doutora Bruna Lyra Duque, os quais fui monitor na graduação e me auxiliaram nessa trajetória.

Agradeço também aos amigos que fiz no curso de Direito da Faculdade de Direito de Vitória - FDV. Especialmente a Brunela Chiabai do Nascimento, Gabrielle Andriêta Carvalho e Júlia Weygand Siqueira Pereira, que proporcionaram momentos únicos.

Agradecimentos ao Escritório Mendonça & Machado Advogados, especialmente nas pessoas de Gustavo Martins Rossetti e Daniel Lube Martinelli, que muito me ensinaram e certamente contribuíram para a conclusão deste estudo.

Agradecimentos à Empresa Júnior de Direito de Vitória - EDV Jr. que, além de proporcionar a prática no mercado, me inseriu no tema de Propriedade Intelectual.

Agradeço, por fim, à Faculdade de Direito de Vitória - FDV, essencial no meu processo de formação acadêmico-profissional.

“A liberdade não tem preço, a mera possibilidade de obtê-la já vale a pena”.

Isaac Asimov

RESUMO

O estudo aqui apresentado tem como objetivo constatar se utilizando-se da Lei Geral de Proteção de Dados (LGPD) existe pretexto por parte dos agentes de tratamento de dados pessoais de descumprirem a legislação, quanto ao atendimento às solicitações dos titulares, em razão do conflito à proteção dos segredos comerciais e industriais. Será traçado, em primeiro plano, direcionamentos principiológicos e dogmáticos sobre a legislação de proteção de dados pessoais, assim como da Lei de Propriedade Intelectual, no que dispõe à concorrência desleal para posteriormente compreender a subdivisão da propriedade intelectual. Por fim, serão destacados diversos exemplos de utilização do *Privacy by Design*, método desenvolvido para proporcionar a proteção de dados aos usuários desde a concepção. Para tanto, foi pesquisada doutrina brasileira sobre o tema, além de casos e decisões recentes, de modo que foi possível que não há qualquer pretexto para a realização de tratamento de dados pessoais desmedido e sob o pressuposto do não atendimento aos titulares de dados pessoais em decorrência da proteção, pela LGPD, aos segredos comerciais e industriais.

Palavras-chave: Segredo Comercial e Industrial; Proteção de Dados; P*rivacy by Design*.

ABSTRACT

The study presented here aims to ascertain whether the use of the General Data Protection Law (LGPD) provides a pretext for data controllers to violate the legislation regarding compliance with data subject requests due to the conflict with the protection of trade secrets and industrial secrets. First and foremost, principled and dogmatic guidelines will be outlined regarding personal data protection legislation, as well as the Intellectual Property Law concerning unfair competition, in order to subsequently understand the subdivision of intellectual property. Finally, various examples of the use of Privacy by Design will be highlighted, a method developed to provide data protection to users from the conception stage. To this end, Brazilian doctrine on the subject was researched, as well as recent cases and decisions, enabling the conclusion that there is no pretext for excessive processing of personal data and the failure to comply with data subject requests due to the protection, provided by the LGPD, of trade secrets and industrial secrets.

Keywords: Commercial and Industrial Secret; Data Protection Law; Privacy by Design.

LISTA DE FOTOGRAFIAS

SUMÁRIO

1 INTRODUÇÃO

Após a promulgação da Lei Geral de Proteção de Dados (LGPD – Lei número 13.709/2018), diversas práticas comerciais passaram a ser analisadas sob uma nova ótica, a da proteção de dados. Antes um assunto relegado, a proteção de dados levanta diversas discussões, sendo considerado um direito fundamental, elencado no rol do artigo 5º, inciso LXXIX, da Constituição da República Federativa do Brasil. Além disso, com a fiscalização e a possibilidade de aplicação de multas, que podem chegar a patamares milionários, cerca de R$50 milhões de reais por infração[1], as empresas de direito privado revelam um olhar mais atento a toda forma de tratamento de dados pessoais.

De modo geral, os dados pessoais são conceituados na lei como sendo informações relacionadas à pessoa natural identificada ou identificável (artigo 5º, I, da LGPD). Motivo pelo qual, qualquer informação fornecida, por mais simples que seja, poderá ser considerada como dado pessoal, como nome, idade, registro geral, cadastro de pessoa física, número de telefone, conta de e-mail, entre diversos outros. Ocorre que todo tratamento de dados pessoais deve ser realizado sob os parâmetros de uma base principiológica, conforme elencados no artigo 6º da LGPD. No caso deste estudo, o recorte será quanto aos princípios do livre acesso, da transparência, assim como da não discriminação.

O primeiro é uma garantia aos titulares dos dados pessoais que, quando necessário, poderão exercer seu direito de consulta, de modo facilitado e gratuito sobre a forma e a duração do tratamento realizado pela empresa, bem como a integralidade de seus dados pessoais, assumindo, desse modo, uma posição de protagonismo (PALHARES, 2021, p. 136). Já o princípio da transparência dispõe que as empresas precisam ser honestas com os titulares dos dados pessoais, devendo informar aos proprietários sobre os agentes de tratamento que exercem quaisquer níveis de controle sobre o fluxo informacional de seus dados (PALHARES, 2021, p. 137).

[1] "Artigo 52, da LGPD. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [...]. II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;".

Quanto ao último princípio analisado neste trabalho, tem-se que os dados pessoais coletados jamais poderão ser objeto de tratamento discriminatório.

Em outra perspectiva, destaca-se a Lei de Propriedade Intelectual (LPI - Lei número 9.279/1996), a qual regula as normas relativas à proteção e defesa dos direitos e obrigações inerentes à propriedade intelectual em todo o território nacional. Tal lei tem como objetivo estimular a inovação e a criatividade, bem como fomentar o desenvolvimento econômico e tecnológico do país, abordando, ainda que de forma sucinta a proteção de segredos comerciais e industriais.

Assim, esta pesquisa parte da seguinte questão-problema: há pretexto por parte dos agentes de tratamento de dados pessoais para o descumprimento da LGPD, quanto ao atendimento às solicitações de titulares, em razão do conflito à proteção do segredo comercial e industrial?

A partir do problema de pesquisa elaborado acima, pretende-se, neste trabalho, verificar a hipótese no sentido de que tendo em vista que a legislação de proteção de dados pessoais não especificou quais informações devem ser repassadas aos titulares dos dados pessoais poderia o controlador deixar de fornecer informações aos titulares.

Desse modo, a presente monografia analisa a questão acima através do método hipotético-dedutivo, construindo premissas com alta probabilidade de serem verdadeiras e fidedignas a compreensão proposta em tela, descartando tudo o que não for verdadeiro ou não adequado, utilizando-se o princípio do falseamento. (POPPER, 2013, p. 144)

A primeira parte explora a importância da privacidade e da proteção dos direitos autorais, evidenciando assim a necessidade de exploração do tema, ainda muito atual e com presença crítica na sociedade contemporânea. Já na segunda parte serão traçadas definições quanto à LGPD e LPI, analisando ambas as legislações do ponto de vista de alcance e conteúdo, não sendo objeto deste estudo a pormenorização dos institutos de cada texto legislativo. Posteriormente, a compreensão do segredo

comercial e industrial sob a ótica da LGPD e, por fim, a contribuição do *privacy by design* (PbD)[2] com o tema em estudo na visão do autor.

