## UNIVERSIDADE DE SÃO PAULO

**Bacharelado em Gestão de Políticas Públicas**

## João Pedro Vieira Bueno Rocha 11206664

**Avaliando os impactos da GDPR e LGPD em perspectiva comparada**

## TRABALHO DE CONCLUSÃO DE CURSO

**São Paulo 2022**

## JOÃO PEDRO VIEIRA BUENO ROCHA

**Avaliando os impactos da GDPR e LGPD em perspectiva comparada**

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina ACH3538 - Trabalho de Conclusão de Curso, do curso de Gestão de Políticas Públicas da Universidade de São Paulo – USP, como requisito parcial para a obtenção do título de Bacharel.

Orientadora: Prof. Dr. Ana Carla Bliacheriene

SÃO PAULO 2022

## AGRADECIMENTOS

A comunidade da EACH, pelo constante incentivo a fazer sempre melhor, bem como amigos, professores, colegas e também a Secretaria da Fazenda do Município de São Paulo que me trouxe experiência no setor público e proporcionou meu crescimento profissional.

Também agradeço a minha família, que mesmo passando por muitas dificuldades, nunca me negou ajuda além de possibilitar minha chegada até aqui.

Por último, um grande obrigado a todos os que participaram direta ou indiretamente em minha formação.

## RESUMO

Rocha, João. **Título do trabalho:** Avaliando os impactos da GDPR e LGPD em perspectiva comparada, 2022. Trabalho de Conclusão de Curso (Graduação) – Gestão de Políticas Públicas. Universidade de São Paulo. São Paulo, 2022.

O trabalho visa abordar em perspectiva comparada por meio de bibliografias institucionais e acadêmicas a Lei Geral de Proteção de Dados brasileira e o Regulamento Geral sobre a Proteção de Dados europeu de forma abrangente, considerando que ambas as leis similares, a fim de comparar princípios legais e impactos das duas legislações. Envolvendo no processo, temas próximos ao direito civil e constitucional, a luz das lentes das políticas públicas.

**Palavras-chave:** LGPD. GDPR. Privacidade. Proteção. Titular.

## ABSTRACT

Rocha, João. **Title of the working:** Evaluating the effects of GDPR and LGPD in a detected perspective, 2022. Course Completion Work (Graduation) – Public Policy Management. University of Sao Paulo. São Paulo, 2022.

The work aims to approach in a comparative perspective through institutional and academic bibliographies the Brazilian General Data Protection Law and the European General Data Protection Regulation in a comprehensive way, considering that both laws are are similar, in order to compare principles laws and impacts of the two legislations. Involving in the process, themes close to civil and constitutional law, in the light of the lens of public policies.

**Keywords**: GDPR. LGPD. Privacy. Protection. Holder.

## LISTA DE SIGLAS

|  |  |
| --- | --- |
| LGPD | Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 |
| GDPR | Regulamento Geral sobre a Proteção de Dados 2016/679 |
| TI | Tecnologia da Informação |
| DSG | Lei austríaca de proteção de dados de 1978 - “*Datenschutzgesetz”* |
| BDSG | Lei alemã de proteção de dados de 1978 - “Bundesdatenschutzgesetz” |

**SUMÁRIO**

1. Introdução........................................................................................................1
2. [Objetivos..........................................................................................................2](#_TOC_250005)
   1. Objetivo Geral 2
   2. Objetivos Específicos 2
3. [Justificativa......................................................................................................3](#_TOC_250004)
4. Metodologia......................................................................................................5
5. [As Gerações de leis de privacidade...............................................................6](#_TOC_250002)

6 [Desenvolvimento............................................................................................11](#_TOC_250001)

7 Considerações finais 26

[Referências 28](#_TOC_250000)

## 1 INTRODUÇÃO

A LGPD e a GDPR são legislações muito parecidas, porém afetando territórios diferentes. No presente trabalhou buscou-se debater em perspectiva comparada ambas as leis, com enfoque principal na questão constitucional e principiológica que as duas normas se baseiam, levando a revisão bibliográfica qualitativa de textos acadêmicos e institucionais, para assim melhor avaliar os possíveis impactos de tais legislações.

Desta forma, buscando responder a pergunta de quais impactos, tanto na iniciativa privada como no setor público, que as normas proporcionaram no funcionamento dos processos organizacionais. Assim tendo como justificativa, a pesquisa dos diversos questionamentos que as leis de proteção abordadas proporcionam e também o entendimento do funcionamento da GDPR e da LGPD em perspectiva comparada.

Por esse propósito, foram recolhidos diversos textos acadêmicos de instituições creditadas e também informações relevantes de portais institucionais legítimos e amplamente reconhecidos.

Tendo o presente trabalho como objetivo, o estabelecimento de uma visão geral e abrangente sobre o tema, de maneira que seja possível traçar um paralelo em perspectiva comparada do Regulamento Geral sobre a Proteção de Dados 2016/679 europeu e da Lei Geral de Proteção de Dados Pessoais brasileira, Lei nº 13.709/2018. Assim dividindo o trabalho nos capítulos: Introdução, Objetivos, Justificativa, Metodologia, A Gerações das Leis de Privacidade, Desenvolvimento e Considerações Finais.

## OBJETIVOS

* 1. Objetivo Geral

Estabelecer uma visão abrangente e global do tema, abrangendo comparativamente a LGPD e a GDPR.

* 1. Objetivos Específicos

Analisar a GDPR e a LGPD nas lentes das políticas públicas; Analisar impactos da GDPR e da LGPD em instituições.

## Justificativa

Nos dias de hoje, a informação funciona como um motor da sociedade humana, então se fazem necessários mecanismos de infraestrutura nas organizações que recolham, armazenem, processem, representem e distribuam os dados. As organizações modernas recorrem à tecnologia da informação e comunicação para garantir o devido fluxo de dados intraorganizacionais. Assim se mostram importantes os conceitos essenciais sobre os sistemas de TI e as suas aplicações. Os sistemas de informação não são provenientes dos computadores e sim anteriores aos mesmos, já que o indivíduo humano consome informação para tomar decisões como forma de concretizar suas intenções. Então se mostram necessários os estudos comparativos acerca das Leis que governam os dados.

Ideias não flutuam no ar, mas sim são encarnadas e defendidas por atores diversos que possuem algum nível de interesse em um objetivo. Assim os interesses e as instituições coexistem conjuntamente, sendo possível que os autores lhes deem vida, então pode se dizer, que quando se há foco nas ideias, então existe o foco nos atores; e os ambientes de tomada de decisão estão repletos de conflitos e relações de poder, mas não necessariamente, de figuras de liderança. Assim devemos e podemos questionar, acerca das circunstâncias tecnológicas e de governança de dados que proporcionam que as novas ideias sejam impulsionadas nos diferentes níveis de organização humanos, à luz das normas legais.

