UNIVERSIDADE DE CAXIAS DO SUL
CAMPUS UNIVERSITÁRIO DA REGIÃO DAS HORTÊNSIAS
ÁREA DE CONHECIMENTO CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

VITÓRIA ESTEFÂNIA DOS SANTOS HERMÓGENES

RESPONSABILIDADES DO INBOUND MARKETING À LUZ DA LGPD: LIMIAR ENTRE CONVENIÊNCIA E ABUSO DO USO DE DADOS PESSOAIS

CANELA
2023

VITÓRIA ESTEFÂNIA DOS SANTOS HERMÓGENES

RESPONSABILIDADES DO INBOUND MARKETING À LUZ DA LGPD: LIMIAR ENTRE CONVENIÊNCIA E ABUSO DO USO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado no Curso de Direito da Universidade de Caxias do Sul, Campus Universitário da Região das Hortênsias, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador Prof. Me. Luiz Fernando Castilhos Silveira

CANELA
2023

VITÓRIA ESTEFÂNIA DOS SANTOS HERMÓGENES

RESPONSABILIDADES DO INBOUND MARKETING À LUZ DA LGPD: LIMIAR ENTRE CONVENIÊNCIA E ABUSO DO USO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso apresentado no Curso de Direito da Universidade de Caxias do Sul, Campus Universitário da Região das Hortênsias, como requisito parcial à obtenção do título de Bacharel em Direito.

Aprovado em: 10 de julho de 2023.

Banca examinadora composta por:

_____
Prof. Me. Luiz Fernando Castilhos Silveira (Orientador)
Universidade de Caxias do Sul – UCS

_____
Profª. Me. Daniela de Oliveira Miranda (Avaliadora)
Universidade de Caxias do Sul – UCS

_____
Prof. Me. Moisés João Rech (Avaliador)
Universidade de Caxias do Sul – UCS

Dedico este trabalho ao meu pai *(in memoriam)*, um empresário visionário e inspirador. Tenho certeza de que ele apreciaria imensamente as informações e conhecimentos aqui apresentados.

AGRADECIMENTOS

Gostaria de agradecer ao meu marido, meu maior companheiro de vida, meu melhor amigo e mentor. Sua presença constante, debates interessantes sobre o tema deste trabalho e apoio incondicional foram essenciais para superar os momentos de insegurança ao longo desse processo. Sua dedicação em me inspirar e encorajar foi fundamental para o sucesso deste trabalho.

Também quero estender um agradecimento especial ao professor Luiz Fernando, meu orientador, pela sua paciência, orientação e flexibilidade ao longo de todo o percurso. Sua experiência e conhecimento foram de imenso valor, e sou grata por ter tido a oportunidade de aprender. Sua orientação foi fundamental para desenvolver, moldar e aprimorar minha pesquisa.

A família Michaelsen, meus empregadores, que através da experiência prática possibilitaram que eu exercesse os aprendizados acadêmicos. E por meio do trabalho possibilitaram que eu realizasse este sonho.

Não posso deixar de mencionar meus amigos, que estiveram ao meu lado durante todo o processo. Todo o apoio e compreensão foram essenciais para minha dedicação e foco na conclusão desta etapa importante da minha jornada acadêmica.

Por fim, quero expressar minha gratidão a todos aqueles que, de alguma forma, contribuíram para a elaboração deste trabalho. Seja por meio de discussões enriquecedoras, sugestões valiosas ou simplesmente palavras de encorajamento, cada um desempenhou um papel importante em minha jornada acadêmica e realização pessoal.

Os dados são o novo petróleo. Protegê-los é tão importante quanto explorá-los.

Clive Humby

RESUMO

A Lei Geral de Proteção de Dados (LGPD) surgiu visando à proteção de milhões de brasileiros que ao acessarem a internet diariamente, compartilhavam tacitamente suas informações com diversas empresas de *e-commerce*. Nesse contexto, esta pesquisa buscou demarcar os limites inerentes à coleta e uso destes dados pessoais na estratégia de marketing denominada *inbound marketing*, frente à conveniência que o usuário busca ao ceder informações. Para isso, foi analisado o atual cenário das campanhas de marketing, com um breve apanhado histórico, visando apontar a mudança de visão que passou a valorizar a informação pessoal do usuário como um elemento primordial para o sucesso de qualquer empresa de e-commerce, criando assim, um novo *commodity*. Lembrando do impacto da pandemia na migração de milhares empresas para o cenário online, muitas vezes sem conhecimento das implicações jurídicas que campanhas mal elaboradas de coletas de dados podem acarretar. Ademais, foram analisados os meios utilizados para coleta e armazenamento, observando a garantia de uma proteção das informações coletadas, pessoais ou sensíveis, por meio de regularização de acesso e encriptação os tornando não identificáveis. Entrou-se assim no mérito dos incontáveis métodos de armazenamentos de dados existentes, e seus administradores. Por fim, abordou-se a responsabilidade civil pelo mau uso, doloso ou culposo da manutenção e vazamento de dados. E suas implicações jurídicas, passíveis de indenização ao consumidor. Nessa assertiva, o principal objetivo do presente trabalho é apontar as possíveis vantagens e desvantagens na cedência de dados através das chamadas campanhas de inbound marketing das empresas de e-commerce. Ponderando que a cedência de informações pode gerar maior facilidade para encontrar o que se procura online, assim como vantagens financeiras no momento da aquisição. Avaliando os riscos envolvidos na realização dessa concessão, assim como os vínculos obrigacionais e implicações legais à luz do ordenamento jurídico. Em contrapartida, apontar a forma adequada que as empresas de e-commerce podem seguir utilizando o tal método. Podendo gerar resultado positivo na interação usuário x empresa no âmbito do e-commerce. Constatou-se, por meio de pesquisa bibliográfica e método hipotético dedutivo, parcialmente indutivo, que apesar dos pressupostos do Código Civil e o Código de Defesa do consumidor, o advento da Lei Geral de Proteção de Dados (LGPD) tornou o fator punibilidade pelas infrações no quesito limites da tutela sobre dados pessoais mais claras. Assim como a obrigatoriedade da anuência do usuário, direcionou o olhar do cliente aos não tão evidentes desvios de finalidades aos quais suas informações são submetidas para questionáveis fins. Todavia, apesar da segurança jurídica existente, ainda são inúmeros os problemas enfrentados diante a série de escândalos envolvendo vazamentos, compartilhamentos, manipulação, vendas e acessos não autorizados a estes bancos de dados. Além disso, em face da massiva utilização do método de inbound marketing, a fiscalização individualizada torna-se inviável. A ponto de diversas denúncias partirem de usuários, iniciando uma era de cooperação em que a internet perde o estigma de “terra-sem-lei” evidenciando assim para a ciência jurídica a importância deste tema.

