UNIVERSIDADE PRESBITERIANA MACKENZIE

GUILHERME DE CARVALHO BELOTO

Aplicação do legítimo interesse como forma de legitimar o tratamento de dados pessoais

São Paulo

2020

GUILHERME DE CARVALHO BELOTO

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

ORIENTADOR: Prof. Ms. Marcelo Romão Marineli, Professor da Faculdade de Direito da Universidade Presbiteriana Mackenzie (Mestre em Direito Civil pela PUC/SP)

São Paulo

2020

GUILHERME DE CARVALHO BELOTO

Aplicação do legítimo interesse como forma de legitimar o tratamento de dados pessoais

Trabalho de Graduação Interdisciplinar apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Aprovado em:

BANCA EXAMINADORA

_____

Examinador(a): Prof. Dr. Diogo Leonardo Machado de Melo, Professor da Faculdade de Direito da Universidade Presbiteriana Mackenzie (Mestre e Doutor em Direito Civil pela PUC/SP)

_____

Examinador(a): Prof. Ms. Fabricio Favero, Professor de Direito do INSPER (Mestre em Direito pela PUC/SP)

Aos meus pais.

(in memoriam)

AGRADECIMENTOS

Gostaria de agradecer em primeiro lugar ao Professor Marineli, que aceitou o desafio e mesmo à distância confiou no meu trabalho de pesquisa. A sua dedicação ao conhecimento e aos seus alunos me levou a ir além em cada página deste trabalho. A todos os demais professores do Mackenzie, que juntos formaram a base do meu conhecimento jurídico-acadêmico. Ao Professor Renato Leite Monteiro, que em seu curso de Direito Digital me mostrou que esta área existe e é pulsante no Brasil.

Agradecimentos também à Patricia Peck e Marcelo Crespo, com os quais tenho a honra de realizar o meu estágio e com os quais aprendo diariamente, não apenas sobre direito, mas também sobre o trato com o cliente, a importância de sempre buscarmos conhecimento e escrever sempre: *verba volant, scripta manent*. Ambos, e Marina Gaspar, foram essenciais para o meu entendimento sobre a proteção de dados pessoais e, assim, para o resultado deste trabalho.

Agradecimentos especiais aos meus pais, que desde minha adolescência sabiam que um dia eu estudaria Direito. E ao meu irmão, sem o qual eu não conseguiria terminar o curso com a tranquilidade necessária. Um amor sem fim a toda a minha família.

Special thanks to Sigrid Heirbrant. You don't need to proofread my work in Portuguese to support me, and you do it every single day. You are my drive and your insights are priceless. Thank you for sharing your life in such a special way. Ik hou van u.

Human nature is not a machine to be built after a model, and set to do exactly the work prescribed for it, but a tree, which requires to grow and develop itself on all sides, according to the tendency of the inward forces which make it a living thing.

John Stuart Mill, On Liberty (1859)

Aplicação do legítimo interesse como forma de legitimar o tratamento de dados pessoais

Guilherme de Carvalho Beloto

Resumo: Este trabalho busca realizar uma análise profunda sobre o legítimo interesse como base legal independente para tratamento de dados pessoais, sob a égide das legislações de proteção de dados pessoais brasileira (LGPD) e europeia (GDPR). São tratadas as origens desta base legal e o seu desenvolvimento legislativo, os requisitos mínimos e as recomendações de acordo com as melhores práticas utilizadas atualmente, bem como as ferramentas que podem ser utilizadas para garantir a correta aplicação desta hipótese de tratamento. Ao final do trabalho, será possível realizar um análise adequada sobre o fluxo de dados pessoais mapeado, identificando-se a partir da finalidade e do caso concreto se o legítimo interesse é uma opção de utilização, ou se os controladores precisarão utilizar outras hipóteses legais do artigo 7º (ou artigo 11, quando envolver o tratamento de dados pessoais sensíveis).

Palavras chave: legítimo interesse; proteção de dados; LGPD; GDPR

Abstract: This paper sought to analyse the legitimate interest as an independent legal basis for the processing of personal data, under the aegis of the Brazilian (LGPD) and European (GDPR) personal data protection legislations. The origins of this legal basis and its legislative development are discussed, along with the minimum requirements and recommendations according to the best practices and guidelines currently in place. We discuss the tools that can be used to guarantee the lawful processing under this hypothesis. At the end of the work, it will be possible to carry out an adequate analysis of the processing activities, identifying a clear purpose and whether the legitimate interest is a viable option, or if another legal possibility should be used.

Keywords: legitimate interest; data protection; LGPD; GDPR

Sumário

1. Introdução

Não é difícil perceber que a sociedade que vivemos vem passando por grandes transformações. Do seu início agrícola à sociedade informacional, marca característica dos nossos tempos, muita coisa mudou, não apenas nos aspectos externos mais visíveis, como moda, cultura, arte. A estrutura de trabalho, produção de conhecimento e riqueza foram seguidamente modificadas. Segundo Castells (2011), quando aborda sobre essas modificações estruturais da sociedade humana, identifica que "cada modo de desenvolvimento é definido pelo elemento fundamental à promoção da produtividade no processo produtivo." Neste sentido, a sociedade informacional tem como força motriz de produtividade a "tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos.", e é justamente a análise realizada massivamente (big data) sobre esse conhecimento que marca a sociedade em que vivemos.

Por conta disso, as antigas fronteiras (físicas e psicológicas) se tornam mais permeáveis, e vive no século XXI uma explosão sem limites. A informação é o elemento base para a convivência e o desenvolvimento social e econômico (BIONI, 2019).

O capitalismo informacional, conforme descrito pelo professor Manuel Castells, precisa de elevada capacidade tecnológica para processar informação, gerando e conhecimento e produzindo riqueza. (CASTELLS, 1999).

Privacidade e proteção de dados pessoais se tornam conceitos que, com o decorrer dessas seguidas evoluções, passaram a ser contemplados pela análise do Direito e, assim, se tornaram bem jurídicos a serem por ele tutelados. Como exposto em um dos textos seminais sobre o direito à privacidade (WARREN & BRANDEIS, 1890), o direito à propriedade e à vida já estavam consolidados há muito tempo, mas de tempos em tempos surgem novos situações e contextos fáticos que exigem do Direito olhar para si e compreender essas mudanças, adaptando-se – ainda que de forma lenta – às demandas da sociedade em constante mutação. Naquele tempo, os autores traziam questões como a privacidade das pessoas em relação a

fotografias publicadas em jornais. Atualmente, as fotografias publicadas podem ser imediatamente analisadas por sistemas de informática complexos e que, para além de identificar uma pessoa em meio a tantas outras, ainda que no fundo da imagem, fazem correlações com outras bases de dados e podem, ao final da análise, elaborar um relatório de perfil sobre aquele indivíduo.

Diante desse cenário, não apenas a Constituição Federal trouxe a intimidade como direito fundamental, em seu artigo 5º, X[1], mas diversas leis foram sendo criadas para proteger os direitos dos indivíduos sobre um uso indiscriminado dos seus dados pessoais. Conforme explicado por Stalla-Bourdillon, Phillips e Ryan (2014), há na Europa atualmente uma dicotomia fundamental, explicitada na distinção de dois direitos humanos fundamentais, quais sejam, o direito à vida privada (artigo 7º) e o direito à proteção de dados (artigo 8º), ambos presentes na Carta dos Direitos Fundamentais da União Europeia (UNIÃO EUROPEIA, 2012)[2]. Os autores defendem que a separação é negativa no sentido de que as leis de proteção de dados não permitirem um exame detalhado das medidas de vigilância adotadas, para determinar a proporcionalidade dos meios adotados (p. 37-38).

De toda forma, cabe avaliar que inicialmente as legislações sobre o tema eram esparsas e davam conta apenas de tutelar os dados pessoais das pessoas em contextos específicos, setoriais, mas com o contínuo desenvolvimento do tema cresceu a pressão por uma legislação que pudesse congregar as diversas áreas em que dados pessoais são tratados, visto que a prática do mercado não é segregada em setores delimitados, mas abrangem todas as esferas da vida dos indivíduos, seja digital ou analogicamente. É nesse contexto que a frase "dados pessoais são o novo petróleo da Internet e a nova moeda do mundo digital"[3], proferida por Kuneva (2009) e que seria repetida tantas vezes, ganha especial significado.