Se por um lado se pode reclamar da eventual incapacidade das políticas públicas de atingirem seu objetivo final, por outro se deve entender que a não inclusão dos destinatários durante o processo decisório afeta diretamente tal fenômeno, e tal participação é inegavelmente trabalhosa. Então talvez, as políticas públicas se tornarão gradualmente mais responsivas à medida que a população toma as rédeas do processo decisório, assim possibilitando a participação democrática ativa.

Desta maneira demonstrando a importância de estudar e produzir conteúdo sobre as políticas públicas que regulam a informação. Desta forma, em uma atualidade que as leis de proteção se encontram em constante evolução, se torna

muito importante a participação cidadã dos indivíduos no debate acerca das leis que afetam os dados, como forma de evitar a discriminação de indivíduos ou grupos sociais e também como forma civil de participação no processo legislativo.

## METODOLOGIA

A omissão do Estado provoca o acréscimo do número de excluídos. A cidadania brasileira pode ser descrita como em construção, carecendo ainda de políticas públicas digitais promotoras de inclusão social.

Então o presente trabalho defenderá a integração do Estado e da Sociedade, por meio de uma revisão bibliográfica comparativa entre o Regulamento Geral sobre a Proteção de Dados europeu e a Lei Geral de Proteção de Dados Pessoais brasileira, e consequentemente do fator de territorialidade destes tipos de políticas públicas digitais.

Podemos pontuar, que as instituições ampliam sua legitimidade, à medida que ampliam o acesso à informação junto à sociedade, já que a informação facilita a ação das pessoas, e conjuntamente, a prática da cidadania. O provimento de dados de forma cautelosa, é dever das instituições públicas, visando assim, a real integração entre a sociedade civil e o Estado.O Estado brasileiro buscado pela maioria da sociedade, é um Estado tecnológico, participativo e permeável, que regula a atuação privada e protege os direitos constitucionais nacionais descritos pela Constituição Federal de 1988. Assim sendo o Estado de inclusão social, aquele que promove, valores de cidadania e democracia participativa.

Para obter os resultados e respostas acerca da problematização apresentada neste trabalho, foi feita a análise acerca da bibliografia acadêmica recolhida de instituições de ensino superior creditadas, por meio de uma pesquisa exploratória. Comparando assim os posicionamentos de diversos autores, visando uma monografia de conclusão de curso que vise revisar a bibliografia, esperando assim resultados qualitativos.

## AS GERAÇÕES DE LEIS DE PRIVACIDADE

Os avanços acerca das legislações de dados, quando olhamos em um aspecto global, passaram por um período de evolução conforme as tecnologias informacionais foram avançando ao longo do tempo. Podemos dizer, assim, que todas elas visam a melhora do ecossistema normativo de proteção por meio da ação dos reguladores legítimos visando a implementação de novos regramentos em determinados territórios nacionais. Considerando as quatro gerações de leis de privacidade (SEAF/PR), no caso do Brasil, quando abordamos a literatura recolhida é possível conferir que o mesmo não entrou na primeira geração das leis de proteção, ao exemplo da LGPD ter forte inspiração na GDPR. Como uma das primeiras iniciativas de proteção, podemos citar a Lei de Hesse, com esse nome devido ter sido uma legislação local Alemã. Sendo uma lei que visava combater eventuais abusos no armazenamento de dados, por exemplo.

*Germany has been and still is the forerunner on privacy and data protection law. In 1970, the German state of Hesse enacted the world's first Data Protection Act. The other states soon followed, and on 1 January 1978, the first German Federal Data Protection Act (BDSG) entered into force. (STEPANOVA, Olga. JECHEL Patricia)*

Um ponto curioso da importação de políticas públicas, é a atenção de outros governos quanto à eficiência, eficácia, e efetividade dos projetos de terceiros. Assim podemos dizer que, assim como a GDPR impactou a LGPD, a lei de Hesse também impactou o Ato Federal de Proteção de Dados Alemão, este último, considerado na literatura como uma lei de segunda geração, em uma situação que mesmo com a Alemanha dividida, pode se argumentar dizer que a primeira lei local impactou uma política pública mais abrangente. Como outros exemplos de primeira geração, temos a Lei Nacional de Proteção de Dados da Suécia de 1973 e em 1974 a Data Legend Privacy Act dos Estados Unidos, como exemplos de outras ações regulatórias que

muito impactaram a literatura. Por exemplo, trazendo primeiramente o exemplo da lei Sueca:

*“The first national legislation aimed at protecting the informational privacy of individuals when their personal data are processed in computers saw the light of day in Sweden in 1973. The Swedish 1973 Data Act only covered processing of personal data in traditional, computerised registers.”* (ÖMAN, Sören)

E posteriormente da lei Americana:

*The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.* (Privacy Act of 1974, USA-DOJ).

Assim, podemos perceber que as leis de primeira geração eram muito atreladas inicialmente a concepções tecnológicas da época. Em que uma rede maior de computadores conectados em nuvem de dados era muito distante da tecnologia do tempo. Então, é possível argumentar que o ambiente legal de formulação das leis de proteção de dados da década de 1970 em muito se baseava, na visão em registros descentralizados e desconectados de uma rede central.

Como exemplo de leis de segunda geração, temos como exemplo: A já mencionada Lei Alemã de Proteção de Dados de 1978 - “*Bundesdatenschutzgesetz” (BDSG)*; a

Lei Francesa de Proteção de Dados Pessoais de 1978 - “*Informatique et Libertés*” e também a Lei austríaca de 1978 - “*Datenschutzgesetz” (DSG)*.

No caso da Lei Alemã de 1978, também chamada de “BDSG”, de forma similar em diversas legislações de proteção de dados, a ação regulatória visava a proteção do titular, em uma época que as entidades privadas e organizações públicas visavam aumentar a eficiência de suas operações por meio do uso dos dados e também a vontade do governo de não depender somente de valores constitucionais principiológicos quanto ao arcabouço normativo, retirando assim certa subjetividade do devido processo legal. Porém, de forma curiosa, a própria BDSG foi criticada posteriormente como não tendo a devida precisão necessária, assim trazendo à luz a dificuldade que é legislar acerca de dados pessoais, já que os impactos de tais normas, podem impactar a economia e também a sociedade como um todo.