Palavras-chave: LGPD, Inbound Marketing, Segurança Jurídica, e-commerce, banco de dados.

ABSTRACT

The General Data Protection Law (LGPD) emerged with the aim of protecting millions of Brazilians who, by accessing the internet daily, tacitly shared their information with several e-commerce companies. In this context, this research sought to demarcate the inherent limits of collecting and using this personal data in the marketing strategy called inbound marketing, in the face of the convenience that the user seeks when sharing information. To do so, the current scenario of proposed marketing campaigns was analyzed, with a brief historical overview, aiming to point out the shift in perspective that now values user personal information as a fundamental element for the success of any e-commerce company, creating a new commodity. Taking into account the impact of the pandemic on the migration of thousands of companies to the online scenario, often without knowledge of the legal implications that poorly designed data collection campaigns can entail, this research also analyzed the means used for data collection and storage, observing the guarantee of protection of collected personal or sensitive information through regulation of access and encryption that makes them unidentifiable. The countless existing methods of data storage and their administrators were also addressed. Finally, the civil liability for the misuse, intentional or negligent, of data maintenance and leakage was examined, as well as its legal implications, which may result in consumer compensation. The main objective of this paper is to point out the possible advantages and disadvantages of providing data through inbound marketing campaigns by e-commerce companies, considering that sharing information can generate greater ease in finding what is sought online, as well as financial advantages at the time of acquisition. It also evaluates the risks involved in making this concession, as well as the legal obligations and implications in light of the legal system. In contrast, it points out the appropriate way that e-commerce companies can follow using this method, which can generate positive results in the user-company interaction in the e-commerce context. Through bibliographic research and hypothetical-deductive, partially inductive method, it was found that despite the assumptions of the Civil Code and the Consumer Protection Code, the advent of the LGPD made the punishability factor for infractions in terms of the limits of protection of personal data clearer. The user's mandatory agreement also directed the customer's attention to the not-so-evident deviations of purposes to which their information is subjected for questionable ends. However, despite existing legal security, there are still numerous problems faced in the face of a series of scandals involving leaks, sharing, manipulation, sales, and unauthorized access to these databases. In addition, in the face of the massive use of the inbound marketing method, individualized supervision becomes unfeasible, to the point that many complaints come from users, starting an era of cooperation in which the internet loses the stigma of a "lawless land," thus highlighting the importance of this topic for legal science.

Keywords: LGPD, Inbound Marketing, Legal Security, e-commerce, database.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Vivemos em um novo cenário digital onde com a transformação tecnológica e social, encontramos incontáveis empresas que buscam vender seus produtos e serviços online[1]. Tendo em vista as diversas interações, seja nas redes sociais, locomoções por aplicativos, pesquisas, gostos, hábitos, comportamentos, imagens, atividades, contatos, etc. Tudo é registrado e pode ser convertido em potenciais dados, para serem armazenados e explorados. O marketing digital está em constante evolução, com novas tecnologias e tendências surgindo a todo momento. As empresas que não acompanham as mudanças e inovações no marketing digital correm o risco de perder competitividade e relevância no mercado. Para isso, uma nova metodologia de marketing domina grande parte das campanhas em sites da web. O Marketing de inbound busca tornar próximos: o cliente e sua necessidade, da resposta somada a uma oferta.

Por meio desta forma de captação de clientes, dados são obtidos cujo, inseridos no panorama econômico atual, possuem alto valor agregado. Quando organizados em uma base de dados podem: identificar, nomear e estabelecer forma de contato entre provável comprador e uma determinada oferta. Estas informações sobre as pessoas têm se transformado numa espécie de commodity, com uma vantagem: não se esgotam quando consumidos, pelo contrário, podem gerar valor exponencialmente.

Diante desta realidade, surgem muitos desafios para o sistema jurídico brasileiro, cada vez mais complexos e presentes na nova sociedade, a qual os direitos precisam estar alinhados; da liberdade dos indivíduos nas relações comerciais, até a privacidade fundamentalmente garantida. Para lidar com esse desafio, as empresas precisam adotar práticas de segurança de dados rigorosas e transparentes, que garantam a proteção e a privacidade dos dados pessoais dos consumidores. Além disso, é importante estabelecer um relacionamento de confiança com os consumidores, demonstrando transparência e ética na coleta e uso de dados.