Uma das mais contundentes respostas legislativas a esse tema nos anos recentes foi a publicação do *General Data Protection Regulation* (GDPR)[4] na União Europeia. O Regulamento (EU) 2016/679 atualizou a Diretiva 95/46/CE que estava em vigor desde 1995,

---

[1] 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;

[2] Essa separação não é observada no texto da Convenção Europeia dos Direitos do Homem, de 1950.

[3] No original em inglês: "Personal data is the new oil of the internet and the new currency of the digital world".

[4] Regulamento Geral sobre a Proteção de Dados, em português. Utilizaremos a nomenclatura em inglês ao longo deste trabalho.

tornando a União Europeia a jurisdição mais avançada em termos de proteção de dados pessoais do mundo. Mais do que isso, o GDPR trabalha com uma forma de aplicabilidade que transcende as barreiras físicas da União, com definição de escopo territorial que a faz incidir sobre empresas estabelecidas em outros países, incluindo o Brasil. Por sua vez, o Brasil publicou, dois anos após o GDPR, a Lei Geral de Proteção de Dados (LGPD) – Lei Federal nº 13.709/2018, inspirada no regulamento europeu e que busca enfrentar os desafios da *data-driven economy* (MARINELI, 2019).

As legislações de proteção de dados pessoais, como regra, trazem as disposições relativas à legalidade do tratamento de dados pessoais, com as chamadas "bases legais". Algumas dessas permissões legais ficaram bastante conhecidas, como o consentimento, e alguns autores a alçaram a "pedra angular" da LGPD (SOARES, 2019). Este trabalho buscará, no entanto, tratar de uma outra base legal disposta na legislação, qual seja, o legítimo interesse.

O legítimo interesse pode ser considerada uma das bases legais mais flexíveis para tratamento de dados pessoais. Isso, no entanto, não significa que as empresas possam utilizar esta opção como salvo conduto, na ausência de outras bases legais para o tratamento dos dados pessoais em determinado fluxo. A leitura apenas da parte inicial do inciso esconde a complexidade inerente a esta base legal.

Trataremos dos requisitos para utilização desta base legal, bem como as formas de mitigar os riscos a ela inerente. Ao fim do trabalho, espera-se ter definido com clareza os momentos em que o operador de direito, e o DPO[5], figura chave para as empresas em busca de adequação à LGPD, poderá e deverá utilizar o legítimo interesse para proteger os interesses de empresas e indivíduos.

2. Lei Geral de Proteção de Dados - LGPD

Leis de proteção de dados pessoais, de maneira geral, correm um grave risco, qual seja, o de se tornarem defasadas rapidamente. Isto porque tratam de assuntos que envolvem, em alguns casos, avanços tecnológicos que colocam em xeque os parâmetros determinados no momento da sanção. O processo legislativo possui um tempo próprio, guiado pelas forças políticas presentes no Congresso Nacional e de uma conjuntura que pode estar em descompasso com a velocidade da sociedade civil e do mercado. Nesse sentido, salutar a utilização de

[5] DPO é a sigla para Data Protection Officer, ou Encarregado na legislação nacional, é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), de acordo com o art. 5º, VIII da LGPD.

princípios que possam ser utilizados para dar sobrevida à legislação, acompanhando a evolução de ferramentas e tecnologias (CRESPO; GASPAR; BELOTO, 2020).

> "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas 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 difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

A lista principiológica do artigo 6º incorpora muito dos princípios estipulados pela legislação de proteção de dados pessoais europeia (GDPR), conforme se observa a seguir:

LGPD	**GDPR**
Finalidade (art. 6º, I)	Licitude, lealdade e transparência (art. 5º, I, "a") e Limitação das finalidades (art. 5º, I, "b")
Adequação (art. 6º, II)	Limitação das finalidades (art. 5º, I, "b")
Necessidade (art. 6º, III)	Minimização dos dados (art. 5º, I, "c")
Livre acesso (art. 6º, IV)	Sem correlação no art. 5º; proximidade com art. 13
Qualidade dos dados (art. 6º, V)	Exatidão (art. 5º, I, "d")
Transparência (art. 6º, VI)	Licitude, lealdade e transparência (art. 5º, I, "a")
Segurança (art. 6º, VII)	Integridade e confidencialidade (art. 5º, I, "f")
Prevenção (art. 6º, VIII)	Integridade e confidencialidade (art. 5º, I, "f")
Não discriminação (art. 6º, IX)	Licitude, lealdade e transparência (art. 5º, I, "a")
Responsabilização e prestação de contas (art. 6º, X)	Responsabilidade (art. 5º, 2)
Sem correlação no art. 6º; proximidade com art. 15 e 16	Limitação da conservação (art. 5º, I, "e")

Sem entrarmos no detalhe de cada princípio, bastará para a nossa análise sobre o legítimo interesse entender que os princípios da LGPD "são complementares entre si e dificilmente serão aplicados isoladamente" (BEPPU; PAIVA, 2019), devendo ser por óbvio compreendidos dentro de um sistema de proteção de dados pessoais amplo e que agrega os direitos fundamentais da privacidade, para orientar todas as atividades de tratamento de dados pessoais, e preencher as lacunas que possam advir da aplicação da legislação.

2.1. Bases Legais

A LGPD se dispõe a regular o tratamento de dados pessoais, para que ele seja feito de acordo com a legislação nacional e em níveis adequados internacionalmente, incluindo o compartilhamento com agentes de países terceiros (transferência internacional).

Para legitimar o tratamento, é necessário que ele se encaixe em uma das bases legais, ou seja, as hipóteses legais de tratamento. A legislação prevê 10 bases legais para tratamento de dados pessoais e 8 bases legais para tratamento de dados pessoais sensíveis. O tratamento, que se inicia na coleta do dado pessoal, só pode ser realizado se o controlador tiver determinado a base legal que apoiará esse processo, visto que a legislação determina, em seu artigo 7º *caput* que "O tratamento de dados pessoais **somente poderá ser realizado** nas seguintes hipóteses" e, para os dados pessoais sensíveis, o artigo 11 *caput* traz que "O tratamento de dados pessoais sensíveis **somente poderá ocorrer** nas seguintes hipóteses". Do texto legal decorre também que o rol é taxativo.

Analisemos o artigo 7º, que contém em seu inciso IX a possibilidade de tratamento de dados pessoais sob o legítimo interesse:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

> **IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou**
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
> § 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
> § 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
> § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
> § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019)

No entanto, apesar de vermos que a legislação permite o tratamento de dados pessoais sob dez hipóteses, é debate recorrente nos meios jurídicos, e fora dele, que a LGPD obriga os controladores a obterem o consentimento do titular. *Prima fascie*, o *caput* do artigo não faz distinção ou priorização entre o consentimento e as demais 9 bases legais, com o texto "O tratamento de dados pessoais somente poderá ser realizado **nas seguintes hipóteses**:" seguido de uma lista de incisos, cada um com uma base legal.

Da mesma forma, a escolha pela conjunção alternativa "ou", ao invés da conjunção "e", indica que apenas uma base legal deve ser utilizada por finalidade de tratamento, e percebe-se que a escolha em determinar quantas ou quais opções podem ser escolhidas pelos operadores do Direito foi utilizada proficuamente pelo legislador ao longo da LGPD[6]. Semelhante opção foi feita pelo legislador europeu, no GDPR, opinião corroborada pela autoridade nacional belga (GBA, 2020, p. 44-45).

Por outro lado, se poderia argumentar que, na medida em que o legislador posteriormente utiliza o texto "ressalvadas as **hipóteses de dispensa do consentimento previstas** nesta Lei" e "A **eventual dispensa da exigência do consentimento** não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da

[6] A conjunção "e" foi escolhida pelo legislador para marcar os artigos 2º, 5º, 9º, 10, 23, 34, 41, 48, 48 §2º, 50 §2º, 52 §1º e §6º, 55-C, 55-J, 58-A, 58-B e 65, enquanto a conjunção alternativa "ou" foi utilizada nos artigos 3º, 4º, 7º, 11, incisos e §4º, 15, 16, 18 §4º, 19 incisos e §2º, 26 §1º, 27, 33 e 43.

observância dos princípios gerais e da garantia dos direitos do titular"[7], estaria dada a existência da chave consentimento-dispensa de consentimento. Nesta linha de argumentação, os incisos II à X do artigo 7º seriam complementares ao fornecimento do consentimento do titular, ou em outras palavras, hipóteses de dispensa do inciso I.