*“The possibility that government or business can gather information on every citizen may, therefore, pose a danger to individual freedom. 12 The German Federal Data Protection Act of 1977 (BDSG)13 represents an attempt by the Legislature of West Germany to deal with that danger” (RICCARDI, J Lee)*

Quanto a Lei Francesa de Proteção de Dados Pessoais de 1978 - “*Informatique et Libertés*”, pode se argumentar que a mesma dispõe a tecnologia da informação a serviço do titular, assim trazendo ao debate garantias como por exemplo a não violação da identidade humana, a não violação de direitos humanos, o respeito à privacidade, e também o respeito às liberdades públicas e privadas. Abordando o tratamento de arquivos pessoais, e diferenciando-o do tratamento de dados não pessoais, sendo possível a verificação da mesma abordagem na Lei Geral de Proteção de Dados brasileira.

*“Article 2 This Act shall apply to automatic processing of personal data as well as non- automatic processing of personal data that is or may be contained in a personal data filing system, with the exception of processing carried out for the exercise of exclusively private activities,(...)”* (Agência dos Direitos Fundamentais da União Europeia)

Trazendo outro exemplo, um aspecto curioso do caso austríaco da DSG, é que o processo de implementação se deu ao longo dos anos, se utilizando de artifícios legais como decretos para complementar DSG. Assim neste processo, envolvendo diversos stakeholders legais, ao exemplo cronologicamente posterior da Comissão de Controle de Dados. A mesma, que se por um lado ampliava o controle estatal cadastrando os controladores, aumentava a informalidade, por ter um processo demasiadamente burocrático aos olhos dos indivíduos da sociedade civil, ao exemplo do processo legal para a instalação de sistemas de câmeras de segurança por indivíduos privados anteriormente a 2009.

*“In Austrian law, all important data protection p rinciples are written down in the Data Protection Act (current version: Datenschutzgesetz*

*– DSG 2000) since the first act on data protection was introduced in 1978.Alongside this, there are several other regulatory parts and pieces that fill in gaps, define exceptions or regulate certain issues in more detail.”* (KRIEGER-LAMINA, Jaro. BIRNGRUBER, Stefan)

Já como exemplo de uma legislação de proteção amplamente classificada como uma norma de terceira geração, podemos trazer o exemplo alemão da “Lei do Recenseamento de População, Profissão, Moradia e Trabalho” de 1983, também conhecida como “Lei do Censo”, e esta por sua vez, era ordinariamente impugnada por grupos da sociedade civil contrários à ampla coleta de dados pessoais de

indivíduos. Sob o julgamento da Corte Constitucional Alemã, foi considerada a inconstitucionalidade parcial da lei, pois a mesma, na visão da corte, deveria tratar os dados pessoais dos indivíduos com mais transparência. Assim firmando o direito à "autodeterminação informativa”, desta forma, por via do tribunal constitucional, o tratamento não transparente começa a violar claramente o direito à dignidade da pessoa humana e também o direito ao desenvolvimento da personalidade. Sendo possível traçar um paralelo com a LGPD, quanto ao importância dos princípios legais. Por meio do supracitado, neste caso, também buscava-se garantir que o indivíduo tenha controle das próprias informações, garantindo o direito de proteção ao titular quanto ao domínio de seus dados privados. Quanto às leis da quarta geração, pode se dar o exemplo da própria GDPR, que visou o melhoramento dos processos regulatórios e também buscou empoderar o indivíduo.

## DESENVOLVIMENTO

Vivemos em um mundo em transformação quando pensamos sobre o desenvolvimento das leis que envolvem o tratamento de dados. Por exemplo a General Data Protection Regulation, esta regulação europeia de número 2016/679 de 27/04/2016 em muito se assemelha com a Lei Geral de Proteção de Dados brasileira, esta última de número 13.709, de 14/08/2018. Assim é possível reconhecer como existentes, nas duas leis, semelhanças e diferenças.

Em ambos os casos, as Leis citadas são regramentos jurídicos que visam estabelecer uma norma acerca do direito de proteção de dados de um titular, natural e não jurídico, em que a base principiológica é a noção de privacidade estabelecida. Então podemos dizer, que tais leis visam fortalecer o direito à privacidade fundamental que o cidadão tem, em ambos os casos, já que os mesmos visam a proteção de dados pessoais, tanto no judiciário europeu como no brasileiro.

Também devemos considerar, que alguns conceitos que influenciaram a GDPR, ao exemplo dos conceitos de dignidade, solidariedade, igualdade e liberdade; já encontrava respaldo jurídico na Carta de Direitos Fundamentais da União Europeia. Então podemos dizer, que certos aspectos da GDPR não são novos, desta forma já existindo anteriormente a aprovação da lei, e que a ideia de proteção de direitos pessoais de pessoas naturais já existia anteriormente. É positiva a comparação das duas leis semelhantes, pois como já dito, ambas visam resguardar os dados pessoais dos indivíduos titulares, a luz de que os direitos que envolvem o mundo digital estão em constante desenvolvimento e caminham para se tornarem direitos amplamente estabelecidos.

Se por um lado os princípios da GDPR são: Licitude , lealdade, transparência, limitação de finalidade, minimização dos dados, limitação de armazenamento, exatidão, integridade e confidencialidade. Por outro lado, os princípios da LGPD, esta última fortemente inspirada na GDPR são: Finalidade, adequação, necessidade, livre acesso, qualidade dos dados, trasparencia, segurança,

não discriminação, prevenção, responsibilização e prestação de contas. Como podemos ver, a GDPR em muito se assemelha a LGPD na questão dos princípios legais que sustentam a lei, inclusive no ponto que permite, em ambas as leis, a exclusão de dados armazenados por solicitação do usuário titular, ressalvando as exceções previstas nas legislações. Dentre elas: Quando o tratamento de dados pessoais é feito para fins de pesquisa, jornalísticos, acadêmicos ou para cumprir obrigações legais. Trazendo o exemplo dos princípios da GDPR:

