

**FACULDADE DE DIREITO DE VITÓRIA  
CURSO DE BACHAREL EM DIREITO**

**DÉBORA MONTEIRO BARRETO CAMARGO VIEIRA**

**AS ESTRATÉGIAS DE COMUNICAÇÃO ORGANIZACIONAL APLICADAS ÀS  
EMPRESAS BRASILEIRAS SOB A ÓTICA DA CONFORMIDADE COM A LEI  
GERAL DE PROTEÇÃO DE DADOS**

**VITÓRIA  
2023**

DÉBORA MONTEIRO BARRETO CAMARGO VIEIRA

**AS ESTRATÉGIAS DE COMUNICAÇÃO ORGANIZACIONAL APLICADAS ÀS  
EMPRESAS BRASILEIRAS SOB A ÓTICA DA CONFORMIDADE COM A LEI  
GERAL DE PROTEÇÃO DE DADOS**

Monografia apresentada ao curso de Graduação em Direito da Faculdade de Direito de Vitória, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Gustavo Senna

VITÓRIA  
2023

DÉBORA MONTEIRO BARRETO CAMARGO VIEIRA

**AS ESTRATÉGIAS DE COMUNICAÇÃO ORGANIZACIONAL APLICADAS ÀS  
EMPRESAS BRASILEIRAS SOB A ÓTICA DA CONFORMIDADE COM A LEI  
GERAL DE PROTEÇÃO DE DADOS**

Monografia apresentada ao curso de Graduação em Direito da Faculdade de Direito de Vitória, como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovada em        de        de

COMISSÃO EXAMINADORA

À minha querida mãe, Fernanda, que com tanto carinho me orientou e cuidou de mim em todas as esferas da minha vida, inclusive a acadêmica, e que sempre foi minha maior inspiração e a pessoa mais extraordinária que eu conheço.

Ao meu amado esposo, Rafael, um verdadeiro príncipe encantado que me apoiou nos meus piores momentos, nas minhas crises mais intensas, e que foi tão zeloso com as minhas necessidades.

À minha irmã Mariana, ao meu pai João, às gargalhadas gostosas que compartilhamos e às orações uns pelos outros que jamais cessaram.

Vocês são a minha vida.

**DEDICATÓRIA**

## AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus, cuja graça e orientação sempre estiveram presentes em minha vida. Sua Palavra iluminou meu caminho e me deu forças para enfrentar os desafios acadêmicos que encontrei. Sem Sua orientação e Sua proteção, este trabalho não teria sido possível. Em meio a todo o caos que é a elaboração de uma monografia, um salmo consolou meu coração: “Lâmpada para os meus pés é tua palavra e luz, para o meu caminho.” (Salmos 119:105).

Agradeço à minha mãe querida, Fernanda, com quem tenho uma dívida eterna de gratidão que não pode ser medida em palavras. Desde o início da minha jornada acadêmica, ela foi minha orientadora, minha inspiração número um e maior incentivadora. Sua dedicação incansável e seu amor incondicional moldaram a pessoa que sou hoje, e este trabalho é um reflexo de nossa jornada compartilhada. Espero um dia me tornar pelo menos metade da mulher que minha mãe é.

Agradeço ao meu amado marido, Rafael, o principal pilar da minha vida. Há quem diga que nos casamos cedo demais, mas só eu e Deus sabemos o bem que ele me fez e o quanto ele foi e é essencial para mim. As massagens nos ombros, os beijos na testa e o café servido naquela xícara que encaixa na mão foram cruciais para que eu chegasse até aqui. Nos momentos de dúvida e de cansaço, ele me motivou a seguir em frente e a acreditar no meu potencial. Ele é a razão pela qual eu não joguei os livros pela janela e desisti de tudo.

À minha irmã caçula, Mariana, e ao meu pai, João, agradeço por estarem sempre ao meu lado. Suas orações, apoio inabalável e risadas compartilhadas trouxeram leveza a cada desafio e significado a cada conquista. Família é alicerce, suporte e colo, e eu sei que posso contar com a minha para o que der e vier.

Pela paciência e pela dedicação que lhe são habituais, agradeço ao meu admirado orientador, professor Gustavo Senna, que não se esquivou do árduo desafio de me guiar durante a confecção desta monografia.

Este Trabalho de Conclusão de Curso não é apenas o resultado do meu esforço, mas também do apoio de todas essas pessoas tão especiais em minha vida. Sou profundamente grata por cada um de vocês, e espero que este seja apenas o começo de nossa jornada juntos.

Com amor e gratidão.



## RESUMO

A pesquisa investiga de que maneira as organizações concebem suas políticas de comunicação e como é feita a correlação dessas políticas à Lei Geral de Proteção de Dados (LGPD). Apresenta, como *locus*, três pontos centrais: a análise das diretrizes e regulamentos da LGPD; o estudo das práticas de comunicação organizacional ou empresarial; e a relação dessas práticas com a Lei Geral de Proteção de Dados. Diante disso, busca responder a seguinte questão: as políticas de comunicação organizacional, no contexto empresarial brasileiro, estão em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD)? Para tanto, dialoga com autores como José Orbilio de Abreu Souza (2019), Fabrício da Mota Alves e Ana Paula Canto Lima (2022), Bruno Ricardo Bioni (2021), Roberto Cezar Bitencourt (2012), Letícia Canut (2021), Manuel Castells (1999), T. A. M. Corazza (2022), Manuella Dantas Corrêa Lima e Maria Emilia de Oliveira Pereira (2015), Sérgio Cavalieri Filho (2020), Américo Bedê Freire Júnior (2014), Margarida Maria Krohling Kunsch (2010), Viviane Nóbrega Maldonado e Renato Opice Blum (2022), Marlene Marchiori (2011), Fábio Mattos (2023), L. S. Mendes e G. C. S. da Fonseca (2020), Nelson Camatta Moreira (2007), Marcelo Novelino (2012), I. Oliveira e Carine F. Paula (2007), Bruno Opice Blum (2021), A. Paulraj e I. J. Chen (2008), Flávia Piovesan (2012), P. R. A. de Azevedo e P. M. de C. Cabacinha (2021), Sá Martino e Salgueiro Marques (2023) e Deezt Stanley (2010). Justifica-se pela importância da proteção de dados pessoais, a relevância da conformidade das práticas de comunicação empresarial com a LGPD e o impacto prático da pesquisa. Trata-se de uma pesquisa teórico-descritiva, com foco na elucidação dos principais pontos de interesse que orbitam a temática da Lei Geral de Proteção de Dados, com base na leitura de fontes doutrinárias, periódicas e científicas, pois une informações de fontes diversas e propicia, na investigação, a abordagem de diferentes conceitos e proposições para o problema do tema pesquisado.

**Palavras-chave:** Direitos humanos fundamentais à intimidade e à vida privada. LGPD. Comunicação Organizacional. Consentimento.

## ABSTRACT

The research investigates how organizations design their communication policies and how these policies are correlated with the General Data Protection Law (LGPD). The locus of the research is three central points: the analysis of LGPD guidelines and regulations; the study of organizational or business communication practices; and the relationship of these practices with the General Data Protection Law. Therefore, it seeks to answer the following question: Are organizational communication policies, in the Brazilian business context, in compliance with the General Personal Data Protection Law (LGPD)? To this end, we dialogue with authors such as José Orbilio de Abreu Souza (2019), Fabrício da Mota Alves and Ana Paula Canto Lima (2022), Bruno Ricardo Bioni (2021), Roberto Cezar Bitencourt (2012), Letícia Canut (2021), Manuel Castells (1999), T. A. M. Corazza (2022), Manuella Dantas Corrêa Lima and Maria Emilia de Oliveira Pereira (2015), Sérgio Cavalieri Filho (2020), Américo Bedê Freire Júnior (2014), Margarida Maria

Krohling Kunsch (2010), Viviane Nóbrega Maldonado and Renato Opice Blum (2022), Marlene Marchiori (2011), Fábio Mattos (2023), L. S. Mendes and G. C. S. da Fonseca (2020), Nelson Camatta Moreira (2007), Marcelo Novelino (2012), I. Oliveira and Carine F. Paula (2007), Bruno Opice Blum (2021), A. Paulraj and I. J. Chen (2008), Flávia Piovesan (2012), P. R. A. de Azevedo and P. M. de C. Cabacinha (2021), Sá Martino and Salgueiro Marques (2023 ) and Deezt Stanley (2010). Carrying out the research is justified given the importance of protecting personal data, the relevance of compliance of business communication practices with the LGPD and the practical impact of the research. This is a theoretical-descriptive research, focusing on elucidating the main points of interest that surround the theme of the General Data Protection Law, based on the reading of doctrinal sources and scientific periodicals as it combines information from different sources and provides, in research, addressing different concepts and propositions for the problem of the researched topic.

**Keywords:** Fundamental human rights to intimacy and private life. LGPD. Organizational communication. Consent.

## SUMÁRIO

INTRODUÇÃO	10
1 DOS DIREITOS FUNDAMENTAIS À INTIMIDADE E À VIDA PRIVADA	11
1.1 DA (DESNECESSÁRIA) DISTINÇÃO ENTRE OS CONCEITOS DE INTIMIDADE E VIDA PRIVADA	12
2 DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)	13
2.1 DO HISTÓRICO DA LEGISLAÇÃO INTERNACIONAL SOBRE A PROTEÇÃO DE DADOS PESSOAIS	15
2.2 DAS DIRETRIZES E REGULAMENTOS DA LGPD	17
3 DA COMUNICAÇÃO ORGANIZACIONAL OU EMPRESARIAL	26
3.1 DO BREVE HISTÓRICO DA COMUNICAÇÃO ORGANIZACIONAL	27
3.2 DAS ESPÉCIES DE COMUNICAÇÃO EMPRESARIAL: INTERNA OU INTRAORGANIZACIONAL	29
3.3 DAS ESPÉCIES DE COMUNICAÇÃO EMPRESARIAL: EXTERNA OU INTERORGANIZACIONAL	31
4 DOS LIMITES DO “CONSENTIMENTO”	33
5 DO ESTUDO DE CASOS	37
5.1 DA EMPRESA “ACESSO SOLUÇÕES DE PAGAMENTO” E DO CADASTRO DE CHAVES PIX	37
5.2 DA OPERAÇÃO DEEPWATER	38
5.3 DO VAZAMENTO DE DADOS DO MINISTÉRIO DA SAÚDE	39
CONSIDERAÇÕES FINAIS	40
REFERÊNCIAS	45

## INTRODUÇÃO

No cenário atual de intensa digitalização e interconexão, as empresas se deparam com desafios cada vez mais complexos no que diz respeito à proteção dos dados pessoais de seus clientes e usuários. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) surge como uma importante legislação brasileira, estabelecendo diretrizes e regras para o tratamento de informações pessoais no ambiente digital.