No entanto, quando se realiza uma leitura global da Lei e, especialmente, a análise das diferenças entre as diferentes versões do texto, desde o anteprojeto até a promulgação da Lei 13.709/2018 e suas alterações posteriores[8], percebe-se que a formulação do §5º é remanescente de entendimento anterior e que não foi adequado durante o processo legislativo. Não haveria, portanto, qualquer indicação na LGPD que permitisse hierarquizar as bases legais, ou aplicação excepcional quando da não "obtenção do prévio consentimento dos titulares" (BEPPU; PAIVA, 2019).

Nesse sentido, BIONI relembra que nas duas primeiras consultas públicas a respeito do anteprojeto de lei (em 2010 e em 2015), o consentimento era a única base legal para o tratamento de dados pessoais, sendo as demais bases legais consideradas hipóteses de dispensa de consentimento. O projeto Pensando o Direito, do Ministério da Justiça, traz explicação semelhante, indicando a necessidade de consentimento do titular para o tratamento legal:

> "**A proposta traz a necessidade de consentimento do titular para o tratamento de seus dados pessoais como a regra geral a legitimar o tratamento de dados pessoais**. Aqui, debateremos o papel do consentimento na proteção dos dados pessoais enquanto ferramenta de efetivo controle do cidadão sobre suas próprias informações. **Assim, o tratamento dependeria do consentimento do titular, salvo em alguns casos excepcionados**. Algumas exceções conhecidas são: dados que já são de acesso público ou casos em que alguma lei específica dispense o consentimento. Por outro lado, há, ainda, casos específicos em que o consentimento poderia ser ainda mais relevante, como no caso dos dados sensíveis – veja os artigos específicos sobre isso e entenda a importância da sua proteção!"[9]

Esse entendimento, no entanto, foi superado após a segunda consulta pública, em 2015, quando o texto foi finalmente enviado ao Congresso Nacional, transformando-se no PL 5.276/2016 (que tramitou apensado ao PL 4.060/2012). A partir daquele momento, o texto passou a trazer as hipóteses de tratamento de dados pessoais já na posição do artigo 7º como promulgado pela Lei 13.709/2018, e o consentimento tornou-se apenas um dentre os demais incisos de hipóteses de tratamento de dados pessoais. A inclusão da conjunção alternativa "ou" entre a penúltima e a última hipótese de tratamento de dados pessoais se deu durante o processo

[7] Conforme § 5º e 6º do art. 7º da LGPD.
[8] A LGPD, promulgada originalmente em 14/08/2018, foi alterada pelas Leis 13.853/2019 e 14.020/2020 ainda dentro da sua *vacatio legis*.
[9] Conforme http://pensando.mj.gov.br/dadospessoais/eixo-de-debate/tratamento-de-dados-pessoais/. Acessado em 28/09/2020.

legislativo e ajudou a esclarecer a questão. Desta forma, entendemos que menções à dispensa de consentimento se baseiam numa concepção anterior da legislação e que devem ser compreendidas à luz do atual texto da LGPD.

Por fim, vale ressaltar que o consentimento, dentre todas as bases legais, é a mais arriscada do ponto de vista operacional ao controlador, posto que pode ser revogado pelo titular a qualquer momento e por procedimento gratuito e facilitado, acarretando a obrigação de cessar o tratamento, conforme já explicamos em publicação anterior (CRESPO; BELOTO, 2020).

Superada a questão do consentimento como principal base legal de tratamento de dados legais no atual momento da LGPD, iremos nos focar no legítimo interesse como hipótese de superação do debate.

3. O Legítimo Interesse

3.1. Surgimento

O Legítimo Interesse (do controlador ou de terceiros) como base legal independente para tratamento de dados pessoais não existia no início das discussões de uma lei geral de proteção de dados pessoais brasileira. De acordo com o texto original do Projeto de Lei 4.060/2012 existia, no entanto, a necessidade de que o tratamento fosse realizado para atender aos legítimos interesses dos seus titulares: "Os dados pessoais serão tratados com lealdade e boa-fé, de modo a atender aos legítimos interesses dos seus titulares", enquanto para os dados pessoais sensíveis, o mesmo Projeto de Lei previa que, quando não solicitado pelo titular, "somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal." Havia, naquele momento, uma sutil diferença quando comparamos com o texto atual da lei. Em 2012, os dados pessoais poderiam ser tratados caso fossem feitos com lealdade e boa-fé, e atendendo os legítimos interesses **dos seus titulares**. Assim, bastava que o controlador atendesse esses requisitos para iniciar o tratamento. A boa-fé, prevista nos artigos 113 e 422 do Código Civil, "é premissa para interpretar os negócios jurídicos, bem como orientação desde a formação até a execução contratual" (CRESPO; GASPAR; BELOTO, 2020). No caso de dados pessoais sensíveis, havia a necessidade de se buscar a autorização (consentimento na terminologia posteriormente adotada) ou que o tratamento se iniciasse a pedido do titular. Em ambos os casos, havia a possibilidade do titular requerer a interrupção do tratamento, excetuado se necessário para cumprimento de obrigação legal ou contratual, de acordo com a parte final do artigo 13:

"devendo ser garantido sempre o direito ao bloqueio do registro, salvo se necessário para cumprimento de obrigação legal ou contratual"[10].

A inclusão da hipótese de tratamento de dados pessoais quando necessário para atender os interesses legítimos **do controlador ou de terceiro** se dará apenas no Projeto de Lei 5.276/2016, seis anos após os primeiros debates e consultas públicas de anteprojetos que efetivamente viriam a se tornar a LGPD.

Segundo o relatório apresentado pelo Deputado Orlando Silva (PCdoB), sob a rubrica " Parecer do Relator n. 1 PL406012"[11], a *raison d'être* do legítimo interesse serviria para:

> "[...]não onerar demasiadamente o titular dos dados com a necessidade de manifestação de consentimento a todo instante, seja porque em diversas situações concretas o tratamento de dados, mesmo sem consentimento, é importante para atender a uma finalidade pública ou a uma finalidade privada legítima, tal como a prevenção a fraudes bancárias ou a garantia de segurança das redes" (2016, p. 32 e 33).

Assim, a utilização da hipótese do legítimo interesse serviria para também trazer benefícios aos titulares, evitando a onerosidade de manifestação do consentimento a todo instante.

A "legítima expectativa do titular", base para o tratamento de dados pessoais conforme artigo 9º do Projeto de Lei 4.060/2012 estava presente como argumento no texto do Parecer aprovado ao Projeto de Lei, elaborado Relator Orlando Silva (PCdoB):

> "O legítimo interesse, contudo, não deve ser lido como um cheque em branco. Em outras palavras, não pode ser utilizado como um subterfúgio para que todo e qualquer tratamento de dados pessoais seja autorizado. Esta a razão dos parágrafos do artigo, mediante os quais se destaca que o legítimo interesse deve sempre vir acompanhado dos princípios da adequação, necessidade e transparência bem como da possibilidade de fiscalização. Ademais, prevemos que deverá se basear em **situação concreta** e desde que atendidas as **legítimas expectativas do titular**" (grifos do próprio Relator) (2016, p. 34 e 35).

Assim, depois de idas e vindas nas audiências públicas, projetos de lei e debates legislativos, o legítimo interesse se consolidou na LGPD com o seguinte texto:

---

[10] Conforme art. 13 do Projeto de Lei 4.060/2012.

[11] O documento está disponível na Ficha de Tramitação do Projeto de Lei 4.060/2012, na Câmara dos Deputados: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=6C9A1A65CF90E0CC855A7B51E61FA03F.proposicoesWebExterno1?codteor=1663305&filename=Tramitacao-PL+4060/2012. Acessado em: 29/09/2020.