*“1-O princípios da legalidade, imparcialidade e transparência exige que os dados pessoais sejam tratados de forma legal, justa e transparente em relação aos titulares dos dados. Requer que todas as informações e a comunicação sobre o processamento dos dados pessoais sejam de fácil entendimento e use uma linguagem clara e precisa. Este princípio garante que os titulares dos dados recebam informações sobre a identidade dos responsáveis pelo processamento e os objetivos do processamento dos dados pessoais. 2-O princípio da limitação da finalidade implica no processamento dos dados pessoais coletados apenas para propósitos específicos, explícitos e legítimos, não sendo permitido processá-los de maneira que não seja compatível com tais finalidades. 3-O princípio da minimização de dados afirma que os dados pessoais devem ser limitados às informações necessárias aos fins para os quais são processados. 4-O princípio da precisão refere- se à necessidade de garantir que os dados pessoais sejam exatos e que sejam mantidos atualizados. Dados pessoais imprecisos devem ser excluídos ou retificados. 5-O princípio da limitação de armazenamento determina que os dados pessoais devem ser mantidos somente pelo tempo necessário aos propósitos do processamento. O armazenamento desses dados por períodos mais longos será permitido quando o processamento dos dados tiver finalidades de interesse público, pesquisa científica, histórica ou fins estatísticos. Devendo-se, também nestes casos, salvaguardar os direitos dos titulares dos dados. 6-O princípio da integridade e confidencialidade exige que o tratamento de dados pessoais seja feito de maneira segura. Os dados devem ser protegidos contra destruição e danos não autorizados ou ilegais. Medidas técnicas ou organizacionais adequadas devem ser tomadas para atender a este requisito, como por exemplo o uso de criptografia, bem como o uso de mecanismos de autenticação e autorização. Além dos princípios de proteção de dados citados, o*

*GDPR introduz no artigo 5 (2) o princípio da responsabilização.”* (AZEVEDO, Adriana.

Princípios de proteção de dados de acordo com o GDPR)

De modo comparativo, também podemos dizer, que quanto ao acesso à informação, ambas as leis dão muita importância ao princípio da transparência, já que ambas as normas responsabilizam o controlador quanto ao dever de informar, da melhor maneira possível, o titular dos dados acerca do tratamento de informações pessoais. O usuário, nas duas leis, pode se opor ao tratamento de seus dados pessoais, e também tem o direito à portabilidade de seus dados, levando em consideração as limitações tecnológicas.

Quanto ao alcance extraterritorial, podemos dizer que tanto a LGPD quanto a GDPR o possuem. A GDPR no entanto, muito por conta da influência da União Europeia , acaba por ser mais conhecida internacionalmente que a LGPD. Porém se uma empresa prestar serviços tanto na União Européia como no Brasil, a mesma deve estar atenta a ambas as legislações. E avaliando em uma ótica de administração empresarial, é mais fácil para as empresas adotarem regulações internas que respeitem o máximo de leis internacionais possíveis ao mesmo tempo, considerando que seria muito difícil adaptar determinada empresa multinacional a funcionar de maneiras diferentes prestando serviços em diversos países.

Podemos dizer, que, seguindo como inspiração a GDPR, a LGPD brasileira visa proteger o direito à privacidade dos titulares. Mesmo que alguns direitos defendidos na LGPD já assegurados pela constituição de 1988, a lei veio como uma forma de assegurar tais direitos constitucionais de uma forma mais clara. Visando que as instituições se adaptem de uma maneira mais uniforme ao tratamento de dados pessoais, estes muito importantes nos dias de hoje, em que a tecnologia se rapidamente desenvolve e que computadores podem entender padrões que as pessoas não conseguem identificar. A LGPD foi sancionada no dia 14 de agosto de 2018, pelo então presidente da República Federativa do Brasil Michel Temer e a atenção às normas legais de tratamentos de dados se tornam muito importantes para as organizações afetadas, já que a desobediência à lei, pode levar a empresa a ser

considerada como infratora das normas legais vigentes, sendo passível a punição descrita em lei.

*“Dentre as sanções administrativas previstas na LGPD para o caso de violação das regras previstas, destacam-se a advertência, com possibilidade de medidas corretivas; a multa de até 2% do faturamento, com limite de até R$ 50 milhões; o bloqueio ou a eliminação dos dados pessoais relacionados à irregularidade, a suspensão parcial do funcionamento do banco de dados ou a proibição parcial ou total da atividade*

*de tratamento.” (Fonte: Agência Senado)*

Devemos pontuar também na LGPD, que no caso da iniciativa privada, a empresa em questão é responsável por nomear um controlador/operador, o qual terá a desafiadora tarefa de gerenciar o tratamento de dados pessoais de uma determinada organização. Com a evolução da tecnologia, verificamos que o mercado de trabalho se transforma a cada dia, e a figura do chamado *Data Protection Officer*, ou oficial de proteção de dados em português, se torna cada vez mais importante nas organizações. Desta maneira, as atividades relacionadas aos bancos de dados se tornam cada vez mais relevantes para o sucesso de determinada organização. Em um ambiente global de insegurança no mundo digital, os computadores da atualidade, são capazes de reconhecer padrões de forma muito mais rápida que um ser humano, mesmo os mesmos possuam uma taxa de erro na maioria dos casos.

Após a GDPR de 2016, a LGPD de 2018 vem com o intuito de reforçar o conceito de privacidade do usuário em território brasileiro. Visando estabelecer normas acerca do tratamento de dados nos meios digitais, envolvendo pessoas naturais, e jurídicas do direito público ou privado. Em certos aspectos a LGPD visa empoderar o cidadão, já que a mesma dá poder sobre o mesmo de saber como seus dados são coletados,

armazenados e processados. Assim protegendo os direitos fundamentais da privacidade e liberdade dos cidadãos brasileiros. O aparecimento de leis específicas que regulamentam o tratamento de dados em sociedades digitais é um fenômeno relativamente recente, mesmo que, anteriormente às leis impostas, os princípios legais que as leis de dados se baseiam já existiam. Considerando a importância das informações na atualidade, as mesmas podem ser consideradas como de alto valor no meio empresarial, também entendendo que informações podem ser vendidas, fica evidente a necessidade de criação de normas que estruturam estas relações entre os indivíduos nesse campo.

Na LGPD, podemos entender como tratamento, toda e qualquer operação realizada com dados pessoais, ao exemplo da coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração. Então podemos dizer que a lei tem amplo impacto.

Com o passar do tempo, o campo da administração dos bancos de dados evolui constantemente, trazendo mais responsabilidades aos operadores e controladores dos dados. Considerando que é possível, fazer análises complexas e até predições para as decisões de uma determinada organização, esse campo se demonstra como central na revolução informacional que vivemos. Então, a GDPR e a LGPD vêm para padronizar os tratamentos acerca das informações. Quando os titulares depositam confiança nas instituições, os mesmos têm o direito de serem respeitados à luz da lei, esta que consolida as garantias cidadãs.