O objetivo deste estudo é a contribuição com temas correlatos, não apenas na área do direito, tendo em vista a ramificação do tema com o avanço da globalização no mundo contemporâneo, seja com o crescimento no fluxo de dados ou na criação de sistemas autônomos e automatizados com capacidade de processamento de dados, especialmente com o objetivo de perfilização, constituindo o segredo comercial e industrial de diversas empresas, mas que deve ser ponderado para evitar ataques aos titulares de dados pessoais, não devendo, observado outro ponto de vista, ser banalizado a proteção aos segredos de negócios das empresas, que constituiu forte proteção ao livre mercado.

[2] “Privacidade por *design*” (Tradução livre).

2 A IMPORTÂNCIA DA PRIVACIDADE E DA PROTEÇÃO DOS SEGREDOS COMERCIAIS

O termo privacidade é um conceito que remonta à antiguidade e que adquiriu diversas nuances ao longo do tempo. Desde os tempos remotos as pessoas já tinham a noção de que certas informações deveriam ser mantidas em sigilo, fato que é presente até os dias atuais, demonstrando a relevância do tema para a humanidade. No entanto, foi com o advento da modernidade e a consolidação do Estado liberal que a privacidade passou a ser vista como um direito fundamental dos indivíduos. O filósofo inglês John Locke, em sua obra "Dois tratados sobre o governo" (LOCKE, 2006), publicada em 1689, defendeu a ideia de que os indivíduos têm o direito à vida, à liberdade, à resistência à tirania e à propriedade, influenciando diretamente a concepção moderna de privacidade.

No século XIX, com o desenvolvimento das tecnologias de comunicação, surgiram novas preocupações em relação à privacidade, motivo pelo qual ela passou a se fazer notar pelo ordenamento jurídico (DONEDA, 2006, p. 07). A partir do telégrafo, por exemplo, as pessoas passaram a temer que suas conversas fossem interceptadas por terceiros, o que demandou a criação de mecanismos de proteção das comunicações à época. No entanto, foi com o surgimento da fotografia e do cinema que as preocupações em relação à privacidade se intensificaram, uma vez que essas tecnologias permitiam a captura e a reprodução de imagens sem o consentimento das pessoas.

Entretanto, até o final do século XIX o indivíduo que tivesse sua privacidade violada não obteria grande sucesso perante os tribunais, como dos Estados Unidos e da Inglaterra. Isso porque as principais cortes estavam ocupadas apenas em reparar situações de violência ou de ataques à propriedade privada, ficando de lado direitos imateriais (RODRIGUEZ, 2021, p. 37).

Já no século XX, com o desenvolvimento da informática e a popularização em massa da internet, assim como o advento de *smartphones* e redes sociais, as preocupações em relação à privacidade se tornaram ainda mais relevantes. Com a facilidade de

coleta e compartilhamento de informações pessoais na rede, as pessoas passaram a ter medo de que suas informações fossem utilizadas de forma indevida.

Hodiernamente, os problemas relacionados à privacidade apenas aumentam, ainda mais quando associados a superestruturas obscuras de monitoramento como o *big brother* de Orwell (DONEDA, 2006, p. 17), inserido no capitalismo de vigilância, um novo sistema econômico que molda as relações existentes na modernidade e emergiu com o avanço das chamadas *big techs*, isto é, empresas capazes de criar demandas anteriormente não pensadas pela humanidade através de investimentos de grande monta e recolhimento massivo de dados pessoais com o uso cotidiano da internet por bilhões de usuários, com cerca de 51% do mundo está conectado (VALENTE, 2019, *on-line*).

Diante desse cenário, surgiram diversas iniciativas para proteger a privacidade dos usuários da internet, como a criação de leis específicas mundo afora para o tratamento de dados pessoais. Destaca-se, nesse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a Lei de Privacidade do Consumidor (CCPA) da Califórnia, nos Estados Unidos da América. Essas leis estabelecem regras para a coleta, o armazenamento, o processamento e o compartilhamento de dados pessoais, com o objetivo de garantir a privacidade e a segurança dos usuários.

A privacidade em todas as suas facetas não é um direito absoluto, pois existem situações em que é necessário abrir mão desse direito em prol do interesse coletivo, como nos casos de investigações criminais ou de saúde pública. No entanto, é fundamental que as limitações à privacidade sejam estabelecidas de forma clara e objetiva, respeitando os princípios do livre acesso, da transparência, assim como da não discriminação, norteadores deste trabalho.

Como indicado anteriormente, a privacidade é um direito fundamental dos indivíduos que evoluiu ao longo do tempo e que adquiriu novas dimensões com o avanço das tecnologias. A proteção da privacidade é essencial para garantir a dignidade e a autonomia dos indivíduos, mas deve ser equilibrada com outros direitos e interesses

da sociedade, uma vez que não é um direito absoluto, podendo ser limitado pelo exercício de outro direito fundamental (CORAZZA, 2022, p. 243-282).

A aplicação da LGPD tem gerado conflitos com a proteção do segredo comercial e industrial, sendo esses outros direitos e interesses da sociedade contemporânea. Assim, as empresas têm o direito de proteger seus segredos empresariais e manter a competitividade no mercado e, em muitos casos, o compartilhamento dessas informações pode ser prejudicial aos negócios. Nesse sentido, a LGPD estabelece a subordinação do direito ao esclarecimento dos titulares de dados pessoais ao segredo comercial e industrial. Isso significa que as empresas podem se recusar a fornecer informações que possam comprometer sua posição no mercado.

Não há proibição pela LGPD, como se sabe, na coleta e o uso de dados pessoais pelas empresas, mas sim o estabelecimento de regras claras para a utilização dessas informações, garantindo aos cidadãos do direito de saberem como seus dados estão sendo tratados, de modo que a subordinação criada pela LGPD ao atendimento das solicitações de esclarecimentos deve ser avaliada caso a caso, com o objetivo de evitar qualquer dano a ambas as partes envolvidas, garantindo um equilíbrio entre a proteção da privacidade e o segredo empresarial.

3 DEFINIÇÕES À LEI GERAL DE PROTEÇÃO DE DADOS

Como se sabe, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em setembro de 2020, inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Seu objetivo basilar é assegurar o direito fundamental à privacidade de proteção de dados, como decidido pelo Supremo Tribunal Federal (STF) (MENDES, 2022). Posteriormente houve, no caso do brasileiro, avanço legislativo para que conste previsão expressa de um direito fundamental *sui generis* à proteção de dados pessoais, incluído pela Emenda Constitucional número 115, de 2022.

> [...]
> Artigo 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: [...]
> LXXIX - é assegurado, nos termos da lei, o **direito à proteção dos dados pessoais**, inclusive nos meios digitais. (Grifou-se)
> [...]

A LGPD estabelece que dados pessoais (artigo 5º, I) são quaisquer informações que permitam identificar uma pessoa natural, de modo direto ou indireto, como nome, endereço, número de telefone, endereço de e-mail, entre outros. Ela é aplicável a qualquer pessoa física ou jurídica que colete, armazene, processe, compartilhe dados pessoais, isto é, realize tratamento de dados pessoais de indivíduos no Brasil, independentemente de sua nacionalidade ou localização.

Já os dados pessoais sensíveis (artigo 5º, II) são aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação e sindicato ou a organização de caráter religioso, filosófico ou político, assim como dados referentes à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. São aqueles dados pessoais que podem gerar contexto de discriminação, em respeito ao direito fundamental à igualdade.