A LGPD, inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, entrou em vigor em setembro de 2020 no Brasil, e desde então tem impactado significativamente a forma como as empresas lidam com as informações dos seus clientes e parceiros comerciais. Em um mundo cada vez mais conectado, a proteção da privacidade e o uso ético dos dados expõem-se como questões cruciais para o pensamento e o sucesso de uma organização.

Logo, a comunicação empresarial exerce um papel fundamental, sendo responsável por transmitir informações relevantes, promover a imagem da empresa e estabelecer um relacionamento de confiança com o público. No entanto, diante das exigências da LGPD, as estratégias de comunicação empresarial precisam se adaptar e adotar medidas para garantir a conformidade com a legislação vigente.

Este trabalho tem como objetivo investigar a relação entre a LGPD e a comunicação empresarial, explorando de que forma a lei impacta as práticas de comunicação e os processos de gestão da informação nas organizações. Foram analisados os desafios e oportunidades que surgem com a implementação da LGPD, bem como as melhores práticas de comunicação que podem ser adotadas para assegurar a conformidade e promover a transparência no tratamento de dados pessoais.

Para tanto, será realizada uma revisão bibliográfica sobre a LGPD e a comunicação empresarial, buscando compreender os princípios e diretrizes da lei, bem como os aspectos relevantes da comunicação corporativa no contexto da proteção de dados. Além disso, serão realizados estudos de casos e entrevistas com profissionais da área, a fim de obter uma visão mais abrangente e prática dos impactos da LGPD na comunicação empresarial.

Espera-se que o estudo contribua para o aprofundamento do conhecimento sobre a interseção entre a LGPD e a comunicação empresarial, fornecendo insights

e orientações para empresas que buscam se adequar à legislação e promover uma comunicação transparente e responsável com seus públicos de interesse.

## **1 DOS DIREITOS HUMANOS FUNDAMENTAIS À INTIMIDADE E À VIDA PRIVADA**

Os direitos humanos fundamentais à intimidade e à vida privada são pilares essenciais da dignidade e da liberdade humana, e sua proteção é crucial para o funcionamento de sociedades justas e democráticas. Afinal, a dignidade da pessoa humana é, na visão de Flávia Piovesan (2012), o sol, a maior estrela do sistema de direitos e garantias fundamentais. Esses direitos estão consagrados em diversos instrumentos internacionais, como a Declaração Universal dos Direitos Humanos (artigos 12 e 17), o Pacto Internacional sobre Direitos Civis e Políticos (artigos 17 e 18) e a Convenção Europeia dos Direitos do Homem (artigo 8º). Eles também são reconhecidos em muitas constituições nacionais ao redor do mundo.

O artigo 5º, X, da Constituição da República prevê que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. Também o novo Código Civil (Lei 10.406/02) tratou dos direitos da personalidade nos artigos 11 a 21, destinando todo um Capítulo ao tema. Assim é que o artigo 21 dispõe que 'A vida privada da pessoa natural é inviolável e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma' (CORAZZA, ÁVILA, p. 243, 2022)

É impossível elaborar um conceito único para os direitos fundamentais à intimidade e à vida privada. Alguns autores sustentam que o primeiro se refere ao espaço pessoal e à esfera íntima de uma pessoa, incluindo seus pensamentos, sentimentos, relações e atividades privadas; enquanto o segundo engloba um espectro mais amplo e envolve todas as áreas da vida humana, como sua casa, sua correspondência, sua saúde, suas reflexões religiosas e sua orientação sexual.

"A pessoa natural é dotada de direitos e deveres no plano internacional. Em relação aos direitos, a própria existência dos direitos humanos, assim como também a do direito humanitário, revelam-se como os principais marcos a favor dos indivíduos" (AZEVEDO; CABACINHA, p.11, 2021).

Os direitos humanos fundamentais à intimidade e à vida privada trazem uma ambiguidade significativa que lhes atribui simultaneamente um sentido

negativo-ideológico e um positivo-reivindicador. Assim, esses direitos podem ser entendidos como políticos enquanto canais simbólicos para a produção de novos sentidos.

Ora, está mais do que óbvio que a proteção desses direitos é fundamental por várias razões. Além da já mencionada conexão entre eles e a dignidade da pessoa humana, o direito à privacidade permite que as pessoas tomem decisões sobre questões pessoais, como suas opiniões, relacionamentos e escolhas de estilo de vida, sem interferência indevida do Estado ou de terceiros. A proteção à intimidade também é crucial para garantir que as pessoas se sintam livres para expressar suas opiniões, explorar novas ideias e buscar conhecimento sem o medo de vigilância ou represálias.

Defendida a necessidade de proteção da vida privada e da intimidade, não podemos fechar os olhos para o ambiente em que elas são mais ameaçadas: o contexto digital de compartilhamento de dados pessoais. Com as novas estratégias de marketing digital e os novos algoritmos das grandes corporações, é essencial compreender a hipossuficiência dos usuários de serviços digitais frente às organizações empresariais e ao próprio Estado. Nesse ínterim:

Diante dessas novas tecnologias e dos problemas que lhes são indissociáveis, as empresas responsáveis por esse novo meio de comunicação têm optado pelo maior monitoramento dos conteúdos publicados em suas plataformas pelos seus usuários, o que gera grande discussão e muita controvérsia acerca de direitos como a privacidade e a liberdade de expressão. (VILHENA.; BARROS, pág. 71, 2021)

Sendo assim, a proteção à privacidade online e aos dados pessoais é fundamental para garantir que as pessoas tenham confiança para compartilhar informações e se envolver em atividades online — como comunicação, compras e serviços bancários — sem preocupações excessivas com sua exposição.

## **1.1 DA (DESNECESSÁRIA) DISTINÇÃO ENTRE OS CONCEITOS DE INTIMIDADE E VIDA PRIVADA**

Na Carta Magna de 1988, art. 5º, inciso X, o legislador diferencia os direitos fundamentais à intimidade e à vida privada. Vejamos: “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”.

Partindo-se do pressuposto pelo qual não há palavras inúteis ou desnecessárias na Lei, convém distinguir, somente para fins didáticos, os conceitos supramencionados:

A Constituição protege a privacidade (gênero) ao reconhecer como invioláveis a vida privada, a intimidade, a honra e a imagem das pessoas (espécies), assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação." (Novelino, Marcelo, 2012, pg. 76).

Segundo Novelino (2012), a esfera privada inclui informações relacionadas a situações de maior proximidade emocional, os chamados contextos relacionais específicos, como a orientação sexual e religiosa; enquanto a esfera íntima se relaciona à essência única de cada pessoa, sua identidade interna ligada às emoções e à personalidade (como autoestima e autoconfiança).

Em outras palavras, a vida privada é composta de informações em que somente seu titular pode optar por divulgá-las ou não. Já a intimidade diz respeito ao modo de ser da pessoa, à sua identidade, que pode, muitas vezes, ser confundido com a vida privada. Podemos dizer, assim, que dentro da vida privada ainda há a intimidade da pessoa humana.

Todavia, conforme explica o professor Bedê (2014), essa distinção entre vida privada e intimidade é academicamente inútil. Isso porque "a subjetividade ínsita na separação dos termos não traz benefícios práticos e, lembrando a famosa navalha de Ockham, deve-se optar pela explicação mais simples de um fenômeno." (Bedê, pág. 74, 2014).

## **2 DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)**

Em uma análise inicial acerca das diretrizes da LGPD, é importante destacar o que *não* é tratado nesse diploma legal. Nas palavras de Maldonado e Blum:

A Lei Geral de Proteção de Dados Brasileira (LGPD) se preocupa e versa apenas e tão somente sobre o tratamento de dados pessoais. Ou seja, não atinge diretamente dados de pessoa jurídica, documentos sigilosos ou confidenciais, segredos de negócio, planos estratégicos, algoritmos, fórmulas, softwares, patentes, entre outros documentos ou informações que não sejam relacionadas a pessoa natural identificada ou identificável. Toda essa miríade de outros tipos de informações ou documentos encontram tutela em distintos diplomas legais, como a Lei de Propriedade Industrial (Lei 9.279/1996), a Lei de Direitos Autorais

(Lei 9.610/1998) e a Lei de Software (Lei 9.609/1998), apenas para citar alguns exemplos. (MALDONADO, pág 55, 2022)

O âmbito de incidência da referida Lei se restringe exclusivamente aos dados pessoais. É importante destacar que a LGPD não faz distinção entre dados digitais e não digitais, abrangendo qualquer tipo de informação pessoal, seja ela física ou eletrônica. Isso significa que a aplicação da Lei ocorre em todas as operações de coleta ou tratamento de dados de indivíduos localizados em território brasileiro, independentemente do meio utilizado, do país onde os dados estavam armazenados ou da sede do responsável pelo controle ou operação desses dados.

E por que a tutela de dados pessoais se fez necessária ao ponto de ter sido aprovada uma lei tão específica quanto a LGPD? Para proteger os direitos humanos constitucionalmente assegurados aos brasileiros.

Nas palavras do professor Américo Bedê:

“Seria um sonho ampliar a privacidade e, a um só tempo, ampliar a segurança, como é um sonho a ideia de máxima efetividade de direitos fundamentais numa lógica de mercado preocupada apenas em como reduzir custos e ampliar lucros e consumidores. Não se pode ter tudo.” (Bedê, pág. 101, 2014).

Diante desse contexto empresarial e mercadológico de guerra por dados pessoais, em que a informação é ouro e o consentimento é viciado, a LGPD surge como um contrapeso estritamente necessário para proteger a inviolabilidade da intimidade e da vida privada.

As regras protegidas pela Lei Geral de Proteção de Dados são regulamentadas com base em alguns princípios fundamentais, ressaltando-se a preservação da privacidade; a salvaguarda da liberdade de expressão, de informação, de comunicação e de opinião e a incolumidade da intimidade, da confiança e da imagem. Tais fundamentos estão intimamente relacionados aos direitos conferidos aos titulares de dados diante de pessoas físicas e jurídicas com os quais mantêm algum tipo de vínculo, seja ele de natureza comercial ou laboral. O processamento de dados pessoais é realizado em consonância com as finalidades empresariais na prestação de seus produtos e serviços, e deve ser feito de forma adequada e compatível com tais finalidades. Como se vê, é gritante a magnitude desta legislação nas relações sociais e comerciais bem como seus impactos nos processos comunicativos empresariais, conforme será estudado em sequência.

## 2.1 DO HISTÓRICO DA LEGISLAÇÃO INTERNACIONAL SOBRE A PROTEÇÃO DE DADOS PESSOAIS

Os anos 1970 trouxeram mudanças absolutas sobre o corpo social como um todo. Graças à evolução da informática e das telecomunicações, ao advento dos computadores e ao incremento no uso de processamento de dados, inclusive pessoais, formaram-se blocos econômicos empresariais, o que, por sua vez, estimulou ainda mais o compartilhamento de dados pessoais em grandes quantidades e em escala internacional. É, como se vê, um ciclo que se retroalimenta.