Se certo indivíduo não tem nenhum controle sobre suas informações pessoais, o mesmo pode ser prejudicado, entendendo que, organizações privadas visam o lucro e que a venda de informações pode ser um negócio lucrativo para uma determinada entidade. Então, as leis de proteção de dados servem de certa forma para regulamentar como se dá o tratamento da informação. Tais leis de proteção, não são de hoje, mas sim foram construídas ao longo do tempo, se adaptando a mudanças e

avanços tecnológicos e visando a harmonização com princípios e direitos constitucionais já existentes.

Podemos argumentar que a LGPD surgiu com forte inspiração na GDPR, e a lei brasileira veio com a finalidade de atualizar as normas vigentes visando a proteção do titular. Com a evolução tecnológica, algumas leis rapidamente se tornam ultrapassadas, devendo o poder público atualizar tais normas para defender os valores constitucionais e defender os direitos dos cidadãos. Devemos pontuar, que tal fenômeno de formulação de propostas legislativas não é exclusivo ao território nacional brasileiro ou europeu, e sim uma ocorrência mundial que acontece ao longo do tempo em diversos países do mundo, entendendo que muitas vezes, empresas atuam em diversos países, e estas devem se adequar aos mercados que atuam.

*“A Lei Geral de Proteção de Dados Pessoais do Brasil, ou LGPD, traz uma necessária classificação ao arcabouço legal brasileiro. A LGPD tenta unificar os mais de 40 diferentes estatutos que atualmente governam os dados pessoais, online e offline, substituindo certas regulações e suplementando outras. Esta unificação de regulamentos, publicados anteriormente e frequentemente díspares e contraditórios, é somente uma das similaridades que compartilha com o Regulamento Geral sobre a Proteção de Dados (GDPR, sigla do nome em inglês) da União Europeia, um documento do qual claramente tira inspiração.”*

*(KOCH, Richie)*

Considerando que os dados são importantíssimos no novo momento de digitalização que vivemos, a regulação por parte dos governos se faz necessária para proteger os titulares. Mecanismos de regulação evoluem, conforme o ambiente muda, e no caso dos bancos de dados, tal ambiente é muito dinâmico. Se avaliarmos comparativamente, podemos perceber que a LGPD traz consigo um conteúdo

menos específico no geral que a GDPR, trazendo uma maior possibilidade de interpretação de normas em alguns aspectos. Porém, ambas as leis visam a transparência como destino fundamental das regulações, impactando as empresas da iniciativa privada a serem transparentes quanto ao uso dos dados que as mesmas coletam. A luz da LGPD, o dado anonimizado não é considerado um dado pessoal, encorajando assim, que as informações sejam anonimizadas sempre que possível. Quando as empresas fazem análises de grandes bancos, incentiva-se que as mesmas trabalhem para que o indivíduo registrado não seja identificado, possibilitando a proteção do usuário ao mesmo tempo que as organizações consigam compreender as melhores decisões estratégicas para o negócio como um todo. A LGPD é muito importante, pois traz segurança jurídica aos envolvidos no processo de tratamento, clarificando assim as regras que devem ser seguidas pelos operadores e controladores dos bancos de dados.

Assim possibilitando a administração sustentável de tecnologias de “*big data*”, visando diminuir as incidências de fraude, inadimplência e golpes, por exemplo, e também melhorar a oferta de produtos e serviços. Melhorando a inteligência de negócios da iniciativa privada, de uma forma que o titular seja respeitado à luz da lei.

Se não há transparência quando uma grande empresa trabalha com uma vasta quantidade de dados, a segurança do titular não pode ser garantida, e em casos mais graves a própria segurança de grupos sociais vulneráveis. O conceito da privacidade desde a concepção, se torna muito importante no começo do século XXI no campo da engenharia de sistemas, já que as regulações de privacidade evoluem rapidamente. Se tal projeto de um sistema visa a privacidade desde sua concepção, eventos que ferem as leis de privacidade podem ser mais facilmente evitados.

Então, podemos dizer que a existência das normas de proteção visa harmonizar a relação entre titulares, controladores e operadores. A LGPD chega ao Brasil, para alinhar o país ao tema de proteção de dados que já era anteriormente debatido em outros países do mundo, desta forma possibilitando melhor alinhamento da nação com normas internacionais. Então considerando que a abrangência de algumas grandes organizações privadas é muito grande, podemos dizer que a LGPD visa facilitar a movimentação internacional de dados, sob a luz da estratégia

macroeconômica mundial da tentativa de entrada na Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

Devemos pontuar, que existem quatro grupos distintos e característicos de dados mencionados na LGPD: Dados pessoais, sendo os mesmos relativos a uma pessoa viva, identificável; os dados pessoais sensíveis, sobre crianças e adolescentes ou que possam ser usados para fins discriminatórios; os dados anonimizados, em que se perde a possibilidade de associação a um indivíduo; e finalmente os dados pseudoanonimizados, em que se perde a possibilidade de associação, mas o controlador pode reverter tal desassociação com dados adicionais. Assim a LGPD deixa fora de sua abrangência o dado anonimizado, já que perde a característica de dado pessoal de um titular. Os requisitos para o tratamento no caso da LGPD, exigem consentimento, e o cumprimento das obrigações legais por parte do controlador, valendo lembrar que em caso de vazamento de dados, o titular deve ser informado imediatamente.

Por outra forma, também é possível argumentar que o Brasil anteriormente possuía, o Marco Civil da Internet, que trazia consigo a defesa do princípio da proteção da privacidade e dos dados pessoais, assim sendo possível argumentar que a LGPD visa posteriormente delimitar de melhor forma o ambiente de normativo acerca da proteção de dados, trazendo uma melhor segurança jurídica.

*“A referida lei prevê como princípios que regulam o uso da internet no Brasil, enumerados no artigo 3º, dentre outros, o princípio da proteção da privacidade e dos dados pessoais, e asseguram, como direitos e garantias dos usuários de internet, no artigo 7º, a inviolabilidade e sigilo do fluxo de suas comunicações e inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial. O artigo 10º, § 1º, que trata de forma específica da proteção aos registros, dados pessoais e comunicações privadas, é bem claro quanto à possibilidade de fornecimento de dados*

*privados, se forem requisitados por ordem de um juiz, e diz que o responsável pela guarda dos dados será obrigado a disponibilizá-los se houver requisição judicial. Caso o responsável se recuse a fornecer os dados solicitados pelo juiz, poderá responder pelo crime de desobediência, previsto no artigo 330 do Código Penal.”* (Tribunal de Justiça do Distrito Federal e dos Territórios)

Também relevante no campo das leis que regulam o ambiente digital temos a Lei de Acesso à Informação (LAI), que visa no setor público, garantir o acesso a dados públicos por parte do indivíduo, assim respeitando o princípio de transparência estabelecido por lei. Possibilitando desta maneira uma melhor participação cidadã nos assuntos públicos, ao exemplo especial das finanças públicas já que governos trabalham com recursos escassos e devem administrar da melhor forma possível o dinheiro público. Sendo fundamental na ideia de um governo aberto, a transparência, a imputabilidade e a participação social. A formação da Parceria para Governo Aberto ou OGP (do inglês Open Government Partnership) vem para fomentar mais ainda o debate de transparência, e consequentemente o aumento da pressão na formulação de políticas públicas do campo.