> *"Art. 7º [...] IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais"*

3.2. Requisitos

Os requisitos para utilização desta base legal estão presentes no próprio texto da LGPD, não apenas no próprio artigo 7º, mas também em outros artigos da lei, a exemplo do artigo 10:

> Art. 10. O **legítimo interesse do controlador** somente poderá fundamentar tratamento de dados pessoais para **finalidades legítimas**, consideradas a partir de **situações concretas**, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, **somente os dados pessoais estritamente necessários para a finalidade** pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a **transparência do tratamento de dados** baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador **relatório de impacto à proteção de dados pessoais**, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Desta forma, Cots *et al.* (2020) trouxeram os requisitos que devem ser observados para que o legítimo interesse seja utilizado, quais sejam: "interesse do controlador ou de terceiros, finalidades legítimas, situações concretas, proteção dos direitos do titular ou benefício ao titular, observando-se a legítima expectativa dele, o princípio da necessidade e o princípio da transparência" (p.66). Há um requisito adicional, que é o registro das operações de tratamento de dados pessoais, indicado no artigo 37 da LGPD:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

O legítimo interesse se torna uma hipótese que permite o tratamento de dados pessoais em situações que não foram antevistas pelo legislador. Porém, não se deve confundir esta afirmação com um entendimento equivocado de que se pode utilizá-lo em qualquer situação, como se fosse um cheque em branco. Nesse sentido, Beppu e Paiva (2019) mostram que o legítimo interesse pode ser utilizado quando:

> "Quando, no mundo dos fatos, depara-se com situação *in concreta*, não antecipada pelo legislador, que impõe intervenção restritiva aos direitos fundamentais dos titulares, para realização de um direito ou interesse prevalecente" (p. 105)

Buscando delimitar as possibilidades de uso, a autoridade nacional do Reino Unido (ICO, na sigla em inglês) indica situações em que esta hipótese de tratamento pode ser a mais adequada:

> "i. O tratamento não é obrigatório por lei, mas traz claro benefício para o controlador ou para terceiros;
> ii. Ocorre um impacto limitado na privacidade do titular;
> iii. O titular deve esperar razoavelmente que o controlador utilize os dados pessoais dessa maneira; e
> iv. O controlador não pode (ou não quer) dar ao titular controle total inicial (ou seja, consentimento) ou incomodá-lo com solicitações de consentimento disruptivas quando é improvável que ele se oponha ao tratamento." (ICO, 2016?b)

Percebe-se que esta autoridade nacional estrangeira segue linha semelhante àquela adotada pelo Deputado Orlando Silva (PCdoB), mencionada acima, a evitar o bombardeamento do titular com repetidas solicitações de consentimento, que poderia causar a chamada "fatiga do consentimento", situação em que o usuário passa a clicar no Aceite sem sequer ler ou entender o contexto do tratamento a ser realizado, pela simples profusão interminável de pedidos de consentimento. Dentre as diversas apostas para evitar-se tal fatiga está o uso do legítimo interesse como base legal para tratamento (MONTEZUMA; TAUBMAN-BASSIRAN, 2019).

A legislação brasileira, por sua vez, identifica duas situações em que o legítimo interesse pode ser utilizado, nos incisos do artigo 10 mencionado acima.

Esta lista não considera todas as situações concretas que possam surgir no horizonte do controlador, e de acordo com o próprio texto legal não pode ser considerada extensiva, ao mesmo tempo em que determina que as situações de tratamento devem ser concretas (não podem estar no campo da pura imaginação).

O primeiro inciso do artigo 10 indica a utilização do legítimo interesse para "apoio e promoção de atividades do controlador". Nesse sentido, o inciso está em linha com o princípio constitucional da livre iniciativa, previsto no artigo 1º, IV, base da atividade econômica, bem como do art. 2º , VI da própria LGPD, que também utiliza a livre iniciativa como fundamento da lei de proteção de dados. Neste sentido Cots *et al.* (2020) tratam da busca de lucro como hipótese de utilização do legítimo interesse, indicando positivamente pela utilização neste contexto "é correto concluir que a busca pelo lucro permite o tratamento de dados pessoais [...]

hipótese de aplicação do Legítimo Interesse" (p. 74). Beppu e Paiva (2019), tratando de situações de marketing empresarial, aponta que uma relação prévia existente entre controlador e titular traria maior relevância ao uso do legítimo interesse. Desta forma, ainda que a legislação possa permitir a busca de lucro como hipótese para utilização desta base legal, ainda assim ela precisaria ser utilizada com cautela.

Mantendo o caráter principiológico da legislação, também é necessário observar os princípios da necessidade (artigo 6º, III) e transparência (artigo 6º, VI):

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
> III - necessidade: **limitação do tratamento ao mínimo necessário** para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> VI - transparência: **garantia**, aos titulares, **de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento** e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

3.3. Registro das operações de tratamento

Outro requisito para utilização desta base legal é o registro das operações de tratamento de dados pessoais, vinculado ao mandamento do artigo 37 da LGPD:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, **especialmente quando baseado no legítimo interesse.**

Ele permite à organização ter visibilidade em relação aos seus processos/fluxos que envolvem dados pessoais e as hipóteses de legitimação definidas para cada fluxo, demonstrando de forma detalhada os fluxos de dados pessoais identificados na operação. Cada fluxo consiste em descrever e analisar o ciclo de vida do dado pessoal, ou seja, todas as etapas do tratamento. Assim, cada fluxo traz visibilidade à empresa em relação às fases do dado pessoal na empresa, desde a coleta até o armazenamento e finalmente sua exclusão.

Este registro, também chamado de ROPA na sigla em inglês (*Records of Processing Activities*), é a criação de um inventário das operações de tratamento, demonstrando de forma detalhada, descrevendo e analisando o ciclo de vida dos dados pessoais, desde a coleta até a sua exclusão. Este instrumento garante visibilidade ao controlador, permitindo controlar os seus processos. Diferentemente do GDPR, que em seu artigo 30 traz as informações que devem

constar do registro, a LGPD, é silente em relação ao tema. Desta forma, vem do GDPR e das melhores práticas adotadas no Brasil a inspiração para uma lista razoável para o registro[12]:

i. Os atores envolvidos no tratamento;
ii. A finalidade e o detalhamento do tratamento;
iii. As categorias dos titulares;
iv. As categorias de dados pessoais;
v. A origem do dado pessoal;
vi. Os sistemas utilizados e as medidas técnicas e organizacionais de segurança utilizadas;
vii. A existência de suporte físico;
viii. Quem tem acesso aos dados pessoais (internamente e externamente, incluindo-se as transferências internacionais);
ix. A documentação que apoia o processo;
x. A existência de tratamento automatizado de acordo com o art. 20 da LGPD;
xi. O tempo de armazenamento; e
xii. A base legal utilizada.

É interessante notar que, para a LGPD, o registro é obrigatório para todos os controladores e operadores, enquanto o GDPR cria uma regra de exceção, no artigo 30 (5), para desonerar as empresas com menos de 250 trabalhadores, exceto se:

> "[...] o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.o, n.o 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.o."

O registro das operações de tratamento possui uma miríade de funções, pois para além de 1) obedecer a uma determinação legal, o ROPA dá 2) visibilidade aos agentes de tratamento sobre as operações realizadas, permitindo ajustes que 3) aumentem a eficiência do tratamento, minimizando a coleta e tratamento de dados pessoais que não são necessários para a finalidade pretendida. Além disso, 4) facilita a resposta a incidentes de segurança, pois na medida em que a informação chega de que um sistema foi comprometido, um filtro no ROPA permitirá identificar todos os fluxos de dados pessoais em que o sistema comprometido é utilizado. O ROPA também pode ser utilizado para uma possível 5) defesa perante a autoridade nacional,

[12] Agradeço o auxílio dos advogados Patricia Peck e Marcelo Crespo na elaboração desta lista.

pois traz incidentalmente o caminho do dado pessoal no tratamento, e auxiliará na demonstração de que o agente de tratamento tomou os melhores esforços para se manter em Compliance com a legislação.

Como se observa, talvez seja ainda mais importante para a própria operação dos agentes de tratamento que seja realizado um registro de suas operações de tratamento do que para o simples cumprimento do artigo 37 da LGPD.