---

[1]THE GLOBAL PAYMENTS REPORT. **Previsões de crescimento do e-commerce.** [Online]. Disponível em: https://proximonivel.embratel.com.br/estudo-aponta-crescimento-de-55-no-e-commerce-global-ate-2025/. Acesso em: jun. 2022.

A Lei Geral de Proteção de Dados busca, entre outras funções, regulamentar até onde poderá ser utilizada determinada informação fornecida. Recentemente as empresas se viram obrigadas a obter anuência dos usuários em relação às informações que constam e/ou passarão a constar em seus históricos. Este cuidado é ainda maior quando ainda não foi estabelecido o vínculo: Fornecedor e Cliente. Pois em muitas campanhas veiculadas, ocorre tráfego de informações, sem necessariamente uma contraprestação por meio de pagamento. Assim passa a ser tutelado, para onde essas informações vão e ficam ao longo do tempo, e quais as naturezas, as finalidades e os métodos de proteção a seu acesso.

Inicialmente abordaremos a evolução do marketing, e a mudança de visão e estratégia do novo mercado. Pelo aumento da oferta e demanda em determinados períodos e revoluções históricas, passou a ser necessário uma forma de aumentar a receita, diferenciado-se da concorrência, criando um relacionamento com o consumidor. Passando a comunicar-se e entender quem precisa de quê, e ainda o que poderá vir a precisar.

Surge então a estratégia revolucionária do *inbound marketing*. Que rompe com décadas de campanhas publicitárias invasivas e investimentos perdidos em anúncios online muitas vezes ignorados ou bloqueados pelas novas tecnologias de "*ad-blocks*". O *inbound marketing* busca a atração de clientes oferecendo exatamente o que eles precisam, quase como uma fórmula mágica, com soluções explicadas em blogs, e-books, cupons de desconto, etc. Em contrapartida o cliente, cativado precisa apenas informar alguns dados.

A tutela destes dados, como foco do estudo, trará medidas que passaram a ser discutidas (Leis setoriais) até o advento da LGPD- Lei Geral de Proteção de Dados. Com o êxodo das empresas para o ambiente online, ainda mais necessário após a pandemia do COVID-19, muitas lojas de e-commerce passaram a coletar dados, buscando aumentar suas vendas, sem atentar-se à obrigação implícita de protegê-los. Outros como nicho de mercado, entenderam que estes "*leads* qualificados" tem muito valor agregado, pois traçam um perfil de consumidor, podendo inclusive ser comercializados. Gerando preocupações a respeito de segurança de banco de dados (Big Data) onde ficam armazenados estes perfis, assim como questionamentos sobre quem detém este acesso.

No tópico da segurança jurídica será mencionado o risco de incidentes e suas penalidades. Por fim algumas sugestões de adequações se fazem necessárias, para uma administração de dados saudável e legal no *inbound marketing*.

2 EVOLUÇÃO DO MARKETING

Apesar da palavra Marketing ter sua derivação do latim ‘’*mercare*’’ termo utilizado para os atos comerciais na Roma Antiga, foi na década de 40 que a prática específica do Marketing começou a surgir como um modelo de coordenação entre a manufatura e o comércio. Com o intuito de fomentação de vendas, tendo em vista que nos séculos passados “o importante era produzir; produzir com o menor custo possível, pois tudo o que fosse produzido era consumido”[2]

Com o desenvolvimento da economia de mercado no século XVI, seja vendedor ou comprador, o comportamento humano passou a ter maior relevância, tornando-se determinante nas relações sociais e econômicas[3]. Seguindo, no séc.XVII o êxodo da sociedade rural, para uma sociedade urbana e trabalhadora assalariada, foi o aspecto modificador muito importante da Revolução Industrial para a transformação social[4].

O Marketing nasce no início do século XX[5], quando a economia de mercado foi disseminada no ocidente. Transformando para sempre as relações sociais por conta da autonomia econômica e das leis de mercado.

Outros marcos importantes na evolução do Marketing foram: surgimento do especialista de mercado[6] e a elaboração de materiais de propaganda e brochuras como ‘’estimulação da demanda’’[7].

A abordagem do desenvolvimento de marketing é segmentado em três ‘’eras’’[8] Com enfoques diferentes, sendo: Era da produção, caracterizada pela demanda maior que a oferta; Em 1930 a era de Vendas, por conta do excesso de produção, iniciaram os primeiros sinais de excesso de oferta. Técnicas de vendas agressivas, que buscavam liquidar os estoques; Por fim, a era do Marketing, em

---

[2] ROCHA, Edison; CHRISTENSEN, Clayton M. A. **Marketing, Teoria e prática no Brasil.** 2. Ed. São Paulo: Atlas, 1999. e-book.
[3] BARTELS, Robert. **Consumers in capitalism, past and present: consumer research, corporate strategy, and social policy in historical perspective**. Journal of Consumer Research, v. 2, n. 2, p. 155-167, 1976.
[4] CANEDO,Letícia Bicalho. **Revolução Industrial e trabalho**. In: SAVIANI, D. et al. História da sociedade brasileira. Campinas: Autores Associados, 1998. p. 149-165.
[5] CHAUVEL, Marie Agnes. (2000). **Consumidores insatisfeitos: uma oportunidade para as empresas.** Rio de Janeiro: Mauad. e-book.
[6] AMBLER, Tim. **Marketing and the bottom line: getting to ROI.** Marketing Intelligence & Planning, v. 22, n. 7, p. 723-739, 2004.
[7] WEBSTER, Frederick. E. **A perspective on the evolution of marketing management.** Journal of Public Policy & Marketing, v. 21, n. 2, p. 239-244, 2002.
[8] LAS CASAS, Alexandre Las. **Marketing: conceitos, exercícios e casos.** São Paulo: Atlas, 2001. p. 18.