Assim, a legislação brasileira adota uma abordagem de proteção de dados pessoais baseada nos direitos dos titulares de dados e determina dez princípios norteadores, sendo: a finalidade (artigo 6º, I), adequação (artigo 6º, II), necessidade (artigo 6º, III),

livre acesso (artigo 6º, IV), qualidade dos dados (artigo 6º, V), transparência (artigo 6º, VI), segurança (artigo 6º, VII), prevenção (artigo 6º, VIII), não discriminação (artigo 6º, IX), responsabilização e prestação de contas (artigo 6º, X). Além disso, a legislação versa que o tratamento de dados pessoais deve ser realizado de forma clara, precisa e acessível ao titular dos dados. No caso deste estudo, o recorte mais importante refere-se aos princípios do livre acesso, da transparência, assim como da não discriminação (MULHOLLAND, C. S. 2018. p. 163).

O princípio do livre acesso é uma garantia aos titulares dos dados pessoais que, quando necessário, poderão exercer seu direito de consulta, de modo facilitado e gratuito sobre a forma e duração do tratamento realizado, bem como a integralidade de seus dados pessoais, assumindo uma posição de protagonismo (PALHARES, 2021, p. 136). Já o princípio da transparência dispõe que as empresas precisam ser honestas com os titulares dos dados pessoais, devendo informar aos proprietários sobre os agentes de tratamento, isto é, empresas terceiras que operam os dados destes, exercendo quaisquer níveis de controle sobre o fluxo informacional de seus dados (PALHARES, 2021, p. 136). Quanto ao último princípio norteador deste trabalho, tem-se que os dados pessoais coletados não poderão ser objeto de tratamento discriminatório, isto é, visando a promoção de abusos contra seus próprios titulares.

Isso ocorre porque as infrações à legislação que podem vir a ocorrer em uma situação de tratamento irregular de dados pessoais atingem diversas esferas da vida de um cidadão, ora titular dos dados pessoais, comprometendo não somente a sua autonomia, mas também a individualidade (FRAZÃO, 2019, p. 47).

A LGPD estabelece a necessidade de obtenção do consentimento explícito dos titulares de dados para a coleta, uso e compartilhamento de seus dados pessoais. O titular dos dados tem o direito de solicitar a exclusão de seus dados a qualquer momento, bem como de receber informações claras e precisas sobre a finalidade do tratamento dos seus dados. Isso ocorre uma vez que é possível, por meio da coleta de informações triviais em plataformas digitais, revelar atributos da personalidade de um indivíduo, tais como orientação sexual, religiosa, política, racial, dentre outros

dados pessoais sensíveis (artigo 5º, inciso II, da LGPD). Assim, essas informações podem ser utilizadas para a elaboração de perfis, possibilitando por exemplo a realização de práticas discriminatórias com o uso inadequado dos dados pessoais.[3]

As empresas devem garantir que as informações que coletam sejam precisas, atualizadas e relevantes para a finalidade do tratamento dos dados, devendo tomar as medidas necessárias para proteger a segurança e a privacidade dos dados pessoais, evitando o acesso não autorizado, a divulgação ou a modificação desses dados.

A LGPD também estabelece a figura dos responsáveis por garantir a conformidade da empresa para com a legislação, sendo o encarregado de proteção de dados (*Data Protection Officer* - DPO) o designado para atuar como ponto de contato para os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), sendo um órgão Ffederal instituído como autarquia especial com autonomia administrativa e financeira, sem vinculações, responsável por zelar, implementar e fiscalizar o cumprimento integral da LGPD em todo território nacional.

Além disso, a legislação de proteção de dados é aplicável a todas as áreas da sociedade, incluindo o setor público e privado, e em todos os setores da economia, desde pequenas empresas até grandes corporações. A conformidade com a LGPD é obrigatória para todas as organizações que realizam qualquer tratamento com dados pessoais.

Diante disso, é fundamental que as empresas implementem medidas de conformidade com a legislação de proteção de dados. Isso ocorre porque a LGPD é uma legislação determinante para a proteção da privacidade e da segurança dos dados pessoais dos indivíduos no Brasil. Motivo pelo qual a conformidade com a lei deve ser respeitada

[3] Como afirma Bioni: “Coletam-se, cada vez mais, informações sobre um indivíduo, a fim de compor um perfil detalhado para alimentar análises preditivas a seu respeito. Isso equivale a classificá-lo e, até mesmo, segregá-lo. Da análise de crédito, do prêmio fixado na apólice de seguro ao anúncio publicitário na rede social, tais práticas estão se tornando corriqueiras, parametrizando as oportunidades de nossas vidas” (BIONI, 2020, p. 28).

pelas empresas, garantindo a transparência, a segurança jurídica e o respeito pelos direitos dos titulares de dados.

Para exemplificar a aplicação da LGPD, pode-se considerar o caso de uma empresa de comércio eletrônico que coleta informações dos seus clientes, como nome, endereço, e-mail, telefone, informações de pagamento, entre outras. Esses dados pessoais são coletados para realizar a venda dos produtos e serviços oferecidos pela empresa.

De acordo com a LGPD, a empresa é obrigada a informar aos seus clientes quais dados pessoais são coletados e para que finalidade são utilizados. Além disso, é necessário que a obtenha o consentimento livre e inequívoco do titular dos dados para o tratamento das informações coletadas. A empresa também é responsável por garantir a segurança dos dados pessoais, adotando medidas técnicas e organizacionais para prevenir acessos não autorizados, perda, destruição, ou qualquer forma de tratamento inadequado dos dados. A LGPD também assegura aos titulares de dados o direito de acessar, corrigir, excluir e portar seus dados pessoais. Se o titular solicitar a exclusão de seus dados pessoais, a empresa deve respeitar a sua vontade, salvo em casos específicos previstos em lei.

4 DEFINIÇÕES DA LEI DE PROPRIEDADE INDUSTRIAL

Em primeiro lugar, é importante distinguir a propriedade intelectual da industrial. A primeira é gênero, já a segunda uma de suas espécies, ao lado do ramo de direitos autorais – como direitos de autor e conexos – e da proteção *sui generis* – relacionada à topografia de circuitos integrados, aos cultivares e aos conhecimentos tradicionais.

A Lei da Propriedade Industrial (LPI), número 9.279 de 1996, é a legislação brasileira que regulamenta todas as formas de propriedade industrial no país. Ela estabelece, por exemplo, as regras para o registro e a proteção das patentes, marcas, desenhos industriais entre outros. Além disso, a lei também define as sanções aplicáveis em caso de violação, com o objetivo principal de proteger a inovação e a criatividade, incentivando a criação de novas tecnologias e produtos.

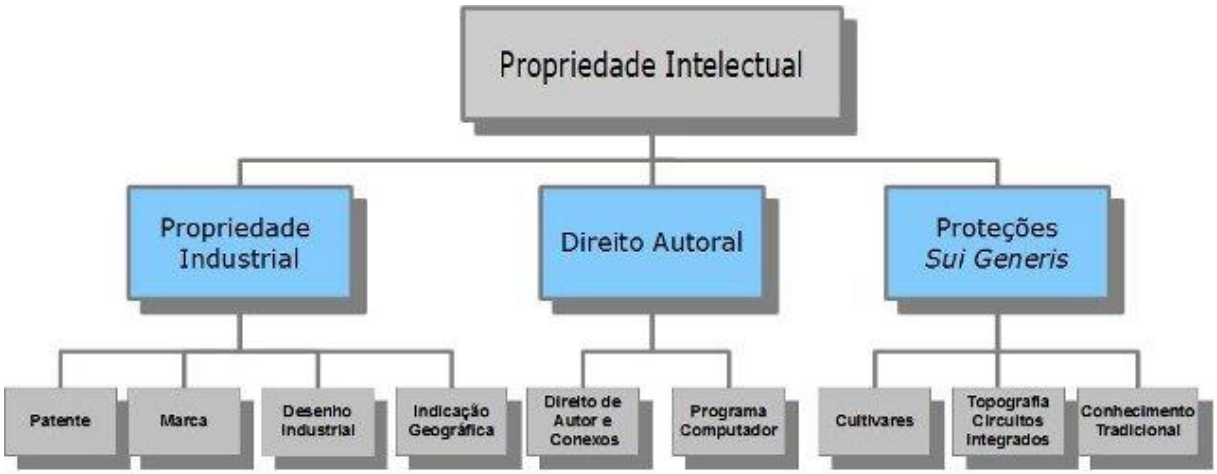
Assim, propriedade intelectual pode ser compreendida como sendo uma área do Direito que se dedica a regulamentar e proteger as diversas formas de propriedade intelectual. No contexto normativo, a propriedade industrial é vista como um direito exclusivo concedido aos criadores e inventores, visando estimular a inovação e a criatividade, além de possuir a vertente de promoção ao desenvolvimento econômico.