3.4. LIA – Legitimate Interests Assessment

Como visto, para se evitar a utilização do legítimo interesse como base legal genérica, que permite o tratamento de dados pessoais sob qualquer interesse legítimo do controlador, se faz necessária uma análise específica, que irá analisar se cada um dos requisitos foram cumpridos, e especialmente colocando, de um lado, os **interesses legítimos do controlador ou de terceiros**, e de outro lado, **os direitos e liberdades fundamentais do titular**. Esse balanceamento entre esses dois direitos é essencial e, portanto, mais do que a existência de um interesse legítimo, é fundamental que este prevaleça frente aos direitos fundamentais em relação a proteção de dados pessoais dos titulares (BEPPU; PAIVA, 2019).

Os direitos e liberdades fundamentais do titular, ou seja, do cidadão, está amparado essencialmente no Título II da Constituição Federal, que dispõe sobre "Dos Direitos e Garantias Fundamentais", mas também na legislação esparsa, que traz direitos e liberdades consideradas a partir de setores ou pontos de vista específicos (como o Código de Defesa do Consumidor – CDC).

Os interesses legítimos do controlador ou de terceiros, no entanto, importado do artigo 6º (f) do GDPR, precisam se valer de outras condições para estarem em condições de serem comparados aos direitos dos titulares. Interesses puramente particulares dos controladores, por exemplo, dificilmente se sobreporiam aos direitos fundamentais dos titulares. Precisam ter "relevância jurídica equiparável àqueles, sob pena de não poderem ser colocados na balança" (BEPPU; PAIVA, 2019). A legitimidade dos interesses dos controladores é encontrada quando, por exemplo, tal interesse possa ser perseguido "de acordo com as leis de proteção de dados e demais legislações esparsas. Em outras palavras, um interesse legítimo deve ser 'admissível nos termos da lei'" (WP29, 2014, p. 25). Embora tal afirmação tenha sido feita com base na

Diretiva 95/46/EC[13], os parâmetros da legitimidade do interesse do controlador permanecem. Ainda, a decisão da autoridade nacional da República Tcheca no caso UOOU-03390/19-7, 07 de outubro de 2019, explicita que "os interesses legítimos do controlador precisam ser legais, ou seja, em conformidade com os regulamentos legais, e claramente formulados (não especulativos)"[14].

Impõe ao controlador realizar esta análise e avaliar a viabilidade ou não da utilização da base legal do legítimo interesse. Não será possível determinar, *a priori*, se a análise foi efetuada com sucesso, ou se o resultado encontrado pelo controlador resistirá ao teste do tempo. Não havendo determinação legal específica, caberá ao controlador realizar seu juízo a respeito, que será confirmada pelos órgãos de controle caso haja provocação futura ou decidam de ofício se manifestar (BEPPU; PAIVA, 2019).

Uma forma de se verificar se os requisitos legais estão sendo atendidos é a realização de um *Legitimate Interests Assessments* (LIA), ou seja, um relatório para avaliação de risco de legítimo interesse, que permitirá realizar as análises necessárias e fundamentar o uso do legítimo interesse como base legal para tratamento dos dados pessoais. Este relatório não é mencionado textualmente na LGPD ou no GDPR, e decorre da situação prática de dar clareza ao cumprimento dos requisitos para utilização do legítimo interesse.

O relatório, de forma livre, é o resultado de uma análise em três etapas que busca mostrar ao controlador a viabilidade da utilização do legítimo interesse, por meio de uma ponderação específica. Seguindo as instruções da autoridade nacional de proteção de dados do Reino Unido (ICO, 2016?b):

i. Finalidade: existe interesse legítimo para o tratamento? Por que o tratamento deve ser realizado? Quais os benefícios esperados do tratamento? Terceiros se beneficiarão? Haverá benefícios coletivos ou públicos? Qual impacto haveria na ausência do tratamento? Existe alguma obrigação legal que será cumprida se o tratamento for realizado? Existem discussões éticas sobre a realização do tratamento?

[13] Importante notar que as Orientações do GT29 se basearam na Diretiva 95/46/EC, que foi sucedida pelo GDPR. Assim, precisa ser analisada com cuidado posto que baseada em norma que não se encontra mais em vigor.
[14] "The controller's legitimate interests must first be lawful, i.e., in compliance with legal regulations, and clearly formulated (not speculative)" no original em inglês.

ii. Necessidade: o tratamento é necessário para atingir a finalidade? O tratamento é proporcional à finalidade? É possível atingir a finalidade sem realizar este tratamento? É possível atingir a finalidade tratando menos dados pessoais, ou de forma menos óbvia ou intrusiva?

iii. Teste de balanceamento: Os interesses dos titulares se sobrepõem ao legítimo interesse do controlador ou de terceiros?

   a. Natureza dos dados: O tratamento inclui dados pessoais sensíveis? Os dados pessoais tratados são considerados normalmente como "privados"? Estão sendo tratados dados pessoais de crianças, adolescentes ou pessoas em situação de vulnerabilidade? Os dados são dados pessoais por questões pessoais ou profissionais?

   b. Expectativas dos titulares: Existe relação anterior com o titular? Em caso positivo, qual a natureza e como os dados pessoais foram utilizados no passado? A coleta de dados pessoais foi feita diretamente do titular? O que foi dito a ele quando da coleta? Se a coleta foi feita por terceiros, o que eles disseram sobre compartilhamento ou reutilização dos dados pessoais? Você se encaixa nesses avisos dos terceiros? Quanto tempo faz que os dados pessoais foram coletados? Houve mudança tecnológica ou de contexto que poderiam afetar as expectativas dos titulares? A finalidade pretendida e método de tratamento são entendidos pelo público? Você está buscando realizar algo completamente novo? Você possui alguma prova sobre as expectativas dos titulares (por exemplo, pesquisa de mercado, grupos focais ou outras formas de consulta)? Existem outros fatores ou circunstâncias particulares que alterariam as expectativas dos titulares?

   c. Probabilidade de impacto: Quais são os impactos possíveis do tratamento? Os titulares irão perder o controle sobre o uso de seus dados pessoais? Qual a probabilidade e a gravidade dos impactos potenciais? Há probabilidade de alguns titulares se oporem ao tratamento ou o considerarem intrusivo? Você estaria confortável em explicar o tratamento para os titulares? Você consegue adotar medidas para minimizar os impactos? Os usuários podem se opor ou solicitar que o tratamento se encerre?

Bruno Bioni (2019) também indica um quarto item a ser incluído no Legítimo Interesse: Salvaguardas, relacionado à transparência nas operações de tratamento com base no

legítimo interesse (artigo 10, § 2º) e minimização dos riscos aos titulares e considerando-se o direito de oposição (*opt-out*) do titular ao tratamento.

Ao final do teste, o controlador deverá ser capaz de responder à pergunta: "Posso utilizar o legítimo interesse como base legal para o tratamento de dados pessoais pretendido?" além de determinar se uma análise adicional, o Relatório de Impacto de Privacidade (Data Protection Impact Assessment – DPIA, na sigla em inglês).

3.1. Relatório de Impacto à Proteção de Dados Pessoais

Para a correta utilização do legítimo interesse como base legal para tratamento de dados pessoais, é necessário observar o que a legislação dispõe sobre o Relatório de Impacto à Proteção de Dados Pessoais, também conhecido como "Data Protection Impact Assessment" (ou DPIA, na sigla em inglês). A definição do relatório se encontra no inciso XVII do artigo 5º da LGPD:

> *Art. 5º (...)*
> *XVII - **relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;*

Como definido pela legislação, o relatório só tem cabimento caso o agente de tratamento seja controlador no fluxo de dados pessoais analisados. Para não deixar dúvidas sobre a quem recai a obrigação do referido, o legislador optou pelo texto "documentação do **controlador**", repetido nas demais instâncias em que o relatório aparece na legislação: artigo 10, § 3º, "A autoridade nacional poderá solicitar **ao controlador** relatório de impacto à proteção de dados pessoais" e artigo 38, "A autoridade nacional poderá determinar **ao controlador** que elabore relatório de impacto à proteção de dados pessoais", ambos da LGPD.