1950, caracterizada pela assimilação das empresas na correta administração de manutenção e conquista de negócios. Com enfoque na valorização da clientela e busca da relação permanente.[9]

Por fim, foi nos anos 90 o avanço da tecnologia causou uma revolução no marketing, o *cybermarketing*:

> O CRM (Customer Relationship Management) e os serviços de atendimento ao consumidor, entre outras inovações, tornaram possível **uma gestão em larga escala do relacionamento com os clientes**. E, como se isso não fosse suficiente, a Internet chegou como uma nova via de comunicação. [...] Ou seja, esta época caracterizou-se por uma constante busca pela **personalização em massa.**[10] (grifo nosso)

Ao longo das décadas, ficou evidente que a internet, fator fundamental da globalização, também tornou-se elemento essencial para o crescimento das empresas. A necessidade da presença digital das marcas, aumentou a área de atuação do marketing tradicional, assim como o alcance das informações propagadas.

Atualmente estima-se que 5,3 bilhões de pessoas estejam conectadas à internet. Assim como a projeção é que este gráfico siga crescente.

> A União Internacional de Telecomunicações (ITU) estima que aproximadamente 5,3 bilhões de pessoas - ou 66% da população mundial - estejam usando a Internet em 2022. Isso representa um aumento de 24% desde 2019, com 1,1 bilhão de pessoas estimadas terem se conectado nesse período.[..][11]

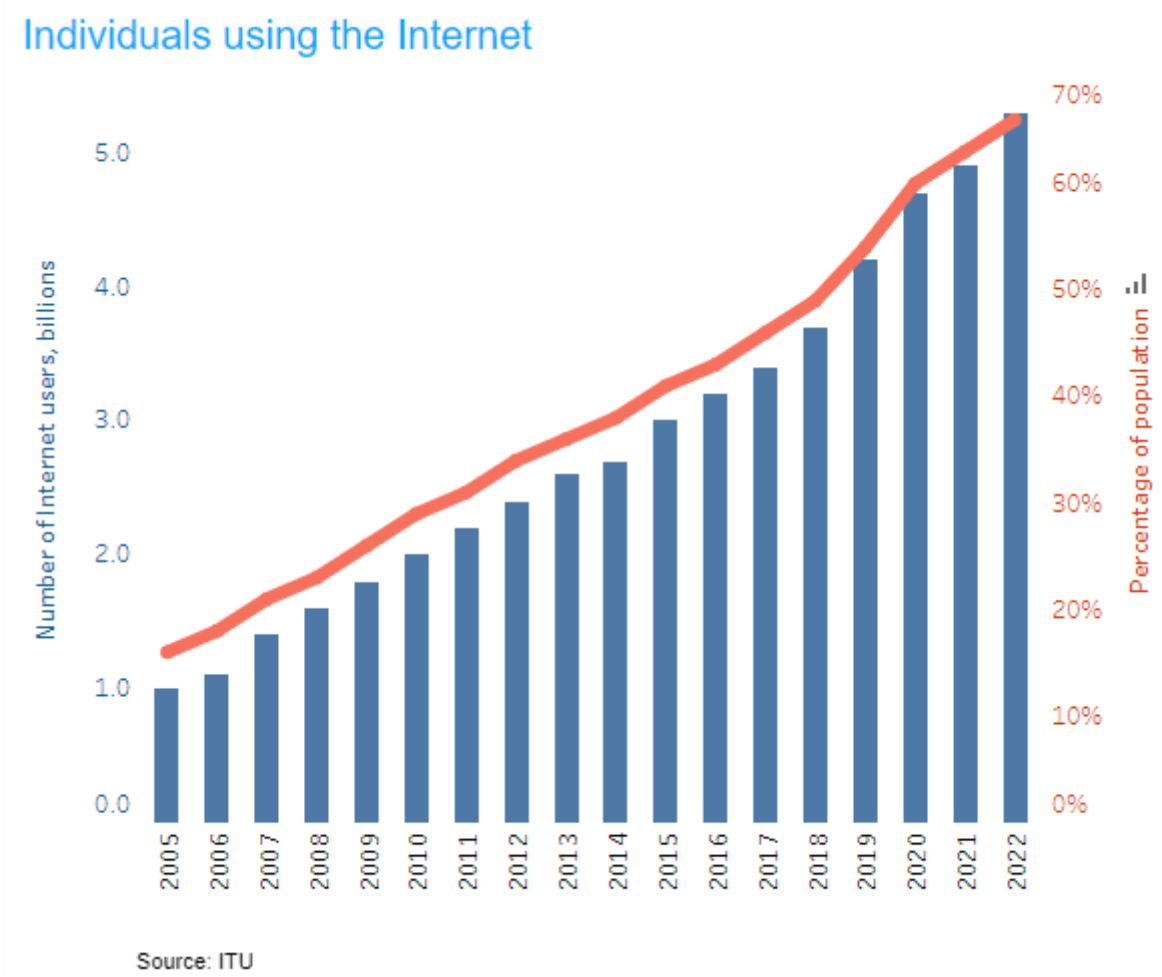
---

[9] ROCHA, Angela. CHRISTENSEN, Carl., **Marketing, Teoria e prática no Brasil.** 2. Ed. São Paulo: Atlas, 1999.p 55.

[10] SANTOS, João Manuel dos; LIMA, Dulce Silva.;BRUNETTA, Luiz Fernando. **Marketing digital: conceitos, estratégias e práticas.** São Paulo: Atlas, 2009. p. 42.