Nas palavras de Maldonado: “Esse cenário revelou um aumento de produtividade e eficiência de empresas e governos e, por outro lado, também fez crescer a preocupação com a proteção da privacidade de indivíduos, sobretudo diante do fluxo transfronteiriço de dados”.

Diante desse quadro, os Estados enxergaram, com razão, a necessidade de se proteger, de forma mais específica, os dados pessoais, que são a força motriz desse novo sistema. De acordo com o professor Bruno Bioni, a Suécia foi o primeiro país a legislar sobre o tratamento de dados de caráter pessoal através da promulgação da lei “Sw. Datalagen”, em 1973.

Já na década de 1980, a Organização para o Desenvolvimento e Cooperação Econômica (OCDE) emitiu diretrizes a respeito do tema, as quais foram atualizadas e ampliadas mais de três décadas depois. Em ambos os momentos, o fio condutor foi justamente o papel estratégico dos dados pessoais para o progresso socioeconômico.” (BIONI, 2021, pág. 54).

Em 1983, foi a vez da Alemanha: o Tribunal Constitucional Alemão, fundamentado no princípio da Dignidade da Pessoa Humana, cunhou a chamada Lei de Direito à Autodeterminação Informativa, “BverfGe 65,1 – Volkszählungsurteil”. Através desse diploma legal, o Estado discorria sobre a importância da proteção aos dados pessoais, que não se restringe ao respeito à privacidade, mas também garante o controle e a liberdade do cidadão.

Ainda sob a visão de Bioni, em 1985, a legislação de proteção de dados foi unificada na Europa:

“A ‘DIRECTIVA 95/46/CE’, também conhecida como “Diretiva sobre Proteção e Fluxo de Informações”, foi o primeiro documento transnacional a respeito de proteção de dados, estabelecendo

parâmetros que são seguidos até hoje, fornecendo garantias aos cidadãos e regulamentando a proteção de dados.”

Foi somente após os anos 2000 que essa questão começou a ser discutida fora da Europa. Uma vez dada a largada dessa “corrida por dados”, em que grandes corporações passaram a disputar os registros pessoais dos indivíduos, os Estados não europeus também fizeram surgir leis de proteção à privacidade alinhadas com o sentimento de equilíbrio entre a proteção das liberdades individuais e a preservação de um fluxo aberto de dados pessoais capaz de sustentar o livre comércio internacional.

Portanto, referidos direitos fundamentais, como o da privacidade, ganharam maior necessidade de proteção legal, como por meio da LGPD, assim como da General Data Protection Regulation (GDPR), norma da União Europeia que inspirou a legislação brasileira, diante da quantidade avassaladora de dados coletados na era digital e do elevado grau de organização e inteligência empregado sobre eles (progresso quantitativo e qualitativo), viabilizando análises valorativas, não apenas pelo Estado sobre os cidadãos, mas também por empresas privadas. (MALDONADO, 2022, pág.23)

Sobre a era digital (pós-2000), Manuel Castells faz alusão à criação de um paradigma inovador durante os anos 70 do século XX, que é o campo da tecnologia da informação. Ele também discute o surgimento subsequente de uma sociedade e economia baseada em informações (CASTELLS, 1999, p.40-209), frequentemente referida por diversos nomes, incluindo o termo "digitais", como sugerido por alguns pesquisadores (CANUT, 2007, p. 47-52).

Em outras palavras, considera-se que houve uma transição do modo de produção industrial para o informacional, no qual as tecnologias responsáveis pela criação de conhecimento, processamento de informações e comunicação de símbolos se tornaram a principal fonte de produtividade.

Nessa linha de raciocínio, cabe citar o artigo “Decisões Automatizadas e o direito à explicação no regulamento geral de proteção de dados da União Europeia”, publicado na Revista de Direitos e Garantias Fundamentais, de autoria de Letícia Canut:

Com o avanço das Tecnologias de Informação e Comunicação ao longo dos anos e das novas potencialidades por elas criadas, observa-se que as tecnologias de processamento, geração e tratamento passam a atuar não apenas sobre a informação, mas sobre quaisquer dados, estejam eles estruturados ou não estruturados. Nesse contexto de criação, coleta, armazenamento,

tratamento, disseminação e transferência exponenciais de dados, de aumento da capacidade de seu processamento e do barateamento das tecnologias voltadas para esse fim, passa-se a falar em sociedade e economia de dados.(CANUT, pág. 106, 2007)

Atualmente, o Regulamento Geral de Proteção de Dados da União Europeia, conhecido pela sigla GDPR, conceitua o tratamento de dados pessoais como:

(...) Uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição (JORNAL OFICIAL DA UNIÃO EUROPEIA)

Para lidar com o *Big Data*, termo elencado pela doutrina para se referir à vasta quantidade de informações digitais e de dados pessoais que surgiram após os anos 2000, passou-se a adotar uma abordagem de inovação centrada em dados. Essa abordagem abrange serviços de armazenamento de dados, infraestrutura de rede e utilização de *softwares* e *hardwares*, incluindo algoritmos associados. Nessa mesma época, surgiram conceitos como computação em nuvem (*cloud computing*) e mineração de dados (*data mining*).

## 2.2 DAS DIRETRIZES E REGULAMENTOS DA LGPD

As diretrizes da Lei Geral de Proteção de Dados (LGPD) são fundamentais para garantir a proteção dos dados pessoais dos cidadãos, estabelecendo limites e responsabilidades para as organizações que tratam dessas informações. Algumas de suas regras são:

- a. **Consentimento e finalidade específica:** a LGPD estabelece que o tratamento de dados pessoais só pode ocorrer com o consentimento do titular dos dados ou mediante outras bases legais previstas na lei. Além disso, as organizações devem informar de forma clara e transparente a finalidade específica para a qual os dados serão utilizados.

Mas, afinal, o consentimento dos donos desses dados basta para as empresas os manusearem livremente? Depende do que se entende por “consentimento”. Será mesmo que o simples aceite dos “termos e condições”

de determinado produto ou serviço é suficiente? A resposta é negativa. De acordo com Bruno Ricardo Bioni, é necessário haver a chamada “adjetivação do consentimento”, de modo que os indivíduos, ao fornecerem seus dados pessoais para as diversas organizações, o façam de forma intencional, expressa e livre de coerção:

Com a publicação da LGPD passa a ser necessário o consentimento expresso do titular dos dados/usuário para a realização de coleta e tratamento desses dados. Alguns critérios devem ser preenchidos para que este consentimento seja considerado válido. Trata-se da chamada “adjetivação do consentimento”. Entre os critérios, estão os que exigem que o consentimento aconteça como manifestação da vontade do titular dos dados, de forma intencional, livre de coerção, expressa, clara e inequívoca, pela qual o titular dos dados concorda com o tratamento desses dados pessoais para uma finalidade determinada, ou seja, a autorização é concedida para um processo específico (BIONI, Bruno Ricardo, 2021, pág. 34)

No mesmo sentido, LS Mendes e GCS da Fonseca, no artigo "Proteção de Dados para Além do Consentimento: Tendências Contemporâneas de Materialização", discutem a necessidade de ir além do mero consentimento formal no que diz respeito à proteção de dados. Os autores destacam que a LGPD traz a necessidade de que as organizações adotem medidas de segurança e realizem estimativas de impacto à proteção de dados.

O art. 9º, inciso I, da LGPD, destaca a importância da finalidade específica do tratamento de dados:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - Finalidade específica do tratamento (LGPD, 2018)

A LGPD destaca o consentimento como um dos princípios fundamentais para o tratamento de dados pessoais. No entanto, o consentimento por si só não é suficiente para garantir a proteção dos dados, sendo necessário considerar outras medidas, como a transparência, a finalidade específica do tratamento e a segurança das informações.

**b. Necessidade de minimização do uso de dados pessoais:** é esperado que as organizações colem apenas os dados pessoais estritamente necessários à realização de suas funções. O princípio da minimização de dados estabelece que as empresas devem evitar a coleta excessiva e desnecessária de informações pessoais. Ele está explicitamente descrito no art. 16, inciso II, da Lei nº 12.965, de 23 de abril de 2014, denominada Marco Civil da Internet (MCI).

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

(...)

Artigo 7º, X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

(...)

Artigo 16.

(...)

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais. (MARCO CIVIL DA INTERNET, 2014)

Muito embora a LGPD e o Marco Civil da Internet tenham âmbitos de incidência diversos — a primeira trata dos dados pessoais específicos de cada indivíduo (*on-line* ou *off-line*), enquanto o segundo disciplina as relações na Internet de forma geral —, eles se comunicam com frequência. Isso porque existe "um espectro enorme de relações na Internet em que se pode identificar concreta ou potencialmente uma pessoa natural" (Maldonado, 2022).

Nesse contexto, o legislador de 2014 achou conveniente inserir, com a promulgação da Lei nº 12.965, duas regras de inequívoca importância no que tange à coleta e o armazenamento de dados pessoais: a primeira delas foi a inclusão de um décimo direito fundamental garantido aos usuários da Internet, qual seja, o direito à exclusão definitiva dos dados pessoais que eles tiverem fornecido a determinada empresa; a segunda regra determina que o tratamento de dados pessoais deve ser realizado somente mediante uma finalidade específica, legítima, explícita e devidamente informada ao usuário.

As duas alterações legislativas supracitadas têm o condão de minimizar ao máximo a utilização, a coleta e o armazenamento de dados pessoais. Nas palavras de Maldonado e Blum:

Assim, o artigo 16 do Marco Civil da Internet, ao vedar a guarda de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, já se encontra sob o paradigma da minimização da coleta de dados pessoais, mas ainda traz o consentimento do titular como destaque das bases legais para o seu tratamento. A LGPD, ao fazer a remissão expressa para as exceções previstas em suas normas, inclui no Marco Civil da Internet todas as hipóteses em que o tratamento de dados pessoais pode ser mantido, como já apontado acerca do artigo 16 da LGPD, e todas as hipóteses em que haja uma nova base legal, que não o consentimento do titular, para o tratamento de seus dados pessoais. (MALDONADO, 2022, pág. 34)

- c. Transparência e informações claras:** a LGPD estabelece a obrigação das organizações de fornecer informações claras, precisas e acessíveis aos titulares sobre como seus dados serão tratados. Isso inclui informações sobre os responsáveis pelo tratamento, os direitos do titular e os prazos de retenção dos dados.

A clareza na coleta, armazenamento e fornecimento de dados pessoais também é fundamental para garantir a conformidade com a LGPD. É responsabilidade das empresas coletoras de dados fornecer informações precisas e compreensíveis sobre suas práticas de proteção deles, garantindo que os titulares saibam exatamente como suas informações estão sendo tratadas e para que estão sendo coletadas.