Já a propriedade industrial é composta de um conjunto de normas e regras que têm como objetivo proteger as criações e inovações das empresas e indivíduos, impedindo que outras pessoas ou empresas possam explorar essas criações sem autorização. Dentre as principais formas de propriedade industrial, temos as patentes, que garantem o direito exclusivo de explorar uma invenção por um período determinado, as marcas, que protegem símbolos, nomes e logotipos, os desenhos industriais, que regulam as características estéticas de um produto, as indicações geográficas, que protegem a origem geográfica de determinados produtos, e os segredos comerciais, que pode ser subdivido em duas ramificações.

O primeiro desdobramento é quanto aos contratos particulares que autorizam os colaboradores internos e externos das empresas a utilizarem de sua tecnologia, a qual muitas das vezes é protegida por meio do *Non Disclosure Agreement* (tipicamente

denominado de NDA)[4]. Já o segundo refere-se aos contratos de uso, que geralmente são onerosos e compartilhados com terceiros que não sejam vinculados com os próprios colaboradores internos ou fornecedores da empresa, sendo este protegido por contratos de *know-how*[5] ou transferência de tecnologia não patenteada.

Com o seguinte organograma (IFNMG, 2022, *on-line*) ilustra as três subdivisões:



Ocorre que a legislação brasileira faz menção ao segredo industrial ou comercial correlacionados ao crime de concorrência desleal, em seu artigo 195, inciso XI, enquanto a legislação internacional versa sobre o tema de modo menos restritivo, como é possível vislumbrar com o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionadas ao Comércio (Acordo de TRIPS). Desse modo, para a legislação brasileira apenas seria possível verificar violação ao segredo industrial ou comercial se fosse constatada a concorrência desleal entre o prejudicado e o violado. No caso em que não houver concorrência desleal, o Direito Penal quem irá figurar como protagonista, na forma dos artigos 153 e 325, do Código Penal Brasileiro (BARBOSA, 2010, p. 632-641).

Além da LPI versar que apenas haverá violação ao segredo industrial e comercial quando for constatada a concorrência desleal, não há estipulação quanto a intersecção com a proteção de dados, muito menos estabelece parâmetros para que ocorra a ponderação entre ambos os sistemas, entendendo que não foi do interesse

[4] “Acordo de não divulgação” (Tradução livre).
[5] “Saber-fazer” ou “conhecimento de normas, métodos e procedimentos em atividades profissionais” (Tradução livre).

do legislador adentrar em tais minúcias, revelando que a problemática deve ser analisada de forma casuística. Aliás, antes que possa ser alegado que a LPI é datada de 1996 visando indicar que se trata de uma lei já ultrapassada, o que não é realidade, destaca-se que poderia ter ocorrido uma alteração legislativa visando melhor especificação quanto à matéria.

5 SEGREDO COMERCIAL E INDUSTRIAL SOB À ÓTICA DA LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) garantiu também, de forma ampla, os direitos das empresas de proteger seus segredos comerciais e industriais. Segundo segundo Elisabeth Fekete (2003, p. 420), trata-se de:

> [...] um conhecimento atualizado na atividade empresarial, de caráter industrial ou comercial, de acesso restrito, provido de certa originalidade, lícito, transmissível, não protegido por patente, cuja reserva representa valor econômico para o seu possuidor, o qual exterioriza o seu interesse na preservação do sigilo através das providências razoáveis.

Motivo pelo a regulamentação e a fiscalização, visa evitar ataques aos titulares de dados pessoais, bem como viabiliza eventuais reparações quando verificado ilícitos à tutela da proteção de dados. Entretanto, não se deve banalizar os segredos de negócio das empresas, que constituiu forte proteção ao princípio livre mercado, um dos fundamentos do país (artigo 1º, inciso IV, Constituição da República Federativa do Brasil - CRFB).

A importância em analisar se as subordinações criadas pela LGPD ao atendimento de esclarecimentos aos titulares de dados pessoais surge a partir do momento em que a legislação supramencionada imprime maior importância ao segredo comercial e industrial do que ao princípio da não discriminação, uma vez que este último aparece apenas uma vez no texto[6], ao passo que o segredo industrial aparece 13 vezes no texto legislativo[7], indicando uma proteção exacerbada do legislador não à tutela da proteção de dados, mas sim às empresas e sociedade que utilizam-se de tecnologias do mundo contemporâneo.

Essa perspectiva impacta diretamente a vida de toda a sociedade brasileira, como é o caso do consumo de medicamentos e o tratamento discriminatório com dados coletados por empresas do ramo farmacêutico e repassados aos planos de saúde. Segundo o Conselho Nacional de Saúde (CNS), existem no Brasil cerca de uma

[6] O termo citado aparece apenas no artigo 6º, IX, da Lei Geral de Proteção de Dados Pessoais - LGPD.
[7] O termo citado aparece nos artigos 5º, VI; 9º, II; 10, §3º; 18, V; 19, II e §3º; 20, §§ 1º e 2º; 38, *caput*; 48, III; 55-J, II, X e §5º, todos da LGPD.

farmácia ou drogaria para cada 3.300 habitantes e o país está, neste momento, entre os dez que mais consomem medicamentos no mundo, segundo dados do Conselho Federal de Medicina (CFM, on-line).

Por esse motivo, o tratamento ilegal dos dados pessoais coletados referentes a quais medicamentos os consumidores – titulares dos dados pessoais sensíveis – estão adquirindo pode acabar por gerar contextos de discriminação, como a oferta de planos de saúde com valores elevados por aqueles pacientes que ingerem com frequência medicamentos para controle da pressão arterial, por exemplo. Em termos práticos, é muito comum que ocorra a discriminação sem que o consumidor tenha noção de quais fatores são os responsáveis, podendo causar violações à tutela do direito fundamental de proteção de dados.

O que se tem, dessa forma, é que enquanto a LGPD tem por objetivo devolver ao cidadão o poder de gestão de seus dados pessoais, conhecido internacionalmente como princípio da autodeterminação informativa[8], a legislação também não pretende inviabilizar a evolução tecnológica da sociedade, que contemporaneamente está baseada no tratamento de dados pessoais.