Assim, à primeira vista o relatório não seria obrigatório para todos os tratamentos de dados pessoais, visto que a legislação afirma que o relatório deve conter a descrição dos processos de tratamento "que podem gerar riscos às liberdades civis e aos direitos fundamentais". Por outro lado, se o operador do direito entende que todas as disposições da LGPD buscam "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", conforme artigo 1º da lei, deve-se tomar com bastante atenção os casos em que o relatório é necessário.

Por sua vez, a legislação garantiu à autoridade nacional permissibilidade para solicitar o relatório quando o tratamento for realizado sob o legítimo interesse (artigo 10, § 3º) ou, ainda, sob determinação da autoridade nacional em qualquer caso (artigo 38), ainda que nesta hipótese precisa haver regulamento editado pela autoridade nacional (conforme artigo 55-J, XIII) que embase a prática. Identificamos, portanto, três situações em que é recomendado aos controladores elaborar o relatório de impacto à proteção de dados pessoais:

i. Quando o tratamento possa gerar riscos às liberdades civis e aos direitos fundamentais;
ii. Quando o tratamento se apoiar no legítimo interesse; e
iii. Quando for realizado tratamento de dados pessoais sensíveis.

Os dois primeiros itens desta lista decorrem da leitura explícita da lei. A inclusão do 3º item à lista se deve ao fato de que a legislação optou por não apenas destacar que o relatório pode ser solicitado pela autoridade nacional para dados pessoais sensíveis, como pois optou em destacar os dados pessoais sensíveis do tratamento de dados pessoais "comuns", indicando seu maior potencial de geração de riscos às liberdades civis e aos direitos fundamentais dos titulares.

Com base neste entendimento, supomos algumas situações em que o relatório de impacto à proteção de dados pessoais poderia ser elaborado:

i. O modelo de negócio da empresa utilizar técnicas de perfilamento (*profiling*), decisões automatizadas que elaborem juízos sobre titulares de dados ou ainda auxílio na tomada de decisões quanto à oferta de produtos, serviços ou benefícios;
ii. For realizado monitoramento sistemático dos titulares de dados;
iii. For realizado tratamento de dados pessoais em larga escala;
iv. O processo de negócio fizer uso de novas tecnologias;

Em relação ao que deve estar presente no relatório utilizaremos também o GDPR, especialmente em seu artigo 35 e nos Recitais 84 e 90, bem como o website sobre o tema, publicado pela autoridade nacional do Reino Unido (ICO, 2016?a):

i. A natureza, escopo, contexto e finalidade do tratamento;
ii. Avaliação da necessidade, proporcionalidade e medidas de Compliance;
iii. Identificação e *assessment* dos riscos aos titulares de dados; e

iv. Identificação de quaisquer medidas para mitigar esses riscos.

v. A descrição dos tipos de dados pessoais coletados;

vi. O procedimento utilizado para a coleta dos dados pessoais;

vii. Os mecanismos aplicados para segurança dos dados pessoais; e

viii. A análise do Encarregado pelo Tratamento de Dados Pessoais (DPO) com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Este relatório, por óbvio, deve ser feito em conjunto com o Encarregado, que irá supervisionar o processo e garantir que as demandas da análise tenham sido atendidas. Neste processo também se buscará entender se não existiria outra hipótese legal de tratamento dos dados pessoais que melhor se adeque ao contexto do tratamento para atender as expectativas razoáveis do titular.

A análise do Encarregado mencionada no "item viii" acima deve levar em conta a probabilidade de o risco acontecer, bem como o impacto aos titulares de dados caso ocorra. Isto é feito, normalmente, através da elaboração de uma matriz de risco, conforme imagem abaixo:

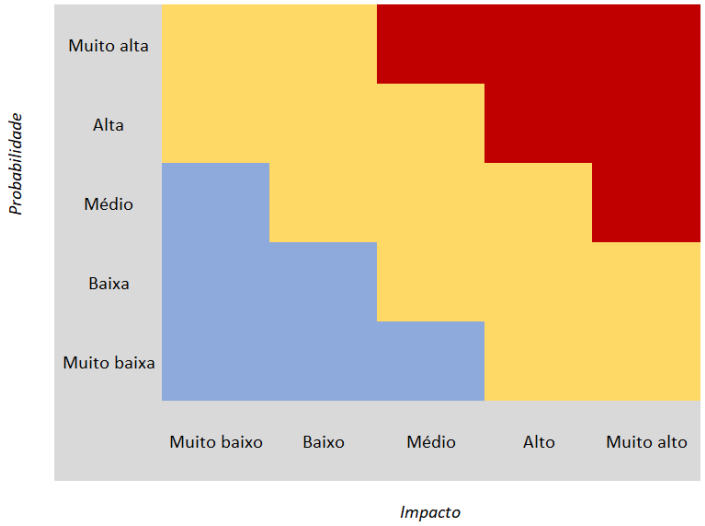


Figura 1 - Matriz de Risco, elaborada pelo autor

Para melhor auxiliar no preenchimento da matriz de risco, antevemos os seguintes parâmetros, em relação à probabilidade de incidente acontecer:

i. Probabilidade muito baixa: muito improvável que ocorra nos próximos 12 meses;

ii. Probabilidade baixa: não é impossível que ocorra nos próximos 12 meses;

iii. Probabilidade média: possível e pode ser esperado pelo menos uma vez nos próximos 12 meses;

iv. Probabilidade alta: é provável que surja uma vez durante os próximos 12 meses;

v. Probabilidade muito alta: quase certo de que ocorrerá várias vezes durante os próximos 12 meses.

E em relação ao impacto para o titular de dados:

i. Impacto muito baixo: pouca ou nenhuma consequência;

ii. Impacto baixo: algumas consequências;

iii. Impacto médio: consequências inegáveis, mas limitadas;

iv. Impacto alto: consequências significativas;

v. Impacto muito alto: consequências imediatas e graves;

Em relação aos passos que devem ser tomados para a correta elaboração de um relatório de impacto à proteção de dados pessoais, seguimos novamente às instruções da autoridade nacional do Reino Unido (ICO, 2016?a), que desenvolveu um fluxo como passo a passo:

Figura 2 - ICO: Passos para realizar um Relatório de Impacto à Proteção dos Dados Pessoais

Cada um desses passos será apenas brevemente analisado, para garantir maior clareza em relação ao passo a passo para elaboração do relatório:

i. Identificar a necessidade do relatório: avaliar em quais atividades de tratamento será necessária a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais, identificando os riscos e formalizando as ações que os minimizam;

ii. Descrever o tratamento: feito de maneira detalhada, analisando o fluxo da atividade de tratamento do início ao fim, ou seja, da coleta à exclusão dos dados pessoais;

iii. Considerar a necessidade de consultas: avaliar a necessidade de consultar os titulares dos dados, parceiros (como operadores), Encarregados (do próprio controlador ou de outras empresas do grupo, quando necessário) e a autoridade nacional;

iv. Avaliar a necessidade e a proporcionalidade: identificar a real necessidade da realização do tratamento para atingir a finalidade proposta e a proporcionalidade dos métodos escolhidos. É possível atingir o mesmo resultado com outro tipo de tratamento, menos invasivo ao titular de dados? Ou ainda, perguntar-se se é possível aplicar técnicas para mitigar o impacto causado, como valer-se do princípio da minimização;

v. Identificar e avaliar os riscos : Na etapa final do relatório, após a descrição da atividade de tratamento e da avaliação de necessidade e proporcionalidade, será possível identificar os eventuais riscos gerados;

vi. Avaliar e armazenar resultados: após identificar os riscos, é necessário avaliar quais medidas deverão ser tomadas para mitigar ou mesmo eliminar os riscos aos titulares dos dados. Algumas medidas que podem ser utilizadas são a minimização dos dados, a eliminação de decisões automatizadas, entre outros;

vii. Integrar os resultados ao tratamento: os resultados obtidos por meio do relatório deverão ser implementados à atividade de tratamento, modificando e/ou trazendo melhorias à operação;

viii. Constante revisão: uma vez que as atividades de tratamento são fluídas e sofrem modificações ao longo de sua aplicação, é necessário manter os relatórios sob revisão periódica e atualizá-los sempre que novidades sejam inseridas no contexto do tratamento.