Inclusive, a própria Lei prevê a nulidade do consentimento dos usuários para o uso de seus dados pessoais “caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.” (art. 9º, §1º, LGPD). Isso significa que as organizações devem fornecer aos indivíduos informações claras e acessíveis sobre o que está sendo coletado, como será utilizado, por quanto tempo será armazenado e com quem será compartilhado.

Outrossim, a transparência contribui para uma relação equilibrada entre as partes envolvidas. Ao saberem como seus dados estão sendo utilizados, os indivíduos têm a capacidade de exercer seus direitos, como o

direito de acesso, retificação e exclusão de seus dados pessoais. Isso empodera os usuários e lhes dá controle sobre suas informações.

A necessidade do fornecimento de informações claras e transparentes sobre a coleta e o armazenamento de dados pessoais aos titulares decorre da própria natureza dessa relação jurídica. Nas palavras de Bruno Bioni:

As relações de trabalho têm por inerente à própria caracterização do vínculo empregatício a subordinação, evidenciando uma relação assimétrica de poder. O mesmo ocorre nas relações de consumo dado o controle dos meios de produção pelo fornecedor e o poder econômico que dele decorre. O reconhecimento da posição de vulnerabilidade de certos grupos redundava no dirigismo legal característico dessas legislações, de modo a reequilibrar a relação (BIONI, 2021, pág. 85)

A interação legal entre as pessoas físicas e jurídicas que armazenam, manipulam, compram e adquirem dados pessoais e os indivíduos detentores dessas informações é caracterizada por uma gritante assimetria de poder. Por esse motivo, a LGPD surgiu como uma forma de equilibrar essa relação jurídica e de evitar a violação dos direitos e garantias fundamentais do titular dos dados. Afinal, de acordo com Maldonado e Blum:

A defesa do titular dos dados de forma individualizada se ressentia da inegável disparidade de meios e recursos entre os contendores. O reconhecimento dessa realidade resultou na previsão pela LGPD de normas de dirigismo que, submetendo o Poder Público aos seus ditames, potencializa o caráter de transparência no tratamento de dados, tornando suas hipóteses excepcionais. (MALDONADO; BLUM, 2022, pág. 76)

**d. Direitos básicos dos titulares sobre seus dados:** a lei concede aos titulares uma série de direitos em relação aos seus dados pessoais. Isso engloba o direito de acessá-los, de corrigir informações incorretas, de excluí-los quando não forem mais necessários, de transferi-los para outra empresa, entre outros direitos. Os cidadãos são, dentro de um contexto de disputa por dados pessoais, sujeitos extremamente vulneráveis e, como tais, devem receber a devida proteção jurídica. É o que dispõe o art. 18 da LGPD:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.(LGPD, 2018)

Nessa ótica, LM Sá Martino e AC Salgueiro Marques abordam as vulnerabilidades e visibilidades dos sujeitos no contexto das mídias digitais. Segundo os autores, a LGPD tem como objetivo proteger a privacidade e a autodeterminação dos indivíduos diante das ameaças e exposições decorrentes do tratamento inadequado de dados. Portanto, é necessário que as organizações adotem medidas para garantir a segurança e a privacidade desses dados, evitando riscos necessários e protegendo os direitos dos indivíduos.

**e. Necessidade de adoção de medidas de segurança:** é responsabilidade das organizações adotar medidas técnicas para garantir a segurança dos dados pessoais. Isso inclui a prevenção de acessos não autorizados, a detecção e resposta a incidentes de segurança e a implementação de políticas internas que promovam a proteção dos dados. De acordo com Maldonado e Blum:

Os agentes de tratamento – leia-se o controlador (aquele a quem compete as decisões referentes ao tratamento de dados pessoais) e o operador (aquele que realiza o tratamento de dados pessoais em nome do controlador), de acordo com as definições do art. 5º, incs. VI, VII e IX da LGPD – devem implementar medidas de segurança, medidas técnicas e medidas administrativas capazes de proteger os dados pessoais. (MALDONADO; BLUM, 2022, pág. 46)

A LGPD define o direito à segurança como a "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”.

As medidas de segurança são, portanto, um gênero cujas espécies são: i. medidas técnicas, isto é, ações adotadas no campo da Tecnologia da Informação (por exemplo, mecanismos de segurança implementados em softwares e hardwares, recursos que controlam o fluxo de dados em redes, instrumentos para detecção de invasões em sistemas, recursos de criptografia, separação de servidores etc.) e ii. medidas administrativas que se referem a "atividades realizadas no âmbito administrativo-gerencial dos agentes de tratamento, incluindo-se as de natureza jurídica" (Maldonado, 2022), a exemplo de políticas de privacidade de sites e aplicativos, capacitação dos empregados cujas atividades envolvam o tratamento de dados pessoais, controle de acesso aos arquivos físicos, entre outras.

Nesse íterim, Fábio Mattos, em seu estudo "Compliance à LGPD no contexto organizacional da IMEPEL INDÚSTRIA METALÚRGICA LTDA", enfoca a importância da implementação de programas de compliance (compliance) nas organizações, a fim de garantir a conformidade com a LGPD. O autor ressalta a necessidade de adoção de políticas, processos e controles internos que assegurem a proteção adequada dos dados pessoais, incluindo a necessidade de diminuição da quantidade de dados pessoais armazenados pelas empresas em seu número máximo. Busca-se, por meio desse princípio, invadir em menor escala possível a privacidade de cada usuário de produto ou serviço.

- f. Responsabilidade e prestação de contas por parte dos operadores de dados:** a LGPD estabelece que as pessoas físicas e jurídicas responsáveis pela coleta, manutenção e manuseio de informações pessoais devem assumir a responsabilidade pelo tratamento adequado dos dados e estar prontas para prestar contas às autoridades competentes em caso de desconformidade ou descumprimento da Legislação. O art. 46, *caput*, LGPD, é assertivo ao determinar que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de

destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

Percebe-se que o legislador enumerou uma série de danos contra os quais os operadores de dados pessoais devem aplicar as supramencionadas medidas de segurança. São eles: i. acessos não autorizados a informações pessoais dos titulares, realizados por "pessoas alheias ao sistema e que não têm legitimidade legal, regulamentar ou estatutária para ingressar" (BITENCOURT, 2012. p. 449-450.); ii. destruição (eliminação) ou perda (desaparecimento) de dados pessoais sem o consentimento de seu titular; iii. alterações no conteúdo dos dados pessoais (realizada por pessoas não autorizadas) ou modificações indevidas (realizadas por pessoas autorizadas); iv. comunicação (transmissão, informação, divulgação, revelação, exposição, difusão) ilícita de informações pessoais e v. qualquer outra forma de tratamento inadequado ou ilícito de dados pessoais (nesse ponto, o legislador deixa claro se tratar de um rol meramente exemplificativo de condutas).

Uma vez constatada qualquer das situações enumeradas pela Lei, o §1º do art. 46 dispõe que

§1º. A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. (LGPD, 2018).

Nesse contexto, os operadores de dados pessoais que desrespeitarem os direitos de seus titulares através de condutas omissivas ou comissivas deverão prestar contas à Autoridade Nacional de Proteção de Dados (ANPD), que é justamente o ente público responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, conforme definição do art. 5º, inc. XIX, do referido diploma. Ademais, como nos ensinam Maldonado e Blum:

Ainda, constata-se que o legislador optou por adjetivar como "mínimos" os padrões técnicos que a ANPD poderá dispor, deixando claro que não se espera a imposição de obrigação do uso de absolutamente todas as ferramentas tecnológicas existentes ou que venham a existir para garantir a segurança dos dados pessoais, situação que seria inviável, inclusive do ponto de vista econômico. Isso porque é impossível garantir segurança absoluta, seja no mundo físico, seja no mundo digital. (MALDONADO; BLUM, 2022, pg. 146)

A prestação de contas à ANPD e aos usuários ocorre conforme um protocolo definido pela própria Autoridade. Em primeiro lugar, tem-se a fase que Mota Alves e Canto Lima denominam “prognóstico”. Nessa etapa, deve-se determinar objetivamente o incidente de segurança que acarretou ou poderá acarretar risco ou dano relevante aos titulares dos dados pessoais. É uma tarefa árdua, cujo tema não foi objeto de regulamentação pela ANPD. De acordo com Bruno Ópice Blum (2021) "cabe a cada empresa estabelecer internamente as premissas para estimar o impacto e os riscos de um incidente de segurança envolvendo dados pessoais."

Finalizado o prognóstico, o próximo nível de reparação de danos é o diagnóstico. Nessa etapa, os operadores de dados devem levantar informações essenciais do incidente de segurança, entre as quais se podem citar: a causa do evento; as circunstâncias do incidente (considerando atributos clássicos da segurança da informação, como perda de confidencialidade, de integridade ou de disponibilidade); as categorias dos dados pessoais que foram atingidos (dados simples, comportamentais, financeiros, sensíveis etc.) e a extensão do incidente, isto é, possíveis consequências aos indivíduos afetados (por exemplo, discriminação, violação a direitos personalíssimos, fraudes financeiras ou roubo de identidade, entre outros). Dessa forma,

[...] O agente de tratamento poderá adotar como referência para a avaliação e documentação dos riscos os critérios já estabelecidos nos posicionamentos iniciais da ANPD, pela Secretaria de Governo Digital (SGD) do Ministério da Economia, ou por entidades internacionais. (LIMA, 2023, pág. 104)

Por fim, com base nos resultados alcançados pelo diagnóstico, que deverão ser devidamente registrados, será viável verificar se os responsáveis pelo processamento dos dados devem ou não informar aos indivíduos titulares e à autoridade reguladora. A comunicação deverá ocorrer, conforme estipulado pela ANPD, em no máximo dois dias contados a partir do conhecimento do incidente de segurança por parte dos tomadores de dados pessoais, prazo este que poderá ser flexibilizado a depender das circunstâncias do evento e da existência de justo motivo, que terá que ser demonstrado. Nos termos do art. 48, § 1º, da LGPD:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. (LGPD, 2018)

Essas seis diretrizes ilustram bem o fundamento da LGPD e são essenciais para garantir a proteção dos dados pessoais e promover uma cultura de respeito à privacidade.

### **3 DA COMUNICAÇÃO ORGANIZACIONAL OU EMPRESARIAL**

Para fins da lei, tratamento de dados é qualquer operação realizada com dados pessoais, como a coleta, a produção, a recepção, a classificação, a utilização e o acesso, além da reprodução, da transmissão, da distribuição, do processamento, do arquivamento, do armazenamento, da eliminação, da avaliação, da modificação, da comunicação, da transferência e da difusão (art. 5º, inciso X, da LGPD), e só é possível a organização realizar o tratamento de dados pessoais em observância ao estabelecido no art. 7º, da Lei, que são as chamadas bases legais, ou seja, as hipóteses autorizativas de tratamento (BRASIL, 2018). Na visão de Canto Lima e Mota Alves:

De um lado, as organizações precisam garantir a necessária proteção aos dados pessoais da pessoa natural, extensão de seus direitos de liberdade e privacidade, atendendo os ditames da Lei nº 13.709/2018 pela adoção de medidas assecuratórias de conformidade à lei e, de outro, assegurar a existência da própria empresa, com programas de compliance robustos capazes de mitigar ou inibir a incidência de sanções legais pelos órgãos regulatórios. (LIMA; ALVES, 2023, pág.103)

Para Batista e Martins (2021), as indústrias acompanharam as mudanças e inovações da sociedade desde a primeira revolução industrial e, com o avanço tecnológico, passaram a usar dados em massa através dos recursos tecnológicos

existentes com o propósito de coletar, analisar e utilizar esses dados em tempo real, impulsionando os processos e a gestão dos sistemas de produção.