Se o cenário hipotético acima indicado fosse constatado em território nacional, o titular de dados pessoais poderia requerer à farmácia o direito à explicação, conforme dispõe o artigo 20, §§1º e 2º, da LGPD:

> [...]
>
> Artigo 20. O titular dos dados tem direito a solicitar a r**evisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses**, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Grifou-se).
>
> §1º. O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados

[8] Entende-se que o princípio da autodeterminação informativa como aquele que derivadoe do direito à privacidade, podendo também ser chamado de direito à privacidade informacional. Foi reconhecido em 1983, no julgamento histórico do Tribunal Constitucional Federal Alemão, no caso que julgou a Lei do Censo Alemão (*Volkszahlungsurteil*), reconhecendo o direito do cidadão de negar informações que fossem de caráter pessoal, podendo constituir uma faculdade o consentimento ou negativa na coleta, com o consequente armazenamento e compartilhamento de tais dados pessoais (RUARO, 2015, p. 41-60).

> para a decisão automatizada, **observados os segredos comercial e industrial**. (Grifou-se).
>
> §2º. Em caso de não oferecimento de informações de que trata o §1º deste artigo **baseado na observância de segredo comercial e industrial**, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (Grifou-se).
>
> [...]

Em suma, a legislação indica que, quando o tratamento de dados pessoais for realizado de forma puramente automatizada, o titular de dados pessoais terá o direito de requerer ao controlador[9] a revisão das decisões, enquanto este último tem o dever – e não a mera faculdade – de fornecer informações de modo claro e transparente, em consonância com os princípios da transparência e livre acesso, inferindo quais foram as razões ou os critérios que levaram a tais conclusões.

Portanto, o que se tem como direcionamento principal é a proteção da autonomia, da dignidade e dos direitos da personalidade daquele titular. Ocorre que, em razão do segredo comercial e industrial, pode não ocorrer o fornecimento das informações requeridas pelo titular, sendo facultado à Autoridade Nacional de Proteção de Dados (ANPD) realizar auditoria para constatação de violações aos direitos individuais e coletivos à proteção de dados pessoais, em razão do tratamento supostamente discriminatório realizado.

Afinal, somente a partir do conhecimento de como foi realizado o tratamento de seus dados será inferir que o titular passou a ter a verdadeira autonomia, traduzida no já elencado princípio da autodeterminação informativa, podendo se opor a qualquer tratamento que considere como discriminatório e cause ou possua potencial de causar prejuízos.

---

[9] Artigo 5º. Para os fins desta Lei, considera-se: [...] **VI - controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018).

6 *PRIVACY BY DESIGN*

Desde antes da entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, diversos outros países já possuíam experiências mais aprofundadas com a área, como é o caso de muitos da Europa, que desde a década de XX se preocupava com a proteção de dados de seus cidadãos, fato que se concretizou ao ano de 2016, com a *General Data Protection Regulation* (GDPR).

Além disso, um dos mais importantes estudos, que teve início no Canadá na década de 1990, refere-se a importância da proteção de dados, que seria responsável, no imaginário da época – e que se concretizou – pela disseminação em massa de informações e pela integração de pessoas ao redor do mundo. A Comissária de Privacidade de Dados e Informações de Ontário à época concluiu naquele estudo que a proteção da privacidade de dados no futuro não pode ser alcançada somente por intermédio do cumprimento de regulamentações, sendo necessário inovar, fazendo com que a privacidade seja incorporada como padrão de operação nas organizações (CAVOUKIAN, 1996, p. 26-31).

Essa ideia vai ao encontro do estudo aqui realizado. Ora, se a legislação de proteção de dados no Brasil impõe ao controlador a obrigação de fornecer, sempre que solicitadas, informações claras e precisas sobre os critérios e os procedimentos utilizados em uma decisão automatizada, o conceito *privacy by design* (*PbD)*, idealizado em 7 princípios, descreve uma metodologia que coloca a proteção da privacidade do usuário em primeiro plano, isto é, um sistema pensado para a garantia do direito fundamental à proteção de dados pessoais do titular desde a sua concepção - e não arranjado posteriormente, evitando assim inseguranças e riscos para ambas as partes.

Os objetivos do *PbD* podem ser alcançados seguindo os 7 princípios idealizados por Ann Cavoukian, quais sejam: (i) proativo e não reativo; (ii) privacidade como configuração padrão; (iii) privacidade incorporada ao design; (iv) funcionalidade completa de soma positiva; (v) segurança completa; (vi) visibilidade e transparência; e (vii) respeito pela privacidade e foco no usuário (CAVOUKIAN, 2011, *on-line*).

Essa abordagem objetiva garantir a proteção da privacidade dos usuários, tanto é que o método *PbD* é útil para se adequar ao artigo 46, §2º, da LGPD:

> [...]
> Artigo 46. 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.
>
> [...]
>
> **§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.** (Grifou-se).
>
> [...]

Quanto aos segredos comerciais e industriais, tal teoria está diretamente relacionada, sendo de suma importância que as organizações adotem medidas para proteger seus segredos comerciais, pois eles certamente representam uma vantagem competitiva frente ao mercado, com capacidade de gerar lucros para a empresa. Nesse contexto, a metodologia *(PbD)* e a LGPD são aliadas na proteção dos segredos comerciais, uma vez que a proteção adequada dos dados pessoais e a adoção de medidas para garantir a privacidade dos usuários minimizam o risco de exposição dos segredos comerciais e industriais das empresas.

Assim, a proteção de dados pessoais deve ser observada e garantida, desde o início, em total atendimento ao artigo 6º, da LGPD, ao indicar que é necessário explicar ao titular como o dado pessoal fornecido está sendo tratado, mas que há certa limitação na explicação, assim como quanto ao artigo 46, da LGPD, impondo a obrigação aos agentes de tratamento, que devem adotar medidas de segurança, técnicas e administrativas visando proteger os dados pessoais.

Do mesmo modo, caberá ao titular de dado pessoal identificar uma suposta violação ao direito fundamental de proteção de dados, seja por um suposto ato discriminatório por parte da empresa prestadora de serviço ou produto, o sistema idealizado sob o viés do *PbD* seria suficiente para fazer com que o titular compreendesse o motivo pelo qual, por exemplo, o crédito solicitado não foi aprovado em determinado banco ou instituição financeira. Caso, desde a concepção do sistema que analisa o crédito, na

hipótese elaborada, fosse pensado uma metodologia de explicação de quais dados são utilizados para o banco ou instituição financeira conceder crédito ou não, nenhum direito fundamental seria violado, na percepção de ambas as partes, evitando, inclusive, qualquer comprometimento ou violação de segredos comerciais e industriais utilizados pela empresa.

Esse cenário foi vivenciado no julgamento relacionado à Lei do Cadastro Positivo (Lei número 12.414/2011 - LCP), através do Recurso Especial ao Superior Tribunal de Justiça (STJ) número 1419697/ RS (STJ, 2014, *on-line*), e mesmo que anterior à promulgação da LGPD, o Ministro Paulo de Tarso Sanseverino pautou-se na proteção de dados, assim como nos princípios da não disciminação, livre acesso e transparência, temáticas amplamente difundidas junto à Corte, motivado especialmente por influências estrangeiras, como a *General Data Protection Regulation* (GDPR), na União Européia.

Trata-se, portanto, da decisão para classificação acerca da natureza jurídica do sistema de *credit score*[10] e a possibilidade de haver indenizações em caso de violações aos direitos do titular. O sistema é utilizado em larga escala por bancos e instituições financeiras para concessão ou não de crédito. Para chegar a pontuação dos consumidores, são utilizados alguns dados pessoais como o histórico de crédito e de dívidas (SERASA, 2021, *on-line*), idade, sexo, estado civil, profissão, renda, número de dependentes e endereço (SUPERIOR TRIBUNAL DE JUSTIÇA, 2014, p. 11).