[11] ITU estimates that approximately 5.3 billion people – or 66 per cent of the world's population – are using the Internet in 2022. This represents an increase of 24 per cent since 2019, with 1.1 billion people estimated to have come online during that period. However, this leaves 2.7 billion people still offline. Fonte: ITU. **International Telecommunication Union. Estatísticas da UIT.** Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Acesso em: 05 mai. 2023.

Figura 1 - Indivíduos usando a Internet



Fonte: ITU[12]

Evidenciando o poder de alcance da comunicação das campanhas de marketing digital. Resumindo, a evolução do marketing se dá pelas seguintes classificações: a) Marketing 1.0 ou Marketing orientado ao produto; b) Marketing 2.0 ou Marketing voltado ao consumidor; c) Marketing 3.0 ou Marketing centrado em valores; e d) Marketing 4.0 ou Marketing Digital.[13]

Ao longo deste estudo, vamos constatar que com a inclusão digital e a enxurrada de publicidade neste meio, os usuários passaram a filtrar seletivamente o conteúdo recebido. Reduzindo a efetividade do ‘’marketing viral’’ e abrindo espaço para o conteúdo personalizado com base em análise de dados.

> Quanto mais sociais somos, mais queremos coisas feitas sob medida para nós. Respaldados pela análise de big data (coleta,

[12] Ibid.,
[13] KOTLER, Philip et al. Marketing 4.0. Rio de Janeiro: Sextante, 2017. 1 recurso eletrônico. Tradução de Ivo Korytowski. e-book. p. 21-31.

> processamento e análise de megadados), os produtos tornam-se mais personalizados e os serviços, mais pessoais. Na economia digital, o segredo é alavancar esses paradoxos, [14]

De acordo com um estudo, a utilização excessiva da publicidade na internet e a saturação de conteúdo reduziram o interesse do público e aumentaram a necessidade de conteúdo personalizado para captar a atenção do usuário.

> Os consumidores digitais têm mais poder e controle do que nunca. Eles podem acessar informações facilmente, comparar produtos, ler avaliações e compartilhar suas experiências com amigos e familiares. Eles filtram seletivamente o que querem e o que não querem ver, e isso reduziu a efetividade do 'marketing viral'. Em vez disso, as marcas precisam oferecer conteúdo personalizado e relevante com base em análise de dados[15]

Também ressalta que a análise de dados se tornou uma ferramenta indispensável para entender as preferências do público-alvo e, assim, criar campanhas personalizadas e mais efetivas. Isso é especialmente importante em um cenário onde os usuários têm a capacidade de escolher o que consomem e o que ignoram.

2.1 Marketing Digital

É notável que todas as empresas iniciaram a corrida na busca por presença e relevância no ambiente virtual. Desta forma, passaram a estudar e utilizar um conjunto de estratégias de anúncio e vendas.

> O atual cenário globalizado possibilitou a mutabilidade de conceitos, valores e negócios numa velocidade ímpar. Desse modo, as mudanças no cenário corporativo vão desde o ingresso de novas tecnologias em vários segmentos até a alteração dos hábitos de consumo da sociedade. O fenômeno da tecnologia colaborou para possíveis modificações na mentalidade de empreendedores, executivos e profissionais em geral.[16]

---

[14] KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. **Marketing 4.0: do tradicional ao digital.** Editora Sextante, 2017.
[15] KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. op. cit., p. 22.
[16] ALMEIDA, G. A. **O uso das tecnologias de informação e comunicação como vantagem competitiva no contexto empresarial**. Revista Científica Visão Acadêmica, v. 18, n. 2, p. 13-28, 2017.

No marketing tradicional uma das estratégias mais utilizadas busca interromper clientes em potencial nas suas atividades diárias, expondo a oferta de forma massiva e chamativa, seja ao vivo através de propagandas de TV, rádio, cartazes, outdoors, telemarketing, carros de som, ou no ambiente digital com pop ups, propagandas em vídeos, em jogos, promoções no canto do site piscando, tudo com o objetivo de atrair a atenção e levar passivamente o cliente a compra.

> Nesse contexto, as marcas não deveriam mais ver os consumidores como meros alvos. No passado, era comum as empresas transmitirem sua mensagem por diferentes mídias publicitárias. Algumas até inventaram uma diferenciação pouco autêntica para poder se destacar da multidão e dar respaldo à imagem de sua marca. Com isso, a marca costuma ser tratada como uma embalagem externa, permitindo uma representação falsa de seu verdadeiro valor. Essa abordagem não será mais eficaz, porque, com a ajuda de suas comunidades, os consumidores se defendem das marcas ruins das quais são alvos.[17]

Essa estratégia de marketing ficou conhecida como ‘’outbound marketing’’ ainda utilizado atualmente em meios digitais associado com análise de perfil, através principalmente, de cookies, para coletar informações sobre os usuários com fins de publicidade.

Uma definição clara de cookie:

> Cookies são pequenas estruturas de dados enviadas de um servidor Web para o seu navegador e salvas em seu disco rígido em um arquivo de texto. Eles nada mais são do que uma sequência de caracteres (letras e números) que armazenam certas informações sobre você.[18] (tradução nossa)

Os cookies são importantes para o comércio eletrônico de empresas e agências de marketing e publicidade. Existe algo chamado segmentação comportamental que usa informações veiculadas por meio de cookies para criar um perfil de usuário gerando assim um ‘’alvo-comportamental’’ [19].