*“In 2011, government leaders and civil society advocates came together to create a unique partnership—one that combines these powerful forces to promote transparent, participatory, inclusive and accountable governance. The Open Government Partnership (OGP) includes 77 countries and 106 local governments – representing more than two billion people – and thousands of civil society organizations.” (Open Government Partnership)*

# Desta forma, se pontua que a LGPD vem para alterar o Marco Civil da internet, acerca do tratamento de dados em meios físicos ou digitais, por

pessoa jurídica ou natural, visando a proteção de direitos estabelecidos pelos titulares, ao exemplo do direito à liberdade e o do direito à privacidade e também do livre desenvolvimento da pessoa natural. Assim de outra forma se verifica quão ampla é a lei, envolvendo diretamente o setor privado e também o setor público. Podemos trazer como exemplo de instituições afetadas, as Cortes de Contas, Sociedades de Economia Mista, Empresas Públicas, Autarquias, Fundações, Judiciário e Ministério Público.

# Alguns princípios da GDPR são comparáveis aos princípios da LGPD, fato este que fortalece ainda mais a relação entre as duas propostas legislativas. Por exemplo, o princípio de Licitude, lealdade e transparência da GDPR em muito se assemelha ao princípio de livre acesso e transparência da LGPD e tal padrão continua, com limitação de finalidade versus Finalidade e adequação, precisão versus qualidade dos dados, minimização dos dados versus necessidade, responsabilidade versus responsabilidade e prestação de contas, integridade e confidencialidade versus segurança e prevenção, respectivamente. Sendo o princípio da não discriminação uma divergência da LGPD quanto a GDPR.

*“Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:(...) §16. Os órgãos e entidades da administração pública, individual ou conjuntamente, devem realizar avaliação das políticas públicas, inclusive com divulgação do objeto a ser avaliado e dos resultados alcançados, na forma da lei.”* (Constituição da República Federativa do Brasil, Art. 37, via Jusbrasil).

# Considerando a importância dos princípios constitucionais de impessoalidade, legalidade e moralidade, publicidade e eficiência descritos no Art. 37; a LGPD vem para reforçar e delimitar o campo das políticas públicas de proteção de dados, dando grande importância ao tratamento à luz destes princípios legais no caso do funcionamento informacional do setor público. E tais valores somados ao artigo 6º da LGPD reforçam ainda mais a responsabilidade do setor público quanto ao manejo de dados, servindo como garantia da defesa de dados pessoais.

*“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*.*”* (Art 6º LGPD, via Jusbrasil)

Conforme o supracitado, é possível dizer que de acordo com o princípio da finalidade exposto, não é possível tratar dados pessoais a fim de um motivo indeterminado. Então, sendo preciso, informar o titular quanto o que será feito com os dados coletados do mesmo. Por exemplo, se o titular apresentar informações pessoais ao serviço de coleta, as mesmas serão protegidas à luz do princípio de finalidade, que visa assegurar fins específicos, informados ao titular e explícitos, não existindo a possibilidade de tratamento posterior sem que o titular seja informado.

Da mesma forma, não é possível que a finalidade seja alterada ao longo do processo sendo o princípio da finalidade relacionado aos princípios de moralidade e legalidade.

De modo comparativo, os princípios da limitação de finalidade e também da minimização dos dados da GDPR em muito se assemelha ao princípio da finalidade da LGPD, mostrando que ambas as legislações adotaram uma postura semelhante quanto a necessidade de uma finalidade específica quanto ao tratamento de dados. Vale ressaltar, que o princípio de minimização dos dados europeu também é diretamente passível de comparação com o princípio de necessidade da LGPD

brasileira, assim em ambos os casos não violando a ideia que as organizações afetadas devem usar a atividade de coleta de maneira não excessiva, usando do mínimo de informações possíveis para atingir a finalidade proposta.

*“Uma empresa-organização não pode simplesmente recolher dados pessoais para fins indefinidos («limitação das finalidades»); (...) a empresa/organização deve recolher e tratar apenas os dados pessoais necessários para cumprir essa finalidade («minimização dos dados»);”* (Comissão Europeia)

# Quanto ao exemplo do princípio de adequação, o mesmo se assemelha aos princípios de legalidade e eficiência, ou seja, fazer da melhor forma e à luz da lei. Assim devendo a organização buscar ativamente a melhoria de processos institucionais, verificando o amplo respeito à lei e os princípios constitucionais. Por exemplo, o princípio do livre acesso da lei brasileira de proteção garante aos titulares, que tenham acesso, de forma gratuita e facilitada, a todos seus dados pessoais, durante toda a duração do tratamento.

Desta maneira é possível verificar que o princípio da licitude, lealdade e transparência da GDPR também é passível de comparação direta com o princípio brasileiro do livre acesso, já que no caso europeu, a norma visa o tratamento de forma lícita e transparente, garantindo a lealdade para com o tratamento com finalidade clara exposto anteriormente. O princípio da qualidade dos dados, na lei de proteção de dados brasileira, traz a garantia aos titulares, quanto à relevância, clareza e exatidão dos dados, sendo também próximo ao princípio de eficiência.

# Por outro lado, na GDPR, o princípio de precisão visa que dados pessoais precisos sejam mantidos, incentivando que dados desatualizados ou sem confiabilidade sejam excluídos do processo de tratamento. Então, somando os princípios citados, ambas as leis visam a garantia de informações claras aos titulares, não permitindo o livre compartilhamento de informações pessoais de forma oculta, sendo no caso da LGPD, um aspecto próximo ao princípio da publicidade. Também, o princípio de prevenção da lei brasileira, visa a proteção de dados pessoais, afirmando que se devem adotar medidas para prevenir danos a dados pessoais. E de outro lado a GDPR, por meio do princípio da integridade e confidencialidade, também visa proteger os bancos de dados contra destruição e ataques ilegais, sendo a pauta da segurança digital muito importante para o debate tecnológico do século XXI. Sendo este um problema que as empresas devem visar combater.