O entendimento da corte foi de que não há qualquer violação ou ilícito na utilização do sistema de *credit score* e que sua aplicação constitui segredo comercial e industrial no que diz respeito à metodologia de cálculo de risco de crédito (brasil, 2014, p. 11-12), mas que isso não afasta o cumprimento de deveres anexos, como de informar ao titular dos dados pessoais como é realizado o tratamento. Inclusive, por haver benefícios coletivos, uma vez que a boa utilização de um sistema de *credit score* proporciona redução dos custos necessários à concessão de crédito ao mercado, havendo, portanto, menor repasse desses custos aos consumidores (PORTO. 2009,

[10] “Pontuação de crédito” (Tradução Livre)

p. 77-80), possibilitando um ecossistema consumerista mais favorecido (MONTEIRO, 2018, p. 09-10), houve a aprovação da Súmula 550, do STJ:

> Súmula 550, do STJ. A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, **dispensa o consentimento do consumidor**, que terá o direito de solicitar **esclarecimentos sobre as informações pessoais** valoradas e as fontes dos dados considerados no respectivo cálculo. (Grifou-se)

Posteriormente, com a promulgação da LGPD, uma das bases legais que autorizam o tratamento de dados pessoais é exatamente a proteção do crédito (artigo 7º, X).

Assim, pode-se afirmar que há limite para a explicação ao titular, que é exatamente a linha tênue entre a informação a ser fornecida constituir um segredo comercial e industrial ou não, que é o cerne da questão analisada neste estudo. Não havendo, portanto, pretexto para os agentes de tratamento de dados pessoais se esquivarem do cumprimento da LGPD, uma vez que não pode utilizar das ressalvas do ordenamento jurídico para se desobrigar de seu cumprimento, mesmo que a legislação de proteção de dados, de propriedade intelectual ou outra não tenha indicado quais dados e informações integram ou não o segredo comercial e industrial de uma empresa.

Em outra perspectiva à ideia de proteção dos segredos comerciais e industriais das empresas, é possível analisar o fenômeno do *open source*[11], isto é, *softwares* que possuem o seu código-fonte aberto e disponível para qualquer outro indivíduo, podendo, inclusive, ser modificado e redistribuído. Esse modelo de desenvolvimento é baseado na colaboração e compartilhamento de ideias entre a comunidade de desenvolvedores em uma variedade de campos, incluindo sistemas operacionais, aplicativos de celular e computador, construção de bancos de dados, entre outros. O *open source* é uma tendência desde a década de 1990 e surgiu como forma de questionamento quanto aos *softwares* que possuíam código-fonte mantido em sigilo pelas empresas (OPEN SOURCE INITIATIVE, 2018, *on-line*). Tal feito só foi possível pela criação da *internet* ou inicialmente a “rede de redes” (TEIXEIRA, 2012, p. 44), desenvolvida através do projeto ARPANET pelo Departamento de Defesa dos

[11] Código aberto (Tradução Livre).

Estados Unidos da América, em 1969 no Departamento de Defesa (MOZZILLA, 2022, *on-line*).

Foi assim que essa nova geração da internet, também conhecida como *web* colaborativa ou *web* 2.0 contribuiu, de forma disruptiva, para o desenvolvimento de interfaces de cooperação (TEIXEIRA, 2012, p. 51). O *software,* como indicado no capítulo 3 deste estudo, é protegido pelo direito autoral, assim como as obras literárias e audiovisuais, e não por propriedade industrial, mas não deixa de abarcar os segredos comerciais e industriais das empresas, podendo constituir seus anseios perante o mercado de consumo, motivo pelo qual, uma empresa que utiliza-se de tecnologia de código-aberto pode vir a possuir segredos comerciais e industriais sem qualquer impasse.

Como exemplo notório há o *Signal*, aplicativo de mensagens instantâneas criptografadas (SIGNAL, 2018, *on-line*) desenvolvido pela *Signal Foundation* através do *Signal Protocol* (SIGNAL, 2018, *on-line*), sendo o protocolo responsável pela criptografia de ponta a ponta nas mensagens e chamadas de voz no aplicativo. O *Signal* possui código aberto (GITHUB, 2023, *on-line*), garantindo acesso a todos os indivíduos. Certo é que o aplicativo se destaca por sua forte proteção de dados e privacidade aos usuários, uma vez que as mensagens nunca podem ser compartilhadas com terceiros, sendo visualizadas apenas pelo usuário e destinatário pretendido.

Outro exemplo pertinente é a rede Tor, desenvolvida pelo *Tor Project*. Trata-se de um navegador anônimo com diversas camadas de criptografia, garantindo o anonimato e segurança do usuário. Também utiliza-se da tecnologia da criptografia ponta a ponta, não sendo possível que as informações sejam interceptadas ou decodificadas por terceiros. Além disso é oferecido ao usuário, por exemplo, a ocultação do endereço IP (*Internet Protocol*)[12]. A navegação no Tor não é realizada na *Deep Web*[13], mas sim na *Surface Web*[14], com acesso a ferramentas cotidianas como *Google*, *Facebook*,

[12] O “endereço de IP” é um número que identifica o dispositivo conectado à rede de computadores.
[13] Internet profunda (Tradução Livre).
[14] Internet superficial (Tradução Livre).

lojas online, *Youtube* e diversos outros *websites* em que as pessoas geralmente utilizam sem maiores dificuldades.

Além disso, há o serviço de e-mail com criptografia nativa de ponta a ponta, *ProtonMail*[15], não permitindo a coleta de dados pessoais dos usuários, como endereço IP, motivo pelo qual não há anúncios direcionados aos seus clientes, tendo em vista que não existe o potencial de identificação. Por fim, o sistema de armazenamento em nuvem de código aberto, *NextCloud*[16], que também utiliza uma série de recursos para que o compartilhamento de arquivos ocorra de forma muito segura em comparação ao convencional, seja através da criptografia ponta a ponta, além da criptografia de chave privada, cujo acesso se dá apenas ao usuário que compartilhou e recebeu o arquivo.

Claro que todos os sistemas indicados acima possuem suas particularidades, mas convergem em dois pontos em comum, seja na popularidade por ser uma excelente opção aos que valorizam a privacidade e segurança de seus dados e informações, ou por possuírem código aberto. Inclusive, o *Signal Protocol* foi o responsável pela criptografia ponta a ponta utilizada atualmente pelo *WhatsApp*, aplicativo que possui esse nível de criptografia, mas que recolhe e utiliza diversos dados dos usuários, como dados da conta, de uso, registro, conexões, dispositivos, localização e *cookies*, assim como os contatos, as transações e pagamentos, especialmente para o compartilhamento entre do Grupo Meta (WHATSAPP, 2021, *on-line*).

Entretanto, não é porque o sistema é baseado no *open source* que devemos afastá-lo dessa análise, mas sim incorporá-los na sistemática da pesquisa aqui realizada. Inclusive, o *PbD* também pode ser constatado em sistemas que utilizam código fechado, como é o caso do serviço oferecido pela *Apple* para a ocultação de e-mail de seus usuários no cadastro e assinatura de serviços em outras plataformas.

A *Apple* é a empresa mais valiosa do mundo, com cerca de U$3 trilhões de dólares em valor de mercado (CNN BRASIL, 2022, *on-line*). Além de ser líder em

[15] Disponível em: https://proton.me/pt-br. Acesso em: 20 maio 2023.
[16] Disponível em: https://nextcloud.com/install/. Acesso em: 20 maio 2023.

investimentos em tecnologia e inovação (APPLE, 2018, *on-line*), se preocupando com a privacidade de seus usuários, como pode ser verificado com seu sistema de ocultação de e-mail, introduzido em 2019, possuindo o objetivo de aumentar a segurança e privacidade com um funcionamento simples, no qual o e-mail aleatório gerado é utilizado pelo usuário, mas vinculado ao e-mail real, onde receberá suas notificações e mensagens através de um *proxy* de e-mail[17].