O usuário é combinado com um perfil amplo, e passa a receber anúncios

---

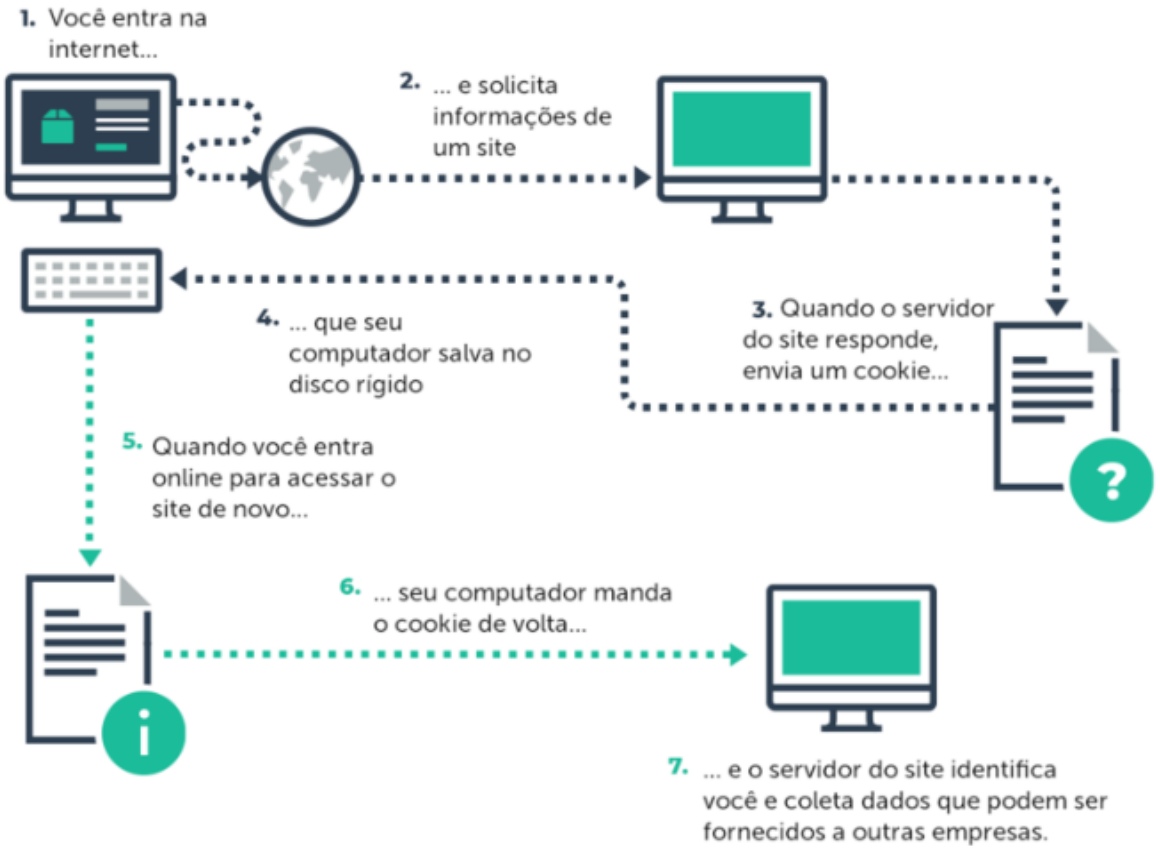
[17] KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. **Marketing 4.0: do tradicional ao digital.** Rio de Janeiro: Sextante, 2017. p. 56.

[18] Cookies are small data structures sent from a Web server to your browser and saved on your hard drive in a text file. They are nothing more than a string of characters (letters and numbers) that store certain pieces of information about you. Fonte: PETERS, Richard; SIKORSKI, Robert (1997), "**Cookie Monster?**", Science, Vol. 278, pp. 1486-7

[19] BORGESIUS, Frederik. 2016. **Online Tracking and Consumer Privacy.** Edward Elgar Publishing. p. 97.

que podem interessá-los, mas isso tem implicações muito sérias na opinião do indivíduo sobre o ambiente online, privacidade e segurança de dados pessoais. A privacidade é a preocupação mais importante, embora cookies não podem danificar o computador como vírus, estes dados de ‘’perfil’’ ficam armazenados no disco rígido para posteriormente se comunicarem com determinada página na web.

Figura 2 - Armazenamento de Cookie



Fonte: Hauk (2022)[20]

Por conta disso, as pessoas têm bloqueado, tanto os cookies quanto propagandas massivas na internet (spam), buscando o fim da comunicação desautorizada. Com a utilização do ad blockings, tanto o consumidor não recebe a mensagem, quanto a publicidade não cumpre seu papel, causando significativa perda na receita de campanhas. A respeito dos softwares de ad blocking:

> Em fevereiro de 2017, um relatório global destacou o crescimento da adesão a esses softwares: em sete anos, o número de usuários no

[20] HAUK, Chris, **Browser Fingerprinting: What Is It And What Should You Do About It?** 2022. Disponível em: <https://pixelprivacy.com/resources/browser-fingerprinting/> Acesso em: 7 jun. 2022.

> mundo aumentou mais de 29 vezes, pulando de 21 milhões, em 2010, para 615 milhões, em 2017, abarcando 11% do total de usuários de internet no planeta (PageFair, 2017). A perda de receita publicitária anual decorrente do uso de bloqueadores foi estimada em US$ 21.8 bilhões em 2015, o equivalente a 14% dos investimentos globais em publicidade daquele ano (PageFair & Adobe, 2015).[21]

Quanto aos anúncios na internet, dentre as razões para o distanciamento[22], esta a recepção dos anúncios como um obstáculo ao objetivo de navegar na internet, o excesso de publicidade e experiências negativas, relacionadas aos descontentamentos gerados pela visualização desses tipos de anúncios no passado.