4. Decisões de consenso pelo artigo 60 GDPR

As especificidades dos requisitos de utilização do legítimo interesse como base legal para tratamento de dados pessoais podem levar a situações de difícil compreensão sobre a

possibilidade ou não de sua aplicabilidade, posto que para além de flexível, é uma base legal que depende de análises subjetivas por parte do controlador. Estas análises só serão checadas em um segundo momento, sob algumas condições, pela Autoridade Nacional de Proteção de Dados Pessoais.

Assim, é importante analisarmos situações concretas de aplicabilidade do legítimo interesse. O GDPR servirá de base para nossa análise, visto que o regulamento já está em vigor desde 2018, com duas decisões proferidas pelo artigo 60, que versa sobre a cooperação entre mais de uma autoridade nacional. Entendemos que, apesar de em menor número, as decisões tomadas pelo artigo 60 possuem mais peso, visto que suas investigações são feitas por uma autoridade nacional principal (líder), assistida por uma ou mais autoridades nacionais interessadas de outros Estados-membro, procurando alcançar um consenso entes as diversas autoridades nacionais envolvidas, em procedimento de controle de coerência para o entendimento de um assunto dentre os Estados-membro.

> *Artigo 60 Cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas*
> *1. A autoridade de controlo principal coopera com as outras autoridades de controlo interessadas nos termos do presente artigo para procurar alcançar um consenso. A autoridade de controlo principal e as autoridades de controlo interessadas trocam entre si todas as informações pertinentes. (UNIÃO EUROPEIA. GDPR, 2016)*

A primeira decisão analisada é a EDPBI:CZ:OSS D:2019:56, de 07/10/2019[15]. Liderada pela autoridade nacional da República Tcheca – *Úřad pro ochranu osobních údajů* (ÚOOÚ) – com participação das autoridades nacionais da Áustria, Hungria, Eslovênia e Eslováquia, bem como todas as autoridades alemãs[16].

O caso trata do tratamento de dados pessoais de devedores, com a publicação, nas páginas online da controladora e em rede social (Facebook), de dados pessoais relativos à esses débitos, quais sejam, o primeiro nome abreviado, o sobrenome, o status de devedor e o crédito devido. O controlador não obteve o consentimento dos titulares e buscava legitimar o

[15] Caso UOOU-03390/19-7 pela numeração da autoridade nacional da República Tcheca.
[16] A Alemanha possui uma autoridade federal (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit), que é responsável pela proteção de dados pessoais nos serviços postais e de telecomunicações. As demais atribuições ficam a cargo das autoridades estaduais.

tratamento pelo legítimo interesse. No entanto, no teste de balanceamento entre os direitos do controlador e os interesses e direitos dos titulares, estes prevaleceriam, em face do risco de impacto negativo que a publicação poderia causar aos titulares. Por fim, foi emitida decisão para que o controlador cessasse o tratamento, removendo os dados pessoais das páginas online.

Trata-se de um caso difícil para o controlador, pois se por um lado existe um interesse – legítimo – em cobrar os devedores, com a existência de um direito apoiado legalmente, por outro lado esse direito se contrapõe aos direitos fundamentais dos titulares. A alta exposição de uma situação financeira negativa pode impactar negativamente os titulares em sua vida particular e profissional, com exclusão social do titular e dos seus familiares e a perda do emprego. Assim, esse tratamento extrapolaria o necessário para finalidade pretendida, sendo desproporcional no resultado do teste de balanceamento realizado pelas autoridades nacionais na análise do caso. Dentre outros pontos, a decisão apontou que ainda que haja interesse legítimo do controlador, o tratamento também precisa ser necessário para a finalidade, e se a finalidade puder ser atingida com tratamento de menos dados pessoais, ou tratamento que atinja os direitos dos titulares em menor grau, assim deve ser feito. Por conta disso, entenderam que não havia base legal para o tratamento dos dados pessoais e, portanto, determinaram o fim do tratamento com a exclusão dos dados pessoais publicados.

Uma segunda decisão analisada segundo os auspícios do artigo 60 do GDPR é a EDPBI:DENW:OSS D:2018:2, de 21 de dezembro de 2018. Liderada pela autoridade alemã estadual de North Rhine-Westphalia e participação das autoridades estaduais alemãs de Rhineland-Palatinate, Mecklenburg-Western Pomerania, Bavaria (priv), Lower Saxony, Saarland e da autoridade nacional espanhola (*Agencia Española de Protección de datos*).

O caso envolve o envio de publicidade (marketing direto) pelos correios e a tentativa do titular de dados de exercer os direitos de acesso (artigo 13) e de exclusão (artigo 17) do GDPR. O marketing é uma hipótese em que o legítimo interesse pode ser utilizado, no GDPR, de acordo com o Recital 47 “Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta”[17]. A investigação das autoridades nacionais não encontrou direitos fundamentais dos titulares que pudessem prevalecer sobre os interesses legítimos do controlador, inclusive porque no caso europeu os dados pessoais utilizados foram considerados acessíveis publicamente. Em relação à impossibilidade de o

[17] Note-se que esta declaração expressa inexiste na LGPD.

titular exercer o direito à exclusão do artigo 17 do GDPR, a decisão diz que os pedidos foram feitos antes da entrada em vigor do GDPR, portanto não aplicáveis naquele momento. Mas indicaram que o controlador precisaria garantir transparência no tratamento, informando os titulares sobre a origem dos dados pessoais[18] em comunicações futuras. Desta forma, o entendimento final sobre o caso foi que o tratamento de dados pessoais disponíveis publicamente para marketing direto é hipótese legal cabível do legítimo interesse sob o GDPR. No Brasil, a LGPD é omissa em relação ao tema do marketing.

Bioni (2019), em linha com a análise europeia (UNIAO EUROPEIA, 2002; WP29, 2014) afirma que "seja quem já mantém uma relação previamente estabelecida com o titular dos dados, seja no caso de terceiros que compõem uma rede de publicidade comportamental" (p.337) possuiria interesse legítimo no tratamento. No entanto, ao aprofundarmos a análise, podemos separar a utilização do legítimo interesse nos casos de marketing direto e em marketing indireto. No primeiro caso, em que existe uma relação prévia entre o controlador e o titular de dados pela aquisição de produtos ou serviços, esta base legal poderia ser utilizada (BIONI, 2019, p. 338). O uso dos dados pessoais por um controlador que possui relação com o titular para anunciar produtos semelhantes aos comprados anteriormente, como por exemplo almofadas para complementar o visual de quem acabou de comprar um sofá, estaria dentro do considerado esperado pelos titulares e compatível com a coleta original, desde que observados os demais requisitos, como a transparência no tratamento (GASPAR, informação verbal [19]).

Já no caso de marketing indireto, em que não há relação prévia entre controlador e titular de dados, encontraria dificuldades em apoiar o processo no legítimo interesse, dada a ausência de qualquer expectativa dos titulares em receberem a comunicação publicitária, restando a utilização do consentimento como base legal (UNIAO EUROPEIA, 2002; WP29, 2014; EDPB, 2020; GBA, 2020).

5. Conclusão

Este trabalho buscou mostrar como a hipótese de tratamento de dados pessoais chamada de "Legítimo interesse" não pode ser considerada uma hipótese residual, a ser utilizada quando não for possível encaixar o tratamento em nenhuma das demais hipóteses

[18] Encontramos disposições semelhante na LGPD, no artigo 6º, VI e, especificamente para o legítimo interesse, no artigo 10, § 2º.
[19] O tema foi debatido largamente por telefone com Marina Limberti Gaspar, advogada na área de Proteção de Dados Pessoais.

legais. Embora ampla, possui condições e requisitos próprios e que devem ser observados pelos operadores do direito.

Não apenas hipótese com características próprias, a utilização do legítimo interesse para apoiar tratamento de dados pessoais deve ser feita com cuidado, utilizando-se ferramentas de avaliação como o *Legitimate Interests Assessment* (LIA), teste de balanceamento e o relatório de impacto à proteção dos dados pessoais (DPIA, na sigla em inglês).