O sistema da *Apple* é um exemplo de *PbD*, ou seja, incorporou a privacidade de seus usuários desde o início do processo de design, objetivando criar um serviço que ofereça segurança e privacidade, sem comprometer a funcionalidade ou sua usabilidade, atendendo a todos 7 princípios já indicados, evidenciando como a empresa está levando a privacidade de seus usuários a sério.

Dessa forma, ao aplicar o *PbD*, as empresas podem identificar de forma prévia os dados pessoais que serão coletados e tratados, estabelecendo assim qual será a base legal para o tratamento, bem como avaliar os riscos e definir eventuais medidas de segurança para protegê-los. Essas medidas incluem, mas não tão somente, aspectos técnicos e organizacionais, seja na criptografia ponta a ponta ou autenticação, seja na definição de políticas claras de privacidade e na capacitação dos colaboradores sobre as melhores práticas de proteção de dados.

Assim, através da adoção do *PbD* podem as empresas se anteciparem quanto às exigências da LGPD. Afinal, a competitividade do mercado pode ser alavancada pela proteção dos dados pessoais, constituindo um verdadeiro diferencial competitivo, pois demonstra o compromisso efetivo com a proteção da privacidade de seus usuários, evitando assim a apresentação de segredos industriais e comerciais que possam estar inseridos em sua operação à Autoridade Nacional de Proteção de Dados (ANPD), conforme preceitua o artigo 20, § 2º, da LGPD.

[17] O “proxy de e-mail” funciona como um intermediário entre o remetente e o destinatário. Quando o usuário envia um e-mail usando um proxy de e-mail, o e-mail primeiro é enviado para o servidor do proxy, que então encaminha o e-mail para o destinatário usando o endereço de e-mail aleatório, motivo pelo qual o destinatário não consegue visualizar o endereço de e-mail real do remetente.

Além do que já foi demonstrado sobre o *credit score*, o setor bancário tem se mostrado pioneiro nas práticas do *PbD*. O Banco Central do Brasil (BCB), por exemplo, através da recente implementação do *open banking*, está idealizado um sistema que permite o compartilhamento de dados dos clientes com outros bancos e instituições financeiras, de forma segura e controlada. A principal ideia é garantir a maior competitividade no setor bancário, proporcionando redução de custos para os consumidores, assim como a promoção de inovação ao setor.

Essa ferramenta possui estreita relação com o *PbD*, sendo de fundamental importância que os dados pessoais sejam compartilhados de modo seguro e que os titulares possuam plena ciência de como estão sendo tratados. Isso é efetivado, por exemplo, com a possibilidade de revogação, a qualquer tempo, do compartilhamento dos dados pessoais. Assim, estão interligados porque o compartilhamento de dados pessoais, com alto grau de discriminação, foi pensado para ocorrer do modo seguro, seja com autorizações e validações prévias junto ao BCB, além das criptografias, monitoramento constante das informações compartilhadas e outras medidas técnicas de segurança (BANCO CENTRAL DO BRASIL, 2021, *on-line*).

Nessa mesma linha, mas em outro setor, a empresa *Uber* tem se destacado no avanço e comprometimento com a proteção da privacidade dos seus usuários, utilizando-se do do *PbD* em seu processo de desenvolvimento e aperfeiçoamento de serviços fornecidos. Em primeiro lugar a *Uber* implementou o controle de privacidade pelos usuários, oferecendo uma central com controle completo sobre as informações pessoais, podendo optar por compartilhar ou não determinados dados pessoais com a Uber e empresas parceiras, assim como a possibilidade explorar os dados pessoais já fornecidos através de um resumo, qual a visão do motorista parceiro tem dos dados pessoais do usuário, a personalização de anúncios e a configuração de dados (UBER NEWSROOM, *on-line*).

Portanto, somente com a alteração de todo o ecossistema de proteção de dados que será possível responder de forma objetiva se os princípios do PbD estão sendo válidos e se respondem ao questionamento se tudo está realmente funcionando conforme anunciado pelas *Big Techs* e não apenas servindo como letra fria para fazer cumprir

de forma hipotética os requisitos legais e regulatórios para, porventura, esquivar-se da aplicação legal.

7 CONSIDERAÇÕES FINAIS

Existe, no sistema jurídico brasileiro contemporâneo, contradição entre a conduta de revelação, como forma de garantia de um direito ao titular dos dados pessoais e o risco de tornar certas informações de conhecimento público, mas que eram consideradas como segredo comercial e industrial. Dessa forma, este estudo buscou responder a seguinte questão-problema: há pretexto por parte dos agentes de tratamento de dados pessoais para o descumprimento da Lei Geral de Proteção de Dados (LGPD), quanto ao atendimento às solicitações de titulares em razão do conflito à proteção do segredo comercial e industrial?

Como pôde ser constatado, não há nenhuma metodologia salvadora, própria ou certa para resolver essa problemática, motivo pelo qual os conflitos devem ser observados e compreendidos caso a caso, atentando-se às legislações específicas. A técnica apontada neste trabalho e que se mostrou exitosa nos diversos exemploscolecionados é a utilização pelas empresas do *Privacy by Design (PbD)*. Uma estrutura que tem por objetivo a incorporação da privacidade e da proteção de dados pessoais em todos os projetos e programas corporativos desde o início e quando não for possível, tentem adotar ao máximo a metodologia em suas operações que já estão em andamento. Assim, a privacidade vai estar incorporada no desenvolvimento de produtos, serviços, processos, práticas, tecnologias, infraestruturas, entre outros.

Por mais que subsista qualquer conflito entre os institutos aqui indicados, visa-se ser possível a convivência pacífica entre os direitos fundamentais à proteção de dados e aos segredos comerciais e industriais, não sendo necessário tratar o princípio da transparência com antagonismo ao desenvolvimento econômico e ao livre mercado.

Os exemplos serviram, um a um, para evidenciar como a utilização do *PbD* pode evitar que empresas tentem se esquivar da aplicação da Lei Geral de Proteção de Dados, sob a justificativa de que a revelação de “informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada” (BRASIL, 2018) poderia violar segredos industriais e comerciais.

Portanto, ao adotar uma abordagem de proteção de dados desde a concepção, as empresas podem garantir a proteção da privacidade aos titulares, assim como aos seus segredos industriais e comerciais. As implementações de medidas de segurança apropriadas podem assegurar que as informações confidenciais sejam acessíveis e protegidas apenas àquelas pessoas autorizadas, sem prejudicar a operação, garantindo a transparência e responsabilidade no tratamento de dados pessoais, gerando maior credibilidade frente aos consumidores e ao mercado, com benefícios econômicos a longo prazo (LISBOA, 2021, *on-line*).

Assim, todas essas abordagens estão interligadas e devem ser consideradas conjuntamente pelas empresas que buscam a adequação à legislação de proteção de dados e a garantia de seus segredos comerciais e industriais.

BIBLIOGRAFIA

ASIMOV, Isaac. **Pedra no céu:** qualquer planeta é a Terra para aqueles que nele vivem. Editora Aleph: São Paulo, 2016.

APPLE. Apple acelera os investimentos e a geração de empregos nos EUA. Disponível em: https://www.apple.com/br/newsroom/2018/01/apple-accelerates-us-investment-and-job-creation/. Acesso em: 17 mar. 2023.