Sem desconsiderar a forma tradicional de marketing, pois ainda tem seu lugar no ambiente moderno, há outra forma de comunicação com compradores em potencial.

> Começamos a falar sobre essa transformação na forma como as pessoas compram e adquirem. Chamamos os métodos tradicionais e interruptivos de “outbound marketing”, porque eles eram fundamentalmente sobre divulgar uma mensagem e começamos a chamar a nova maneira de “inbound marketing”. Inbound foi sobre atrair as pessoas compartilhando informações relevantes, criando conteúdo útil e geralmente buscando ajudar.(tradução nossa)[23]

Por conta da ineficácia crescente do *outbound marketing*, os operadores de marketing têm adotado uma nova técnica, que ao invés de "empurrar" conteúdo tem “puxado” quem tenha interesse nele. Com este interesse gerado, surge a permissão, que garantirá o contato com este indivíduo cujo a intenção de compra no que foi anunciado passa a ser genuína e expressa.

2.2 Inbound Marketing

Enquanto o velho marketing utilizava técnicas que ‘’empurravam’’ produtos e/ou serviços para os clientes, o novo marketing se baseia em ganhar o interesse

---

[21] ERBISTI, Marcos; SUAREZ, Maribel Carvalho. **Ad Blocking: Discursos de Adoção e de Anticonsumo da Publicidade. Revista de Administração de Empresas**, São Paulo, v. 59, n. 3, p. 227-238, jun. 2019. Disponível em: <https://www.scielo.br/j/rae/a/dnbzhY8bZdyvjKzJTW5pNzR/?lang=pt>. Acesso em: 01 jun. 2019.

[22] CHO, Chang-Hoan.; CHEON, Hongsik. **Why do people avoid advertising on the internet?** Journal of Advertising, v. 33, n. 4, 2004. DOI: 10.1080/00913367.2004.10639175.

[23] We started talking about this transformation in how people shop and buy. We called the traditional, interruptive methods “outbound marketing,” because they were fundamentally about pushing a message out, and started calling the new way “inbound marketing.” Inbound was about pulling people in by sharing relevant information, creating useful content, and generally being helpful. Fonte: HALLIGAN, Brian; SHAH, Dharmesh. **Inbound marketing: Get found using Google, social media, and blogs**. John Wiley & Sons, 2009, não paginado.

das pessoas em vez de comprá-los, *''marketing de atração"*.

> Podemos definir o Inbound Marketing como qualquer tática de marketing digital cujo objetivo é alcançar e ganhar clientes por meio da oferta de conteúdo que ele precisa e quer receber. Trata-se, portanto, de uma mudança de atitude em relação à abordagem ao cliente.
> Mas essa mudança não se deu do dia para a noite, e sim de maneira processual. E justamente por se configurar como uma mudança gradativa, não podemos precisar uma data de surgimento do Inbound Marketing, mas a criação da Hubspot, em 2006, por Brian Halligan e Dharmesh Shah, nos Estados Unidos, é considerada o marco inicial dessa estratégia. Já no Brasil, os registros de uso de Inbound Marketing começam a aparecer por volta de 2010. [24]

A estratégia do *inbound marketing* é atrair o público alvo e potenciais compradores, através de desenvolvimento e criação de conteúdo informativo, como artigos de blog, ofertas de conteúdo e mídias sociais, que agreguem valor. Os exemplos incluem guias sobre como usar os produtos, *ebooks*, informações sobre uma suposta solução que pode resolver os desafios ou desconfortos e ainda depoimentos de clientes e detalhes sobre promoções ou descontos.

> ''Em suma, o trabalho do marketing é converter as necessidades em constante mudança das pessoas, em oportunidades lucrativas. O objetivo do marketing é criar valor oferecendo soluções superiores, economizando tempo e esforço de busca e transação de compradores e entregando a toda a sociedade um padrão de vida mais alto. A prática de marketing hoje deve ir além da fixação em transações que muitas vezes levam a uma venda hoje e a um cliente perdido amanhã. O objetivo do profissional de marketing é construir um relacionamento de longo prazo mutuamente lucrativo com seus clientes, não apenas vender um produto. Uma empresa não vale mais do que o valor vitalício de seus clientes. Isso exige conhecer seus clientes o suficiente para fornecer ofertas, serviços e mensagens relevantes e oportunos que atendam às suas necessidades individuais. ''[25](tradução nossa)

---

[24] DUARTE, Juliano Franco. **O livro proibido do marketing: Inbound Marketing, Marketing de Conteúdo e Hacks para sua empresa crescer**. Edição do Kindle. 2020.

[25] In short, marketing's job is to convert people's changing needs into profitable opportunities. Marketing's aim is to create value by offering superior solutions, saving buyer search and transaction time and effort, and delivering to the whole society a higher standard of living. Marketing practice today must go beyond a fixation on transactions that often leads to a sale today and a lost customer tomorrow. The marketer's goal is to build a mutually profitable long-term relationship with its customers, not just sell a product. A business is worth no more than the lifetime value of its customers. This calls for knowing your customers well enough to deliver relevant and timely offers, services, and messages that meet their individual needs. Fonte: KOTLER, Philip. **Marketing Insights from A to Z: 80 Concepts Every Manager Needs to Know.** 2003. e-book. p. 13.

O *cookie* no *outbound marketing* leva informações mais simples, de preferência do usuário, sem necessariamente carregar informações pessoais. Por exemplo, uma visita em um site ou busca por um item. Os cookies são utilizados em ambos os tipos de marketing *(outbound e inbound)*[26] para rastrear o comportamento do usuário na internet e oferecer publicidade personalizada.