De acordo com o supracitado verificamos, que o princípio brasileiro da responsabilidade ou da prevenção de contas visa que o agente apresente medidas concretas e com eficácia, garantido o cumprimento e observância das normas vigentes. E por outro lado a GDPR, por meio do princípio da responsabilização, visa também a demonstração de conformidade às normas. Único ao caso da LGPD, temos o princípio da não discriminação, que proteja o titular quanto a ações com fins discriminatórios, abusivos ou ilícitos.

*“Entender o direito como parte da dimensão institucional de políticas públicas é supor que normas jurídicas estruturam seu funcionamento, regulam seus procedimentos e se encarregam de viabilizar a articulação entre atores direta e indiretamente ligados a tais políticas.”* (COUTINHO, Diogo Rosenthal)

# Desta maneira, a LGPD defende a responsividade do agente público, respeitando os direitos fundamentais, enquanto o gestor público é submetido aos controles efetivos e legais das políticas públicas por meio do devido funcionamento dos poderes constitucionais sob a luz da legalidade administrativa.

# Então podemos afirmar que a LGPD brasileira está amplamente relacionada aos princípios administrativos da moralidade, impessoalidade, legalidade, publicidade e eficácia. Colocando assim os controladores em uma situação de elevada responsabilidade, em que a ênfase se dá no titular. Por meio do ciclo constante de políticas públicas, as políticas se aprimoram mediante análise e diagnóstico ao longo do tempo, assim sendo possível a avaliação de desempenho e resultados reforçando as políticas de proteção em um ciclo eficiente e contínuo.

## CONSIDERAÇÕES FINAIS

Em conclusão, verificamos, que as organizações devem estar preparadas e atentas as mudanças regulatórias e que a pauta de proteção de dados seguem em amplo debate nas estruturas legislativas ao longo do tempo. Então é possivel pontuar, que as organizações modernas devem levar a ideia da privacidade desde a concepção de uma maneira séria, já que tal estratégia, pode evitar problemas ao longo do tempo e garantir o respeito as normas legais vigentes.

A observação não só das normas como também dos principios constitucionais locais por parte das organizações, se torna vital para o processo de relação institucional das empresas, levando em conta que o direito e a análise de dados estão se consolidando no campo de banco de dados, e o mesmo está um ambiente intersetorial. Assim, se tornam mais valorosos os sistemas de implementação contínua, em que um sistema não é abandonado após o lançamento e sim o mesmo continua a ser melhorado ao longo do tempo por uma equipe dedicada.

Desta forma, tanto no setor público quanto no privado o campo de banco de dados envolve cada vez o ambiente legislativo e o direito, assim colocando pressão nas organizações para que as mesmas se adéquem as novas leis, exigindo por muitas vezes a criação de novos planos e mecanismos para evitar as punições previstas em lei. Tais novas propostas, devem impulsionar o gerenciamento legitimo de informações, a fim de garantir resultados valiosos por meio da inteligencia de negócios.

Explicita-se então, por meio do presente texto, a importância da colaboração interdisciplinar entre diversas áreas de atuação como forma de garantir a proteção do titular sem causar danos a inovação. Assim devendo ser estabelecidas, métricas de implementação para o acompanhamento da adesão as normas legais estabelecidas. Visando a atenção aos principios legais locais

e também a outras normas especificas, como forma de garantir o sucesso institucional em determinada organização publica ou privada.

Então levar em consideração a territoriedade de que um sistema está sendo implantado se torna muito importante para o desenvolvimento do projeto e valores como moralidade, licitude e transparência tomam papel central no debate legislativo acerca da formulação das políticas públicas de proteção de dados. Assim os operadores possuidores de dados pessoais, podem e devem tentar evitar irregularidades, como forma de evitar ataques e garantir a proteção de grupos vulneráveis contra vazamento de informações discriminatórias.

## REFERÊNCIAS

LORENZON, Laila Neves. **ANÁLISE COMPARADA ENTRE REGULAMENTAÇÕES DE DADOS PESSOAIS NO BRASIL E NA UNIÃO EUROPEIA (LGPD E GDPR) E SEUS RESPECTIVOS INSTRUMENTOS DE**

**ENFORCEMENT**. (Centro de Tecnologia e Sociedade (CTS) FGV - Direito Rio)

NUNES, Amanda, NASCIMENTO Gabriel. **AS SANÇÕES E PENALIDADES DO DESCUMPRIMENTO DA LGPD QUAL O SEU IMPACTO NAS EMPRESAS PRIVADAS**. (Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente).

NEVES, Rebeca**. GDPR e LGPD: Estudo comparativo**. (Centro Universitário de Brasília - UniCEUB)

CASTRO, Andrés. **Impacto del alcance extraterritorial del GDPR en materia de protección de datos en Colombia, su concordancia con el régimen nacional y el estado actual del debate.**(Biblioteca Digital de Bogotá)

PINHEIRO, Patrícia **NOVA LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E O IMPACTO NAS INSTITUIÇÕES PÚBLICAS E PRIVADAS** (Revista dos Tribunais)

SILVA, Jacqueline Maria Cavalcante da. Revista da Faculdade de Direito da UFG: **POLÍTICAS PÚBLICAS COMO INSTRUMENTO DE INCLUSÃO SOCIAL.**

<https://revistas.ufg.br/revfd/article/view/15589>.

Acesso: 17/01/2023

GOUVEIA, Luis Borges; RANITO, **João. Sistemas de Informação de Apoio à Decisão (2004)**. Publisher: Principia.

Punições pelo uso indevido de dados pessoais começam a valer no domingo. Agência Senado.

[https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-](https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo#%3A~%3Atext%3DDentre%20as%20san%C3%A7%C3%B5es%20administrativas%20previstas%2Cpessoais%20relacionados%20%C3%A0%20irregularidade%2C%20a) [de-dados-pessoais-comecam-a-valer-no-](https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo#%3A~%3Atext%3DDentre%20as%20san%C3%A7%C3%B5es%20administrativas%20previstas%2Cpessoais%20relacionados%20%C3%A0%20irregularidade%2C%20a) [domingo#:~:text=Dentre%20as%20san%C3%A7%C3%B5es%20administrativas%20previstas,pessoais%20relacionados%20%C3%A0%20irregularidade%2C%20a](https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo#%3A~%3Atext%3DDentre%20as%20san%C3%A7%C3%B5es%20administrativas%20previstas%2Cpessoais%20relacionados%20%C3%A0%20irregularidade%2C%20a)

Acesso: 17/01/2023

KOCH, Richie. Artigo: **LGPD: a versão brasileira do regulamento europeu**

<https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais>

Acesso: 17/01/2023

FOUILLEUX, Eve. **Analisar a mudança: políticas públicas e debates num sistema em diferentes níveis de governança**