Desde as microempresas até as grandes corporações, é essencial que todas essas organizações se ajustem e cumpram cada qual as leis pertinentes ao seu setor de atuação, com ênfase na integridade e na ética. É fundamental que elas compreendam a importância de transmitir esses princípios aos colaboradores, delineando as atitudes esperadas e regulamentando as diretrizes a serem seguidas.

Nesse contexto, a comunicação organizacional surge como um instrumento assecuratório para garantir a conformidade da atuação de empresas públicas e privadas às diretrizes da LGPD.

Antes de adentrarmos nesta seara, é necessário entender melhor o contexto histórico de surgimento do conceito de comunicação empresarial e suas principais espécies: comunicação intraorganizacional e comunicação interorganizacional.

### **3.1 DO BREVE HISTÓRICO DA COMUNICAÇÃO ORGANIZACIONAL**

Assim como em qualquer evento histórico, não se pode dizer com certeza quando surgiu o conceito de comunicação organizacional. Há, na doutrina, quem indique as décadas de 1920 a 1950 como um provável período de nascimento das estratégias de comunicação empresarial, o que faz sentido, considerando a ascensão das esteiras de produção fordistas e do consumista *american way of life*. Nesse contexto, a comunicação empresarial funcionava como mais uma das ferramentas que visavam ao aumento da produtividade em larga escala.

Após esse período e até meados de 1970, porém, surgiu uma nova preocupação para as organizações empresariais, as relações humanas: “destacavam-se, principalmente, as práticas de uma comunicação que partia do alto escalão gerencial, a precisão de relatórios e eficiência dos diferentes meios de comunicação”. (CORRÊA LIMA, OLIVEIRA PEREIRA, pág. 36., 2015.).

No Brasil, a comunicação empresarial foi apresentada à comunidade científica por uma multinacional canadense: a Light & Power, transformada na AES Eletropaulo. Em 1925, a empresa estabeleceu no país o primeiro serviço de relações públicas (ABREU SOUZA, 2019).

A partir de 1960, assistiu-se a uma ampliação notável dos departamentos de relações públicas em empresas multinacionais, acompanhada de uma crescente

valorização das demandas da comunidade e da opinião pública. Essa origem, descrita pela ênfase nas publicações corporativas, identificou uma ligação fundamental entre a compreensão da comunicação organizacional e o uso de ferramentas para estreitar os laços entre a organização e seus diversos públicos.

O período entre 1990 e 2000 foi marcado por muitos estudos que buscavam ampliar o olhar em torno da comunicação organizacional com base em novos métodos e novas percepções teóricas, passando a adquirir uma forma mais abrangente. Não bastava somente informar, era preciso que as informações estivessem em harmonia com os propósitos da organização. Assim, “a comunicação ganha notoriedade, pela sua função de conhecer, analisar e direcionar esses fluxos informacionais para o objetivo geral da organização, dando um sentido estratégico à prática comunicacional” (OLIVEIRA, 2007, p. 2).

A partir dos anos 2000, a concepção de uma comunicação organizacional planejada e estratégica, fundamentada na investigação dos interesses dos públicos, em detrimento de um foco na empresa, ganhou proeminência tanto no âmbito acadêmico quanto no mercado. A comunicação dentro da organização adquiriu caráter estratégico ao se voltar para a realização da missão e dos objetivos propostos pela instituição:

Assim, o tema estratégico nas organizações está ligado à efetiva adaptação da organização com seu ambiente, por meio do tempo, entendendo por estratégia a criação e prática dos meios adequados para atingir os resultados desejados, melhorando a capacidade total de planejamento e organização para que possa adaptar-se ou inovar com sucesso aos tempos.” (MARCHIORI, 2011, p.164)

A comunicação, que antes fora concebida unicamente como uma “ferramenta” para atingir as metas pujantes das empresas e que era empregada de maneira arbitrária por meio de uma abordagem hierárquica, agora é contemplada como um processo deliberado e estratégico. Contudo, para efetuar o planejamento e a gestão da comunicação nas organizações, em meio a um ambiente complexo e a um mercado altamente competitivo, os gestores devem examinar conhecimentos que transcendam o meramente nível técnico e adentrem uma perspectiva mais abrangente. Essa perspectiva considera a implementação de estratégias que, por vezes, levam em conta fatores externos e conflitos potenciais, em oposição a uma abordagem linear de comunicação.

Esse novo cenário, segundo Abreu (2019, pg. 12), apresenta a comunicação organizacional como fator de humanização das organizações. O autor destaca que “mesmo em tese, atualmente, há uma renovação nos estilos de gestão, que ora se apresentam mais voltados às pessoas com foco na descentralização e participação dos indivíduos, buscando a valorização e a satisfação das necessidades humanas como a dignidade e a valorização de competências individuais”.

A comunicação organizacional tem três esferas principais, de acordo com a visão de comunicação institucional, a comunicação mercadológica, a comunicação interna e a comunicação administrativa. Existe, ainda, uma mescla entre os quatro conceitos, formando a chamada comunicação integrada, que busca alcançar de maneira eficaz e harmoniosa os objetivos da organização.

Entendemos por comunicação integrada uma filosofia que direciona a convergência das diversas áreas permitindo uma atuação sinérgica. Pressupõe uma junção da comunicação institucional, da comunicação mercadológica, da comunicação interna e da comunicação administrativa, que formam o mix, o com o composto da comunicação organizacional. (KUNSCH, 2010, p. 150)

Deetz (2010), por sua vez, deixa de lado a taxonomia de Kunsch e opta por dar enfoque às intenções, aos significados e aos efeitos das mensagens emitidas no contexto de comunicação empresarial. Para ele,

A comunicação vem sendo reconhecida como um processo fundamental pelo qual as organizações existem e como ponto central da produção e reprodução organizacionais demonstrando assim novas concepções de pensar e descrever a comunicação organizacional. Se, anteriormente, o foco estava na transmissão de mensagens, hoje se observa muito mais a formação do significado, da informação e do conhecimento. (DEETZ, 2010, p. 84).

Entendo ser esta a posição mais sensata, apesar da classificação sugerida por Kunsch, é mais conveniente dividir a comunicação organizacional conforme as intenções dos discursos e os sujeitos passivo e ativo das mensagens. Por isso, considere dois grandes subgrupos que compõem a comunicação organizacional, cada qual com objetivos específicos e com diferentes estratégias: a intraorganizacional e a interorganizacional.

### **3.2 DAS ESPÉCIES DE COMUNICAÇÃO EMPRESARIAL: INTERNA OU INTRAORGANIZACIONAL**

A comunicação intraorganizacional refere-se à troca de informações, ideias, dados e mensagens entre os membros de uma mesma organização. Essa forma de comunicação ocorre dentro dos limites da empresa e tem como objetivos principais manter uma coordenação eficiente das atividades, disseminar informações relevantes e promover um ambiente de trabalho colaborativo. A comunicação interna se divide em quatro áreas principais. São elas:

**a. Comunicação Vertical:** nesse tipo de comunicação, as informações fluem entre diferentes níveis hierárquicos da organização, como dos líderes para os funcionários e vice-versa. Isso inclui comunicações descendentes (de cima para baixo) e ascendentes (de baixo para cima). Vejamos brevemente cada uma delas:

**a.1. Comunicação vertical ascendente:** trata-se de uma comunicação em que o emissor da mensagem é um funcionário e o receptor é seu superior hierárquico, que tem a oportunidade de, imediatamente, oferecer uma mensagem de retorno.

Para exemplificar, imaginemos a situação de um grupo de empregados que acredita que as metas da empresa para um determinado departamento são muito altas e difíceis de serem alcançadas sem afetar a saúde mental dos trabalhadores. Diante desse quadro, eles decidem expor suas queixas ao diretor daquele setor, que poderá argumentar em sentido contrário ou refletir sobre a situação apresentada.

Como se vê, essa modalidade de comunicação tende a criar relações mais cordiais e transparentes entre diferentes estratos hierárquicos. A adoção de uma comunicação vertical ascendente sincera gera resultados positivos no ambiente organizacional, proporciona soluções ágeis para os desafios enfrentados pela empresa e contribui para o cumprimento de seus objetivos.

**a.2. Comunicação vertical descendente:** *contrario sensu*, na comunicação vertical descendente, a mensagem é emitida de um gestor, gerente ou supervisor para os seus subordinados. Diferente do que ocorre na comunicação descendente, inexistente a possibilidade de retorno ou de interação por parte dos receptores. As informações transmitidas nesse tipo de comunicação, incluem,

normalmente, regras, normas e políticas, além de instruções de tarefas e funções. Apesar de parecer limitada, a comunicação vertical é importante para as empresas que desejam manter a ordem e o alinhamento das atividades. Ela garante que as informações cheguem a todos os colaboradores de forma clara e objetiva, evitando possíveis conflitos e ruídos na comunicação.

**b. Comunicação Horizontal:** a comunicação horizontal se refere às interações que se estabelecem entre indivíduos que ocupam o mesmo patamar hierárquico em uma organização empresarial. A principal característica desse modelo de comunicação é a troca bidirecional de informações, que se opera em ambas as direções e ocorre de maneira transversal.

A comunicação horizontal é altamente valorizada em organizações que primam pelo trabalho em equipe e pela colaboração mútua, pois possibilita aos colaboradores compartilharem conhecimentos, habilidades e experiências, fomentando a inovação e a criatividade. Além disso, desempenha um papel fundamental na construção de um ambiente de trabalho saudável, onde os profissionais são reconhecidos e respeitados.

**c. Comunicação Diagonal:** é chamada de comunicação diagonal aquela cujo objetivo é inter-hierárquico, pela qual equipes distintas, gestores e diretores recebem a mesma informação da mesma forma. Ela é indicada para situações nas quais a empresa busca informar a todos os seus colaboradores sobre novos projetos, diretrizes e normas ou até mesmo enviar mensagens motivacionais.

**d. Comunicação Informal:** Por fim, a comunicação informal se refere às conversas não estruturadas que ocorrem entre os membros da organização. É a chamada “fofoca de escritório”. Embora não seja oficial, a comunicação informal desempenha um papel importante na cultura organizacional e pode afetar significativamente o ambiente de trabalho, seja para o bem ou para o mal.