BANCO CENTRAL DO BRASIL. **Open Banking**. Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/OD_live_Open%20Banking_13.7.pdf. Acesso em: 27 mar. 2023.

BARBOSA, Denis Borges. **Uma Introdução à Propriedade Intelectual**. Rio de Janeiro: Lumens Juris. 2010, p. 636 - 641.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020, p. 28)

BRASIL. **Lei número 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 mar. 2023.

CAVOUKIAN, Ann Cavoukian. Information and Privacy Commissioner of Ontario. **Privacy by Design:** The 7 Foundational Principles. Canadá: 2011. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 16 fev. 2023.

CORAZZA, T. A. M.; ÁVILA, G. N. DE. A proteção de dados do banco de perfil genético criminal: privacidade e liberdade versus segurança pública. **Revista de Direitos e Garantias Fundamentais**, v. 23, n. 2, p. 243-282, 9 dez. 2022.

CONSELHO NACIONAL DE SAÚDE. **Consumo de Medicamentos: um autocuidado perigoso.** Disponível em: http://www.conselho.saude.gov.br/ultimas_noticias/2005/medicamentos.htm. Acesso em: 20 mar. 2023.

CAVOUKIAN. Ann. **Who Knows:** Safeguarding Your Privacy in a Networked World. Nova York: McGraw Hill, 1996, p. 26-31.

CNN BRASIL. **Apple acaba de se tornar a primeira empresa de U$3 trilhões do mundo**. Disponível em: https://www.cnnbrasil.com.br/economia/apple-acaba-de-se-tornar-a-primeira-empresa-de-us-3-trilhoes-do-mundo/. Acesso em: 16 mar. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 7.

MOZILLA. **Mozilla**. Disponível em: https://developer.mozilla.org/pt-BR/docs/Glossary/Arpanet. Acesso em: 19 mar. 2023.

FEKETE, Elisabeth Kasznar. **O regime jurídico do segredo de indústria e comércio no direito brasileiro**, 2003, p. 420.

FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 47.

GITHUB. **Github**. Disponível em: https://github.com/signalapp/Signal-iOS. Acesso em: 15 mar. 2023.

INSTITUTO FEDERAL DO NORTE DE MINAS GERAIS. **Pesquisa em Propriedade Intelectual**. Disponível em: https://www.ifnmg.edu.br/pesquisa/27-portal/pesquisa/1273-propriedade-intelectual-texto. Acesso em: 27 mar. 2023.

LOCKE, John. **Dois tratados sobre o governo**. São Paulo: Edições 70, 2006.

MENDES. Laura Schertel. **Decisão histórica do STF reconhece o direito fundamental à proteção de dados pessoais**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 09 mar. 2022.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?**. Instituto Igarapé, nº 39, 2018, p. 09-10. Rio de Janeiro. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 28 mar. 2023.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, *[S. l.]*, v. 19, n. 3, p. 159–180, 2018. DOI: 10.18759/rdgf.v19i3.1603. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 30 abr. 2023.

OPEN SOURCE INITIATIVE. **History of the OSI**. Disponível em: https://opensource.org/history/. Acesso em 15 mar. 2023.

PALHARES, F. PRADO; L. VIDIGAL, P. **Compliance Digital e LGPD (Coleção Compliance)**. São Paulo: Thomson Reuters Brasil, 2021, p. 136.

POPPER, Karl. **A lógica da pesquisa científica**. São Paulo, Cultrix, 2013.

PORTO, Antonio José Maristrello. **O Direito e a economia do cadastro positivo**. Conjuntura Jurídica, nº 77, 2009, p. 77-80. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rce/article/viewFile/24693/23466. Acesso em: 28 mar. 2023.

RODRIGUEZ. Daniel Piñeiro. **O direito fundamental à proteção de dados: vigilância, privacidade e regulação**. Rio de Janeiro: Editora Lumen Juris, 2021, p. 37, APUD MILLER, Arthur R. **The assault in privacy: computers, data banks and dossiers**. Michigan: The University of Michigan Press, 1971, p. 169.

RUARO, Regina Linden. Privacidade e Autodeterminação Informativa Obstáculos ao Estado de Vigilância?. **Arquivo Jurídico**. Teresina/PI. 2015. v. 2, n. 1, pg. 41-60

Rafael Lisboa. Exame. 2021. **Conformidade de empresas com LGPD é cobrada pelo mercado e vira valor competitivo** Disponível em: https://exame.com/bussola/conformidade-de-empresas-com-lgpd-e-cobrada-pelo-mercado-e-vira-valor-competitivo/. Acesso em: 09 mar. 2023.

SERASA. **Serasa passa a permitir que dados de pagamento, transferência, débito e crédito sejam considerados na análise do Serasa Score**. Disponível em: https://www.serasa.com.br/imprensa/serasa-passa-permitir-dados-de-pagamento-na-analise-de-score. Acesso em: 08 mar. 2023.

SIGNAL. **Signal**. Disponível em: https://signal.org/legal/. Acesso em: 15 mar. 2023.
_____. **Signal's Blog**. Disponível em: https://signal.org/blog/signal-foundation/. Acesso em: 15 mar. 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Resp nº 1419697/RS**. Relator Ministro Paulo de Tarso Sanseverino, 2ª Seção, 3ª Turma, DJe 17/11/2014, pg. 11.

TEIXEIRA, Bruno Costa. **Cidadania em rede:** a inteligência coletiva enquanto potência recriadora da democracia participativa. Dissertação (Mestrado em Direitos e Garantias Fundamentais) - Programa de Pós-Graduação em Direitos e Garantias Fundamentais, Faculdade de Direito de Vitória, Vitória, 2012.

UBER. **Uber newsroom**. 2022. Disponível em: https://www.uber.com/pt-BR/newsroom/uber-lanca-sua-nova-central-de-privacidade/. Acesso em: 11 abr. 2023.

VALENTE, Jonas. **Quase metade do planeta ainda não tem acesso à internet, aponta estudo**. Agência Brasil Economia, Brasília, 28 set. 2019. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2019-09/quase-metade-do-planeta-ainda-nao-tem-acesso-internet-aponta-estudo. Acesso em: 02 mar. 2023.

WHATSAPP. **Política de Privacidade do WhatsApp**. Disponível em: https://www.whatsapp.com/legal/privacy-policy/?locale=pt_BR. Acesso em: 15 mar. 2023.

APÊNDICE A - Termo de Autorização para depósito e disponibilização da produção científica no Repositório Institucional da Faculdade de Direito de Vitória - FDV

Na qualidade de titular de direitos de autor da presente publicação, autorizo a Faculdade de Direito de Vitória (FDV), a publicar em ambiente digital institucional, sem ressarcimento de direitos autorais, conforme previsto na Lei 9.610/98 e em outras legislações que regulam ou vierem a regular a matéria, o texto integral do material abaixo citado, conforme permissões assinaladas, para fins de leitura e/ou impressão, a título de divulgação da produção científica brasileira

Tipo de Documento: Trabalho de Conclusão de Curso

Nome do Autor: Matheus Corona Patricio

E-mail: matheuscoronapatricio@gmail.com | matheus.corona@fdv.digital

Telefone para contato: (27) 99739-1785

Título do Trabalho: PROTEÇÃO DO SEGREDO COMERCIAL E INDUSTRIAL À LUZ DA TUTELA DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Nome do Orientador: Bruno Costa Teixeira

Membro da Banca (1): _____

Membro da Banca (2): _____

Data de Defesa: ___ / 06 / 2023