<https://revistaesa.com/ojs/index.php/esa/article/view/337>

Acesso: 17/01/2023

Constituição Federal -

<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html>

Acesso: 17/01/2023

LGPD: **Como coordenar a atuação do município para a governança de dados aplicada Secretaria Especial de Assuntos Federativos - SEAF/PR (Enap)**

<https://www.escolavirtual.gov.br/curso/491>

Acesso: 17/01/2023

The Privacy, **Data Protection and Cybersecurity Law Review: Germany** - Olga Stepanova and Patricia Jechel WINHELLER Attorneys at Law & Tax Advisors 27 October 2022

[https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-](https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany) [review/germany](https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany)

Acesso: 17/01/2023

Stockholm Institute for Scandianvian Law 1957-2010 - ÖMAN, Sören.- **Implementing Data Protection in Law.**

<https://scandinavianlaw.se/pdf/47-18.pdf>

Acesso: 17/01/2023

**Privacy Act of 1974**. Office of Privacy and Civil Liberties, Departamento de Justiça dos Estados Unidos.

<https://www.justice.gov/opcl/privacy-act-1974>

Acesso: 17/01/2023

RICCARDI J. Lee**. The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?.** LIRA (the Legal Institutional Repository and Archives) Boston College Law School.

<https://core.ac.uk/download/pdf/80399406.pdf>

Acesso: 17/01/2023

Agência dos Direitos Fundamentais da União Europeia. **Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties**. [https://fra.europa.eu/en/law-reference/act-ndeg78-17-6-january-1978-data-](https://fra.europa.eu/en/law-reference/act-ndeg78-17-6-january-1978-data-processing-data-files-and-individual-liberties) [processing-data-files-and-individual-liberties](https://fra.europa.eu/en/law-reference/act-ndeg78-17-6-january-1978-data-processing-data-files-and-individual-liberties)

Acesso: 17/01/2023

KRIEGER-LAMINA, Jaro. BIRNGRUBER, Stefan. **Exercising Democratic Rights under Surveillance Regimes** - AUSTRIA COUNTRY REPORTS [https://www.researchgate.net/publication/264220555\_Exercising\_Democratic\_Rights\_u](https://www.researchgate.net/publication/264220555_Exercising_Democratic_Rights_under_Surveillance_Regimes_-_AUSTRIA_COUNTRY_REPORTS) [nder\_Surveillance\_Regimes\_-\_AUSTRIA\_COUNTRY\_REPORTS](https://www.researchgate.net/publication/264220555_Exercising_Democratic_Rights_under_Surveillance_Regimes_-_AUSTRIA_COUNTRY_REPORTS)

Acesso: 17/01/2023

Tribunal de Justiça do Distrito Federal e dos Territórios. **Marco Civil da Internet.** [https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-](https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#%3A~%3Atext%3DO%20Marco%20Civil%20da%20Internet%2Cda%20internet%20no%20Brasil%E2%80%A6) [facil/edicao-semanal/marco-civil-da-](https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#%3A~%3Atext%3DO%20Marco%20Civil%20da%20Internet%2Cda%20internet%20no%20Brasil%E2%80%A6) [internet#:~:text=O%20Marco%20Civil%20da%20Internet,da%20internet%20no%20Br](https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#%3A~%3Atext%3DO%20Marco%20Civil%20da%20Internet%2Cda%20internet%20no%20Brasil%E2%80%A6) [asil…](https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/marco-civil-da-internet#%3A~%3Atext%3DO%20Marco%20Civil%20da%20Internet%2Cda%20internet%20no%20Brasil%E2%80%A6)

Acesso: 17/01/2023

Open Government Partnership.

<https://www.opengovpartnership.org/about/>

Acesso: 17/01/2023

**Constituição da República Federativa do Brasil, Art. 37, via Jusbrasil.** [https://www.jusbrasil.com.br/topicos/2186546/artigo-37-da-](https://www.jusbrasil.com.br/topicos/2186546/artigo-37-da-constituicao-federal-de-1988) [constituicao-federal-de-1988](https://www.jusbrasil.com.br/topicos/2186546/artigo-37-da-constituicao-federal-de-1988)

Acesso: 17/01/2023

Site Oficial: Comissão Europeia.

[https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_pt#%3A~%3Atext%3DUma%20empresa%2Dorganiza%C3%A7%C3%A3o%20n%C3%A3o%20pode%2C(%C2%ABminimiza%C3%A7%C3%A3o%20dos%20dados%C2%BB)%3B) [organisations/principles-gdpr/what-data-can-we-process-and-under-which-](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_pt#%3A~%3Atext%3DUma%20empresa%2Dorganiza%C3%A7%C3%A3o%20n%C3%A3o%20pode%2C(%C2%ABminimiza%C3%A7%C3%A3o%20dos%20dados%C2%BB)%3B) [conditions\_pt#:~:text=Uma%20empresa%2Dorganiza%C3%A7%C3%A3o%20n%C3](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_pt#%3A~%3Atext%3DUma%20empresa%2Dorganiza%C3%A7%C3%A3o%20n%C3%A3o%20pode%2C(%C2%ABminimiza%C3%A7%C3%A3o%20dos%20dados%C2%BB)%3B)

[%A3o%20pode,(%C2%ABminimiza%C3%A7%C3%A3o%20dos%20dados%C2%BB)](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_pt#%3A~%3Atext%3DUma%20empresa%2Dorganiza%C3%A7%C3%A3o%20n%C3%A3o%20pode%2C(%C2%ABminimiza%C3%A7%C3%A3o%20dos%20dados%C2%BB)%3B)

[%3B](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_pt#%3A~%3Atext%3DUma%20empresa%2Dorganiza%C3%A7%C3%A3o%20n%C3%A3o%20pode%2C(%C2%ABminimiza%C3%A7%C3%A3o%20dos%20dados%C2%BB)%3B)

Acesso: 17/01/2023

**REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF**

**THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC** (General Data Protection Regulation)

AZEVEDO, Adriana. Artigo: **Princípios de proteção de dados de acordo com o GDPR.** https:/[/www.l](http://www.linkedin.com/pulse/princ%C3%ADpios-de-)i[nkedin.com/pulse/princ%C3%ADpios-de-](http://www.linkedin.com/pulse/princ%C3%ADpios-de-) prote%C3%A7%C3%A3o-dados-acordo-com-o-gdpr-adriana-de- azevedo?trk=public\_profile\_article\_view

Acesso: 17/01/2023