### **3.3 DAS ESPÉCIES DE COMUNICAÇÃO EMPRESARIAL: EXTERNA OU INTERORGANIZACIONAL**

A comunicação externa ou interorganizacional, por outro lado, ocorre quando duas ou mais organizações trocam informações, ideias ou recursos entre si. Isso pode envolver parceiros comerciais, fornecedores, clientes, concorrentes e outras entidades externas.

“A comunicação interorganizacional é vista de forma diferente nas empresas. Uma empresa visualiza a comunicação como fundamental e parte da sua cultura e práticas e, outra, como algo que é incerto quanto ao valor positivo que pode ter, comparado com as perdas ou custos para a empresa. A comunicação de informações com os parceiros numa aliança possibilita a criação de vantagem estratégica e benefícios para o desempenho da empresa.” (Paulraj, Lado; Chen, 2008).

As empresas, com suas peculiaridades e objetivos distintos, adotam diversas abordagens em relação à comunicação externa. Algumas organizações optam por não compartilhar informações devido ao receio de que isso possa proporcionar uma vantagem injusta aos clientes e fornecedores. Além disso, há empresas que questionam o valor da comunicação interorganizacional quando comparada aos custos financeiros, recursos humanos e infraestrutura física envolvidos.

Por outro lado, existem organizações empresariais que tratam a comunicação interorganizacional como uma questão essencialmente tecnológica, investindo e desenvolvendo nessa área. A aposta na tecnologia é pautada sobre os benefícios que ela proporciona ao facilitar a conexão entre pessoas e empresas, resultando em uma melhoria na partilha de informações, ideias e conhecimentos.

Certas empresas, por outro lado, encaram a comunicação externa como uma parte intrínseca de sua cultura corporativa. Ao adotar essa abordagem, a troca de informações é feita de forma aberta, permitindo o compartilhamento de dados sensíveis relacionados a custos, planos de produção e estratégias tecnológicas.

De todo modo, a comunicação interorganizacional é essencial para estabelecer relacionamentos colaborativos, redes de negócios eficazes e parcerias bem-sucedidas. Alguns exemplos de aplicação dessa forma de comunicação incluem: i. comunicação com clientes e fornecedores para que as reais necessidades e expectativas dos primeiros sejam compreendidas e satisfeitas e para garantir um fluxo contínuo, econômico e eficaz de recursos e produtos; ii. formação de alianças e parcerias, tendo em vista que empresas que colaboram em projetos, *joint ventures*, ou acordos estratégicos dependem de uma comunicação aberta e eficaz para garantir o sucesso dessas parcerias; iii. ampliação das redes de negócios através do compartilhamento, entre associações empresariais, de

informações relativas a melhores práticas do setor, tendências do mercado e oportunidades de negócios e, por fim, iv. comunicação com concorrentes, que pode se fazer necessária para resolver questões regulatórias de preços ou de mercado.

Em resumo, tanto a comunicação intraorganizacional quanto a comunicação interorganizacional desempenham papéis essenciais ao sucesso das empresas. A comunicação eficaz dentro de uma organização promove a colaboração, a produtividade e o controle de metas, enquanto a comunicação entre organizações ajuda a estabelecer relações comerciais sólidas e adaptadas às demandas em constante mudança do mercado.

#### **4 DOS LIMITES DO “CONSENTIMENTO”**

Compreendidos os conceitos supramencionados, é importante enfatizar a necessidade de, em todas as esferas da comunicação empresarial, as diretrizes e regulamentos da LGPD serem defendidas e respeitadas. Seja em conversas informais entre os colaboradores de uma mesma empresa ou entre regulamentos e relatórios compartilhados entre CEOs de organizações concorrentes, é crucial que as violações aos dados pessoais sensíveis dos usuários e clientes sejam devidamente identificadas e punidas.

O conhecimento sobre as interferências dos algoritmos na tomada de decisões ou mesmo nas decisões automatizadas ainda é muito limitado e o tema tem sido objeto de estudos e políticas públicas internacionais e, também, nacionais. Apesar de tais iniciativas, trata-se de realidade que tem gerado crescente sentimento de impotência e perda de controle em relação ao tratamento de dados pessoais e à tutela de diferentes direitos fundamentais. (CANUT, pág.102, 2007)

Sob esse íterim, segundo o professor Nelson Camatta, as possibilidades de escolhas, no contexto digital, nada mais são do que uma “aparência de escolha”, já que são maiores do que se podem efetivamente realizar:

Vivencia-se, cada vez mais, na sociedade contemporânea, uma complexidade, na qual as possibilidades de escolhas são sempre maiores do que se podem efetivamente realizar. Além disso, essas mesmas possibilidades têm grandes chances de não se concretizarem: trata-se de um elemento contingente, determinando aquilo que se pode chamar de reflexividade social. (MOREIRA, pág. 190, 2007)

Nesse contexto, “os dados pessoais são o petróleo, o insumo ou uma *commodity*”, estando para a economia da informação como a destruição do meio ambiente estava para a economia industrial” (BIONI, 2021, pg. 17). Portanto, não é hiperbólico afirmar que a era atual é marcada pela morte da privacidade e pela crise

ou erosão da intimidade, pois as informações pessoais desempenham um papel central e dinâmico na economia atual. Além disso, elas representam uma base essencial e um recurso estratégico crucial para uma variedade de modelos de negócios. Estamos testemunhando uma sociedade e uma economia cada vez mais ligadas e dependentes desse constante fluxo de dados: “nesse contexto, historicamente, normas de proteção de dados pessoais sempre tiveram a dupla função de não só garantir a privacidade e outros direitos fundamentais, mas também fomentar o desenvolvimento econômico.” (BIONI, 2021, pg. 17).

De acordo com o professor Bioni, no contexto de comunicação organizacional, o suposto consentimento dos usuários é apenas um pressuposto objetivo para o compartilhamento de dados pessoais. Da leitura do art. 5º, inciso XII da LGPD, pode-se definir “consentimento” como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

O consentimento é apenas uma das dez bases legais previstas para o tratamento de dados pessoais. Porém, em razão do alto grau de transparência perante o titular, é a hipótese que pode trazer mais segurança jurídica para o controlador, a quem incumbe o ônus da prova que foi obtido em conformidade com a Lei. " (Maldonado, pág. 86, 2022)

Nesse sentido, para ser considerado válido, o consentimento deve ostentar cinco características principais:

- a. **Inequivocidade:** o consentimento para o compartilhamento de dados pessoais deve ser dado de forma inequívoca. Isso significa que as pessoas precisam entender o que estão consentindo, como seus dados serão usados e quem terá acesso a eles:

Significa que o titular, mesmo que implicitamente (uma vez que não precisa ser expresso), precisa concordar com aquilo que está disposto de modo claro para ele. Deve ser um ato positivo do titular e armazenado pelo controlador, para fins de prova, que indique essa manifestação." (Maldonado, pág. 102, 2022)

- b. **Informação:** pela característica da informação, o consentimento não deve ser obtido de forma ambígua ou por meio de linguagem complexa. Ora, é dever das empresas controladoras e operadoras de dados pessoais fornecer informações claras e precisas sobre o uso que fazem dos dados, sem utilizar jargões, termos técnicos ou informações enganosas:

Também caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca, o consentimento será considerado nulo." (Maldonado, pág. 56, 2022)

**c. Especificidade:** o consentimento deve ser solicitado para finalidades específicas e legítimas. As organizações não devem coletar dados sob um pretexto e depois usá-los para propósitos diferentes daqueles para que o consentimento foi originalmente concedido:

O consentimento também deverá ser previsto para finalidade determinada. Autorizações genéricas para o tratamento de dados pessoais serão nulas. Portanto, deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade e nos casos em que o tratamento sirva para fins múltiplos, de acordo com a avaliação da especificidade, deverá ser conferido consentimento para cada um desses fins." (Maldonado, pág. 67, 2022)

**d. Liberdade:** o consentimento deve ser dado livremente, sem coerção, pressão tolerada ou consequências negativas para aqueles que optam por não dar consentimento. Qualquer forma de canto ou manipulação não é aceitável.

“Livre” é conferir ao titular a oportunidade de dispor ou não de dados que não sejam fundamentais à prestação de um eventual serviço, em que pese o tratamento de dados pessoais poder ser condição para o fornecimento de produto ou de serviço. Sobre o assunto, como o conceito de consentimento do GDPR é semelhante ao da LGPD, interessante trazer algumas de suas disposições acerca do tema: ‘há que se verificar, com a máxima atenção, se a execução de um contrato está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato’. Não deverá se considerar que o consentimento foi manifestado de forma livre se o titular dos dados não dispuser de uma escolha verdadeira ou não puder recusar ou retirar o seu consentimento sem ser prejudicado. O Art. 29 WP cita o caso de um banco que solicita aos clientes o consentimento para usar seus dados de controle de pagamentos para fins de marketing. Esse tratamento não é necessário para a execução do contrato com o cliente. Se a recusa do cliente em consentir com esse propósito levar à negação dos serviços bancários, o encerramento da conta bancária ou o aumento da taxa, haverá violação à liberdade de consentir." (Maldonado, pág. 72, 2022)

**e. Possibilidade de retratação:** aos usuários dos serviços digitais deve ser dada a opção de retirar seu consentimento a qualquer momento. As organizações devem tornar fácil para os indivíduos revogarem o consentimento sem penalizações, suspendendo qualquer operação de dados

e/ou excluindo o conjunto de dados pessoais armazenados por operadores. É o que dispõem os incisos XIII e XIV, art. 5º, LGPD:

Art. 5º Para os fins desta Lei, considera-se:

(...)

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.”. (LGPD)

Além disso, quando se trata de dados de crianças e adolescentes, a LGPD estabelece uma idade mínima para que os indivíduos possam dar consentimento por conta própria, qual seja, 18 (dezoito) anos. Em geral, os dados de menores de idade são mais sensíveis e têm proteção especial. De modo análogo, para dados sensíveis, como informações ou orientação médica, muitas vezes, é necessário haver um nível mais alto de consentimento, considerando a natureza delicada dessas informações. Por fim, no ambiente de trabalho, considerando o poder diretivo do empregador, a questão do consentimento é mais complexa devido às relações de poder existentes. A pressão para permitir o compartilhamento de seus dados pessoais é maior, e as organizações empresariais precisam garantir que o consentimento seja dado voluntariamente.

Sobre esse tema, é importante discorrer brevemente sobre o conceito de autodeterminação informativa. Nas palavras de Maldonado e Blum,

“A autodeterminação informativa, que é o controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo – conjuga as duas já mencionadas concepções de privacidade de dados: a primeira de caráter negativo e estático; e a moderna, em que a intervenção (proteção) é dinâmica, durante todo o ciclo de vida dos dados nos mais variados meios em que possa circular. Nas palavras de Stefano Rodotà é um “poder permanente de controle sobre seus próprios dados”. (Maldonado, pág. 87. 2022).