Avaliamos também casos práticos onde o legítimo interesse pode ou não ser utilizado, apoiados por decisões de autoridades nacionais europeias. Entendemos que o LGPD, apesar de não ser mera tradução do regulamento europeu de proteção de dados pessoais (GDPR), no caso do legítimo interesse possui inúmeras similaridades, desde a sua origem na legislação e, assim, é de se esperar que o entendimento da Autoridade Nacional de Proteção de Dados brasileira (ANPD) seja semelhante às conclusões das autoridades europeias.

Não podemos olvidar do aspecto humano nas das decisões. No mais das vezes, será necessário que o Encarregado dos Dados Pessoais, seu time e a direção da empresa realizem uma análise sobre os riscos envolvidos na operação, seus benefícios e os limites impostos pela autoridade nacional por meio de regulamentos e opiniões. A resposta sobre se a decisão pela utilização do legítimo interesse foi correta poderá demorar anos para ser respondida, mas as pesadas sanções que a legislação impõe deve ser levada em conta a todo momento. Por outro lado, entender a LGPD como um incentivo à criação de um programa de *Privacy Compliance* pode trazer benefícios às empresas no médio e longo prazo, com a solidificação de uma cultura de proteção de dados pessoais que reduzirão significativamente os riscos aos quais ela está exposta.

Por fim, cabe lembrar que a proteção de dados pessoais é tema novo no Brasil e ainda há um longo caminho a ser percorrido para que os entendimentos acerca de temas complicados como a aplicação de bases legais se consolidem.

6. Referências

ARTICLE 29 DATA PROTECTION WORKING PARTY (WP29). **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Acesso em: 09 abr. 2014.

BEPPU, Ana Claudia; PAIVA, Tomás Filipe Schoeller Ribeiro. Os Fundamentos Legais para Tratamento de Dados Pessoais: os incisos I e IX do Artigo 7º da Lei nº 13. In: BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia (org.). **Proteção de Dados Pessoais no Brasil**: uma nova visão a partir da lei nº 13.709/2018. Belo Horizonte: Forum, 2019. Cap. 4. p. 101-122.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. 316 p.

BOEHM, Camila. **Número de empresas com home office deve crescer 30% após pandemia**. 2020. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2020-04/numero-de-empresas-adotam-home-office-deve-crescer-30-apos-pandemia. Acesso em: 01 jun. 2020.

BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia (org.). **Proteção de Dados Pessoais no Brasil**: uma nova visão a partir da lei nº 13.709/2018. Belo Horizonte: Fórum, 2019. 326 p.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Marco Civil da Internet**. Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1 jun. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **LGPD**. Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 jun. 2020.

CASTELLS, Manuel. **A Sociedade em Rede**. 6. ed. São Paulo: Paz e Terra, 2011. 720 p. Tradução de: Jussara Simões.

CASTELLS, Manuel. **Roda Viva (Manuel Castells | 1999)**. São Paulo: Fundação Padre Anchieta, 1999. Legendado. Disponível em: https://www.youtube.com/watch?v=TaXeu4k4OJE. Acesso em: 02 jun. 2020.

COTS, Márcio *et al* (org.). **O Legítimo Interesse e a LGPDP**. São Paulo: Thomson Reuters, 2020. 312 p.

CRESPO, Marcelo *et al*. Risk Assessments e Relatórios de Impacto: Ferramentas para avaliação de riscos em programas de Compliance Digital e de Proteção de Dados. In: CRESPO, Marcelo (org.). **Compliance em Direito Digital Volume 3**. São Paulo: Thomson Reuters - Rt, 2020. p. 1-1.

CRESPO, Marcelo; BELOTO, Guilherme. Privacy compliance challenges in 2020 and beyond. **Compliance And Ethics Professional (Cep) Magazine**, Minneapolis, v. 5, n. 10, p. 1-1, jan. 2020. Mensal.

CRESPO, Marcelo; GASPAR, Marina; BELOTO, Guilherme. Os desafios de implementação da LGPD: uma visão a partir dos princípios do art. 6º da LGPD. In: PECK, Patricia (org.). **Direito Digital Aplicado 4.0**. São Paulo: Thomson Reuters - Rt, 2020. p. 1-1.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 08/2020 on the targeting of social media users**. 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf. Acesso em: 24 ago. 2020.

GEGEVENSBESCHERMINGSAUTORITEIT (GBA)/ AUTORITÉ DE PROTECTION DES DONNÉES (Bélgica). **RECOMMANDATION n° 01/2020 du 17 janvier 2020**. 2020. Disponível em: https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdf. Acesso em: 17 jan. 2020.

ICO (Reino Unido). **Data protection impact assessments**. 2016?a. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/. Acesso em: 08 set. 2020.

ICO (Reino Unido). **When can we rely on legitimate interests?** 2016?b. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-r. Acesso em: 14 jun. 2020.

KAUER, Gisele; BELOTO, Guilherme; CRESPO, Marcelo. Compliance Digital, GDPR e LGPD: expectativas, oportunidades e desafios. **Revista de Direito Digital**, São Paulo, v. 1, n. 1, p. 31-42, set. 2019. Semestral.

KELSEN, Hans. **Teoria Pura do Direito**. 6. ed. São Paulo: Martins Fontes, 1999. 271 p. Tradução de: João Baptista Machado.

KUNEVA, Meglena. **Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling**. 2009. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156. Acesso em: 14 jul. 2020.

MANUEL Castells | 1999. São Paulo: Fundação Padre Anchieta, 1999. Son., color. Legendado. Disponível em: https://www.youtube.com/watch?v=TaXeu4k4OJE. Acesso em: 02 jun. 2020.

MARINELI, Marcelo Romão. **Privacidade e Redes Sociais Virtuais**. 2. ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. 272 p.

MASSO, Fabiano del; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (org.). **Marco Civil da Internet**: lei 12.965/2014. São Paulo: Thomson Reuters, 2014. 272 p.

MONTEZUMA, Luis Alberto; TAUBMAN-BASSIRAN, Tara. **How to avoid consent fatigue**. 2019. Disponível em: https://iapp.org/news/a/how-to-avoid-consent-fatigue/. Acesso em: 29 jan. 2019.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais**: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraiva, 2018. 120 p.

REDAÇÃO E-COMMERCE BRASIL. **Com pandemia, e-commerce cresce 81% em abril e fatura R$ 9,4 bilhões**. 2020. Disponível em: https://www.ecommercebrasil.com.br/noticias/e-commerce-cresce-abril-fatura-compreconfie-coronavirus/. Acesso em: 01 jun. 2020.

SOARES, Pedro Silveira Campos. **A questão do consentimento na Lei Geral de Proteção de Dados**. 2019. Disponível em: https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados. Acesso em: 11 maio 2019.

STALLA-BOURDILLON, Sophie; PHILLIPS, Joshua; RYAN, Mark D. **Privacy vs. Security**. Londres: Springer, 2014. 124 p.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**. 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=HR. Acesso em: 06 jul. 2020.

UNIÃO EUROPEIA. **Convenção Europeia dos Direitos do Homem**. 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 06 jul. 2020.

UNIÃO EUROPEIA. **ePrivacy Directive**. Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Bruxelas, 2002. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=EN. Acesso em 16 ago. 2020.

UNIÃO EUROPEIA. **GDPR** - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acesso em: 01 jun. 2020.

WARREN, Samuel D.; BRANDEIS, Louis D.. The Right to Privacy. **Harvard Law Review**, [s.l.], v. 4, n. 5, p. 193, 15 dez. 1890. JSTOR. http://dx.doi.org/10.2307/1321160.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Guilherme de Carvalho Beloto

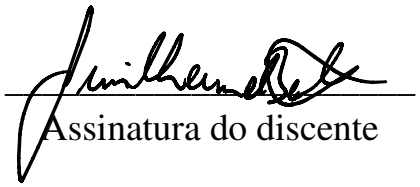
Aluno(a), regularmente matriculado(a), no Curso de Direito, na disciplina do TCC da 10ª etapa, matrícula nº 41533763, Período Noturno , Turma T ,

tendo realizado o TCC com o título: Aplicação do legítimo interesse como forma de legitimar o tratamento de dados pessoais

sob a orientação do(a) professor(a): Prof. Ms. Marcelo Romão Marineli
declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 09 de novembro de 2020.



Assinatura do discente