Em outras palavras, o princípio mencionado aqui vai muito além do âmbito pessoal do cidadão, pois também se aplica às informações de natureza pública que estão relacionadas aos titulares, como suas opiniões políticas, filiação a sindicatos ou grupos religiosos, filosóficos ou políticos, incluindo o tratamento de dados pessoais de acesso público. Nesse contexto, é necessário levar em consideração a

questão específica, a honestidade e o interesse público que justificaram a divulgação dessas informações. Afinal,

De tal sorte, pensar que o cidadão possa ter o controle sobre seus próprios dados parece, atualmente, utopia. Porém, a autodeterminação informativa se apresenta como fundamento da LGPD, justamente nesse momento em que ainda predomina uma coleta e tratamento massivo e desenfreado de dados, como forma de devolver para o titular o poder sobre o fluxo e o uso dos seus próprios dados, mediante o estabelecimento de determinações objetivas aos agentes de tratamento. (Maldonado, pág. 92, 2022)

## **5 DO ESTUDO DE CASOS**

Para comprovar a relevância prática da pesquisa em questão, serão analisados a seguir, três casos de vazamento de dados pessoais no Brasil que eram operados e/ou controlados por grandes organizações empresariais.

### **5.1 DA EMPRESA “ACESSO SOLUÇÕES DE PAGAMENTO” E DO CADASTRO DE CHAVES PIX**

No dia 21 de janeiro de 2022, o Banco Central informou a ocorrência de um incidente de segurança relacionado ao vazamento de dados pessoais associados às chaves PIX, que estavam sob a responsabilidade da empresa Acesso Soluções de Pagamento. No incidente, ocorrido entre os dias 03 e 05 de dezembro de 2021, os dados de 160.147 chaves foram potencialmente expostos, incluindo informações como nome completo, CPF, instituição, número da agência e número da conta.

Nesse caso, o Banco Central atuou como empresa controladora de dados pessoais e a Acesso Soluções de Pagamento, como controladora. Nos termos do art. 5º, incisos VI e VII:

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;” (LGPD, 2018).

É importante destacar que, de acordo com o comunicado do Banco Central, não foram comprometidos dados confidenciais, como senhas, extratos ou outras informações protegidas por sigilo bancário. O próximo passo, conforme indicado

pela autoridade monetária, foi notificar individualmente às pessoas cujos dados foram expostos por meio do aplicativo ou *internet banking*.

*In casu*, estamos diante de uma falha na comunicação empresarial externa ou interorganizacional: o Banco Central, ainda que seja uma autarquia federal vinculada, assume o papel de organização e se comunica com a empresa Acesso Soluções de Pagamento. Trata-se, conforme supramencionado, da comunicação entre controlador e operador de dados:

Os agentes de tratamento – leia-se o controlador (aquele a quem compete as decisões referentes ao tratamento de dados pessoais) e o operador (aquele que realiza o tratamento de dados pessoais em nome do controlador), de acordo com as definições do art. 5º, incs. VI, VII e IX da LGPD – devem implementar medidas de segurança, medidas técnicas e medidas administrativas capazes de proteger os dados pessoais." (Maldonado, pág. 83, 2022)

Não é necessária uma cognição exauriente para perceber que os agentes de tratamento falharam na adoção de medidas de segurança administrativas ou corporativas, que "são as atividades realizadas no âmbito administrativo-gerencial dos agentes de tratamento, incluindo-se as de natureza jurídica" (Maldonado, 2022), por exemplo, políticas de privacidade de sites e aplicativos, políticas corporativas para proteção dos dados pessoais e capacitação dos empregados cujas atividades envolvam o tratamento de dados pessoais.

Esse erro, no contexto da comunicação organizacional, gerou o dever de os controladores de dados pessoais indenizarem os seus titulares. Sobre o tema, considerando que, nesse caso, os usuários dos dados pessoais são consumidores equiparados, convém colacionar a transcrição dos ensinamentos de Sérgio Cavaliere Filho:

O consumidor, portanto, como nos demais casos de responsabilidade objetiva já examinados, tem, apenas, que provar o dano e o nexo causal. A discussão da culpa é inteiramente estranha às relações de consumo. Mesmo em relação ao dano e ao nexo causal pode vir a ser beneficiado com a inversão do ônus da prova, artigo 6º, VIII." (CAVALIERE Filho, pág. 234, 2020).

No entanto, não houve notícias de responsabilização de quaisquer das empresas pela falha cometida.

## 5.2 DA OPERAÇÃO DEEPWATER

Em janeiro de 2021, a empresa PSafe identificou um suposto vazamento de dados pessoais de mais de 223 milhões de cidadãos brasileiros, um número superior à população do país. A pessoa jurídica acionou a Autoridade Nacional de Proteção de Dados (ANPD), que requisitou investigação por parte da Polícia Federal.

Em um comunicado divulgado na época, a ANPD anunciou sua intenção de investigar a origem do vazamento, como ele ocorreu, as medidas tomadas para conter e mitigar os danos por meio de um plano de contingência, bem como as possíveis consequências e prejuízos causados pela violação.

Os dados vazados se inseriam na definição de dados sensíveis, pois continham informações como: nome completo dos usuários, fotos, endereço, renda mensal e CPF, inclusive de pessoas falecidas. O art. 11 da LGPD descreve o conceito de dados pessoais sensíveis como:

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (LGPD)

Em março de 2021, a Polícia Federal, autorizada pelo ministro Alexandre de Moraes, cumpriu dois mandados de prisão de pessoas suspeitas de terem oferecido o banco de dados em fóruns da internet.

Pois bem, nesse caso, percebe-se que a empresa PSafe adotou estratégia correta de comunicação externa para com os titulares dos dados pessoais: imediatamente acionou a ANPD e comunicou os usuários sobre o vazamento.

### **5.3 DO VAZAMENTO DE DADOS DO MINISTÉRIO DA SAÚDE**

Em dezembro de 2020, reportagem do jornal O Estado de S. Paulo revelou que dados de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ou como beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança do Ministério da Saúde.

Os dados pessoais que foram expostos também eram sensíveis e deveriam estar protegidos por login e senha, mas havia uma vulnerabilidade no código que permitia que qualquer usuário consultasse o banco de dados.

Os dados pessoais sensíveis, em linhas gerais, são dados pessoais que possam trazer algum tipo de discriminação quando do seu tratamento (origem racial, convicção religiosa, opinião política, dado referente à saúde, para citar alguns exemplos) bem como, diante da sua criticidade, dados genéticos e biométricos. Ou seja, são dados pessoais que poderão implicar riscos e vulnerabilidades potencialmente mais gravosas aos direitos e liberdades fundamentais dos titulares. (Maldonado, pág. 67. 2022)

Nesse ínterim, para fins de responsabilização dos operadores de dados pessoais, Maldonado e Blum apontam que:

Prever a responsabilização e a prestação de contas como princípio demonstra a intenção da Lei em alertar os controladores e os operadores de que são eles os responsáveis pelo fiel cumprimento de todas as exigências legais para garantir todos os objetivos, fundamentos e demais princípios nela estabelecidos. E não basta somente pretender cumprir a Lei, é necessário que as medidas adotadas para tal finalidade sejam comprovadamente eficazes. Ou seja, os agentes deverão, durante todo o ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos. (Maldonado, pág. 72, 2022)

Determina a LGPD que a responsabilidade pela prestação de contas, por parte dos operadores de dados, deverá ser objetiva. Sobre o assunto, vejamos o que diz o art. 6º, inciso 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”.

Não foi o que se verificou no caso concreto, que se mostrou mais um exemplo de falha na comunicação organizacional externa (entre os titulares dos dados pessoais violados e seu operador). O Ministério da Saúde não foi claro o suficiente com os cidadãos sobre o vazamento, foi emitida apenas a seguinte nota: “os incidentes reportados estão sendo investigados para apurar a responsabilidade da exposição de base cadastral do ministério”. A pasta acrescentou também: “ações de segurança estão sendo tomadas para impedir novos incidentes, assim como ações administrativas para apurar o ocorrido”. O sistema DataSUS ficou inacessível durante todo o mês de dezembro, deixando as pessoas sem informações e de mãos atadas.

## **CONSIDERAÇÕES FINAIS**

Após vasta investigação sobre a maneira como as organizações concebem suas políticas de comunicação e como é arranjada a correlação dessas políticas à Lei Geral de Proteção de Dados (LGPD), na busca por compreender se as políticas de comunicação organizacional, no contexto empresarial brasileiro, estão em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), compreendemos que a comunicação organizacional evoluiu ao longo do tempo, passando de uma abordagem focada na produtividade para uma compreensão mais estratégica e abrangente, que reconhece a importância das relações humanas, das demandas da comunidade e das preocupações e significados das mensagens. Isso destaca a relevância crescente da comunicação organizacional no ambiente complexo e altamente competitivo das organizações, contribuindo para sua humanização e adaptação bem-sucedida aos desafios do mercado contemporâneo.

Sendo assim, no primeiro capítulo, exploramos com profundidade os direitos humanos fundamentais à intimidação e à vida privada. Como destacado por Américo Bedê Freire Júnior, a evolução desses direitos ao longo da história reflete a importância crescente da preservação da privacidade na era moderna, com destaque para o influente artigo "*Right to Privacy*" de Warren e Brandeis como um marco significativo.

Em suma, os direitos humanos fundamentais à intimidação e à vida privada constituem pilares cruciais para a preservação da dignidade, da liberdade e da autonomia dos indivíduos. Sua evolução ao longo da história reflete a crescente importância da preservação da privacidade na sociedade moderna. Esses direitos não apenas garantem que as pessoas tenham controle sobre suas informações pessoais e decisões privadas, mas também desempenham um papel crítico no mundo digital de hoje, onde a proteção da privacidade online é essencial para a confiança nas interações digitais. Portanto, a promoção e defesa desses direitos continuam sendo desafios cruciais em nossa era contemporânea, à medida que lidamos com novas tecnologias e questões complexas relacionadas à privacidade e aos dados pessoais.

No segundo capítulo, nossos esforços foram direcionados em estudar as diretrizes e regulamentos da Lei Geral de Proteção de Dados (LGPD). Trata-se de uma legislação fundamental que se concentra na proteção de dados pessoais no Brasil. Ela não abrange informações relacionadas a pessoas jurídicas, documentos

sigilosos, segredos de negócios ou outros tipos de dados não relacionados a indivíduos identificáveis.

A LGPD não faz distinção entre dados digitais e não digitais e se aplica a todas as operações de coleta e tratamento de dados pessoais, independentemente do meio utilizado ou da localização do responsável pelos dados. A razão para a criação da Lei é a proteção dos direitos humanos garantidos pela Constituição brasileira, incluindo a privacidade, a liberdade de expressão e a intimidação.

O referido diploma legal estabelece princípios fundamentais, como a preservação da privacidade e a proteção da liberdade de expressão, que devem ser respeitados por todas as entidades que lidam com dados pessoais. Isso inclui empresas que dependem do processamento de dados para a prestação de serviços, especialmente no setor de saúde, no qual a regulamentação se torna ainda mais rigorosa devido à sensibilidade dos dados envolvidos.

As empresas também devem cumprir os prazos legais para a conservação dos dados e estar preparadas para fornecer informações quando solicitadas pelo Poder Judiciário ou pelos titulares dos dados. O não cumprimento da LGPD pode resultar em diversas avaliações, desde notificações até deliberações mais diversas.

No terceiro capítulo, o tema central foi a comunicação organizacional ou empresarial. Em um panorama histórico da evolução da comunicação organizacional, torna-se evidente que este conceito não surgiu em um momento específico, mas sim evoluiu ao longo das décadas. Desde as décadas de 1920 a 1950, quando as estratégias de comunicação empresarial começaram a tomar forma, até os anos 2000, quando a comunicação organizacional se tornou planejada e estratégica, houve uma notável transformação no modo como as organizações se relacionam com seus públicos.

Inicialmente, a comunicação empresarial era vista como uma ferramenta para aumentar a produtividade, mas, ao longo do tempo, as preocupações evoluíram para incluir as relações humanas e a valorização das demandas da comunidade e da opinião pública. Esse processo culminou em uma compreensão mais abrangente da comunicação organizacional, assim, a informação deve estar em harmonia com os propósitos da organização e desempenhar um papel estratégico.

A partir dos anos 2000, a comunicação organizacional passou a ser planejada e estratégica, baseada na pesquisa dos interesses dos públicos externos para o cumprimento da missão e dos objetivos da instituição. Essa abordagem

reflete uma mudança no paradigma, acompanhando a comunicação como um processo deliberado e estratégico em oposição a uma abordagem hierárquica.

Além disso, a comunicação organizacional se ramifica em diversas modalidades, incluindo comunicação institucional, comunicação mercadológica, comunicação interna e comunicação administrativa. A comunicação integrada, que busca os objetivos da organização de maneira eficaz e harmoniosa, unindo essas modalidades, também ganhou destaque.

Embora existam diferentes abordagens para classificar a comunicação organizacional, a ênfase nas intenções, significados e efeitos das mensagens é crucial. Essa perspectiva mais sensata confirma a importância da formação de significados, informações e conhecimento no contexto da comunicação empresarial.

No quarto e último capítulo, através do breve estudo de casos, constatou-se que, de um modo geral, no contexto empresarial brasileiro, a maioria das estratégias de comunicação organizacional não estão em conformidade com as diretrizes e regulamentos da Lei Geral de Proteção de Dados (LGPD). Essa situação se intensifica quando se trata da comunicação organizacional externa, seja aquela realizada entre organizações empresariais ou entre uma empresa e seus usuários ou clientes. Percebe-se que a maioria das organizações raramente adotam políticas adequadas de reparação de danos no caso de vazamento de dados pessoais, não obstante a previsão legislativa.

A LGPD é um instrumento rico em estratégias de proteção de dados e muito abrangente. No entanto, se não for bem aplicada, não será capaz de alterar a realidade brasileira.

Na presente pesquisa, restou demonstrada a imprescindibilidade da aplicação efetiva das normas jurídicas para que estas alcancem sua finalidade específica de promover a justiça e a ordem social. Em um sistema jurídico permeado por princípios norteadores e preceitos normativos, torna-se iniludível a certeza de que a mera existência de leis, por si só, não garante a efetividade do ordenamento jurídico.

A constatação de que nenhuma lei opera de maneira eficaz sem uma aplicação judicosa e equitativa emerge como corolário inafastável do estudo desenvolvido. A legislação, por mais clara e abrangente que seja, é, em última instância, um instrumento passível de interpretação e aplicação, incumbindo aos operadores do direito a missão crucial de conferir-lhe concretude no contexto fático.

No cenário jurídico contemporâneo, marcado por desafios complexos e dinâmicas sociais multifacetadas, a aplicação da lei não deve ser encarada como um mero ato burocrático, mas sim como um exercício hermenêutico que busca atender aos anseios de uma sociedade em constante evolução. A equidade, a proporcionalidade e a celeridade processual figuram como elementos-chave na consecução desse desiderato.

Diante do exposto, conclui-se que a eficácia da LGPD, assim como a de qualquer outra legislação, está indissociavelmente ligada à habilidade e ao comprometimento dos agentes responsáveis por sua aplicação. Nesse contexto, é imperativo que os operadores do direito atuem com zelo, sensibilidade e discernimento, promovendo uma justiça que transcenda a tensão formalista, assegurando, assim, a plena realização dos valores e objetivos insculpidos no ordenamento jurídico vigente.

## REFERÊNCIAS

ABREU SOUZA, José Orbilio de. *A Comunicação como ferramenta da gestão pública: subsídios para um plano de comunicação interna da Escola Politécnica de Saúde Joaquim Venâncio*. Dissertação apresentada ao Programa de Mestrado Profissional da Pós-graduação em Saúde Pública, da Escola Nacional de Saúde Pública Sergio Arouca, Fundação Oswaldo Cruz. Rio de Janeiro, 2019.

ALVES, Fabrício da Mota. LIMA, Ana Paula Canto. *Comentários aos Regulamentos e Orientações da ANPD*. 3. Ed. Revista dos Tribunais. São Paulo, 2022.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: A Função e os Limites do Consentimento*. 3. Ed. Forense: 2021.

BITENCOURT, Roberto Cezar. *Tratado de direito penal*. 12.ed. São Paulo: Saraiva, 2012.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF: Senado Federal, 1988.

BRASIL. Lei nº 12. 965 (2014). *Marco Civil da Internet*. Brasília, DF: Senado Federal, 2014.

BRASIL. Lei nº 13.709/2018 (2018). *Lei Geral de Proteção de Dados (LGPD)*. Brasília, DF: Senado Federal, 2018.

CANUT, L. *Decisões automatizadas e o direito à explicação no regulamento geral de proteção de dados da União Europeia*. Revista de Direitos e Garantias Fundamentais, [S. I.], v. 22, n. 1, p. 101–130, 2021. DOI: 10.18759/rdgf.v22i1.1573.

CASTELLS, Manuel. trad. Roneide Venâncio Majer. 6 ed. *A sociedade em rede*. São Paulo: Paz e terra, 1999.

CORAZZA, T. A. M.; ÁVILA, G. N. de. *A proteção de dados do banco de perfil genético criminal: privacidade e liberdade versus segurança pública*. Revista de Direitos e Garantias Fundamentais, [S. I.], v. 23, n. 2, p. 243–282, 2022. DOI: 10.18759/rdgf.v23i2.1906.

CORRÊA LIMA, Manuella Dantas. PEREIRA OLIVEIRA, Maria Emilia de. *Comunicação Organizacional: Histórico, Conceitos e Dimensões*. Universidade Federal do Amazonas, Manaus, AM. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação. XIV Congresso de Ciências da Comunicação na Região Norte – Manaus - AM – 28 a 30/05/2015.

FILHO, Sérgio Cavalieri. *Programa de responsabilidade civil*. 14. ed., rev., atual. e reform. São Paulo, Atlas, 2020.

FREIRE JÚNIOR, Américo Bedê. *O conteúdo retórico do direito à privacidade e a validade da prova obtida mediante filmagens nos ambientes público e privado*. 2014. 228 f. Tese (Doutorado em Direitos e Garantias Fundamentais) - Programa de

Pós-Graduação em Direitos e Garantias Fundamentais, Faculdade de Direito de Vitória, Vitória, 2014.

KUNSCH, Margarida Maria Krohling. *A dimensão humana da comunicação organizacional*. Tradução . São Caetano do Sul: Difusão, 2010. Acesso em: 02 nov. 2023.

MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. *Lgpd - Lei Geral de Proteção de Dados Pessoais Comentada*. 4. Ed. Revista dos Tribunais. São Paulo, 2022.

MARCHIORI, Marlene. *Cultura e Comunicação Organizacional: um olhar estratégico sobre as organizações*. 2. Ed. São Caetano: Difusão Editora, 2011.

MATTOS, Fábio. *Compliance à LGPD no contexto organizacional da IMEPEL INDÚSTRIA METALÚRGICA LTDA*. Universidade Do Sul De Santa Catarina - Programa de Pós-Graduação em Administração. Santa Catarina, 2023.

MENDES, L. S.; FONSECA, G. C. S. da. *Proteção De Dados Para Além Do Consentimento: Tendências Contemporâneas De Materialização*. REI - REVISTA ESTUDOS INSTITUCIONAIS, [S. l.], v. 6, n. 2, p. 507–533, 2020. DOI: 10.21783/rei.v6i2.521.

MOREIRA, N. C. *A função simbólica dos direitos fundamentais*. Revista de Direitos e Garantias Fundamentais, [S. l.], n. 2, p. 163–192, 2007. DOI: 10.18759/rdgf.v0i2.45.

NOVELINO, Marcelo. *Direito Constitucional*. 1.ed. São Paulo, Método, 2. ed. 2012

OLIVEIRA, I. & PAULA, Carine F. (2007). *O que é comunicação estratégica nas organizações*. São Paulo: Paulus.

OPICE BLUM, Bruno e Vainzof Advogados Associados. *Como identificar e reagir a incidentes de segurança*. Mar. 2021. p. 12. Disponível em: <https://opiceblum.com.br/wp-content/uploads/2021/02/Cartilha-Como-identificar-e-reagir-a-incidentes-de-seguranca.pdf>.

PAULRAJ, A. Lado, A. A. e CHEN, I. J. (2008). *Inter-organizational communication as a relational competency: Antecedents and performance outcomes in collaborative buyer– supplier relationships*. Journal of Operations Management, 26, 45–64.

PIOVESAN, Flávia. *Direitos Humanos e o Direito Constitucional Internacional*. 14. ed. São Paulo: Saraiva, 2012.

P. R. A. de Azevedo e P. M. de C. Cabacinha, *Proteção multinível dos direitos humanos: lógica monista ou dualista do direito?*, *Rev. Dir. e Garantias Fundamentais*, vol. 22, nº 1, p. 11–36, dez. 2021.

Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation) 2016/679.

SÁ MARTINO, L. M.; SALGUEIRO MARQUES, A. C. *Vulnerabilidades, visibilidades e insurgências dos sujeitos em organizações no ambiente das mídias digitais: um estudo exploratório*. PAULUS: Revista de Comunicação da FAPCOM, [S. l.], v. 6, n. 12, 2023. DOI: 10.31657/rcp.v6i12.612.

STANLEY, Deezt. Comunicação organizacional: fundamentos e desafios. In: MARCHIORI, Marlene. *Comunicação e organização: reflexões, processos e práticas*. São Caetano do Sul, SP: Difusão editora 2010.