Agora o *cookie*, tem papel fundamental no *marketing inbound*, tornando o usuário identificado ou identificável. Pois, havendo um cadastro de, por exemplo: nome, telefone e e-mail. Ocorrerá identificação, caracterizando trânsito de dado pessoal que poderá ser carregado por um cookie a fim de armazenamento em banco de dados e contato posterior.

Os clientes atraídos, passam por um ‘’funil de vendas’’ se transformando em *leads*, que por sua vez geram armazenamento de dados pessoais. Conforme figura 3. Haja vista que, antes da LGPD o acesso, manutenção e compartilhamento dos *leads* contidos neste ‘’funil de vendas’’ não costumava ser supervisionado, gerando em alguns casos vazamentos, comercialização e até roubo dessas informações.

2.3 Funil De Vendas

O funil de vendas é um padrão estratégico dividido por estágios, estruturado visualmente, demonstrando a jornada de compra de um cliente captado através de uma campanha de *inbound marketing*.

De acordo com os fundadores da *hubspot* e precursores do *inbound marketing* Brian Halligan e Dharmesh Shah, o funil de vendas é uma ferramenta crucial para a estratégia essa estratégia, pois ajuda a acompanhar o processo de compra do cliente desde o momento em que ele se torna um visitante até a sua conversão em cliente efetivo. Ainda segundo os autores, "o funil de vendas é composto por três etapas: topo do funil (ToFu), meio do funil (MoFu) e fundo do funil (BoFu), representando as diferentes fases da jornada de compra do cliente" [27]

O ToFu, ou topo do funil, é a fase em que o cliente ainda está conhecendo a marca e os seus produtos ou serviços. Já o MoFu, ou meio do funil, é a etapa em que o cliente já reconheceu uma necessidade e está considerando diferentes

---

[26] GABRIEL, Martha; KISO, Rafael. (2010). **Marketing na Era Digital: Conceitos, plataformas e estratégias**. Novatec Editora. Página 174.
[27] HALLIGAN, B. SHAH, D. **Inbound marketing: Get found using Google, social media, and blogs.** John Wiley & Sons, 2009, não paginado.

opções de compra. Por fim, o BoFu, ou fundo do funil, é a fase em que o cliente está pronto para tomar uma decisão de compra e se tornar um cliente efetivo da marca. A estratégia de inbound marketing visa conduzir o cliente de forma eficiente por cada uma dessas etapas até a conversão em venda.

Figura 3 - Funil de Vendas

Fonte: Marques e Levi (2020).[28]

Neste acompanhamento é comum que haja interação entre empresa x visitante, pois ao passo que o visitante busca a solução oferecida pela empresa, o mesmo precisa conceder informações, dados pessoais, em troca. Assim passando à lead a empresa estabelece primeiramente uma comunicação com o cliente.

A possibilidade de personalização dos meios digitais acessados pelo consumidor, faz com que essa troca possa vir a representar mútuo benefício. Além disso, a transparência na alteração, limitação e acesso aos conteúdos armazenados proporciona sensação de controle ao mesmo.

> [...] a personalização aumenta a satisfação e a lealdade do cliente, o que, por sua vez, aumenta a aceitação do compartilhamento de dados. Se os benefícios concretos da personalização superarem a ameaça da violação de privacidade, o cliente se tornará mais propenso a compartilhar informações pessoais. A chave é aceitar a seletividade da atenção humana e criar uma percepção de controle. O consumidor acha a personalização mais aceitável quando isso facilita sua tomada de decisões e ao mesmo tempo lhe confere

[28] MARQUES, Humberto; LEVI, Renato. **Funil de Vendas: um jeito fácil para você realizar bons negócios**. Edição do Kindle. Editora Senac São Paulo, 2020.

> algum controle[29]

Assim, cedidos os dados pessoais por parte do consumidor, a questão de segurança está em como serão armazenados os dados (big data), quem os acessa e para que fim serão utilizados. Lembrando que a permissão e o legítimo interesse são o que confere, a princípio, o mínimo de legalidade nesta coleta.

> Além de ajudar os profissionais de marketing na definição do que deve ser oferecido, o big data também é útil para determinar como fazer a entrega. Na comunicação de marketing, o profissional usa o big data para definir o público-alvo, criar conteúdo e selecionar as mídias. Ele é valioso para o push marketing, como na seleção dos canais e na geração de leads. Também é comum utilizar os dados para a assistência pós-venda e a retenção do cliente. O big data é muito usado para prever desistências e determinar medidas de recuperação do serviço.[30]

Ainda, segundo Júlio Cezar de Souza Ribeiro[31]:

> os dados pessoais armazenados e utilizados por empresas estão sujeitos a diferentes ameaças, desde o vazamento de informações, passando por acessos indevidos, até ataques cibernéticos que buscam obter informações sensíveis para fins ilícitos

Portanto, a segurança dos dados é um fator crucial na gestão da privacidade de dados pessoais.

Ainda nessa esteira *"o acesso aos dados deve ser limitado a pessoas autorizadas e deve haver mecanismos de segurança que previnam o acesso indevido, incluindo a criptografia e outras técnicas de segurança"*[32]. Ressaltando a importância das empresas se atentem à proteção dos dados pessoais coletados.

Por fim, conforme Marcel Leonardi[33]:

> A permissão do titular para a coleta e o tratamento de seus dados pessoais é o primeiro passo para garantir a legalidade do processo. A partir daí, as empresas precisam implementar medidas técnicas e

---

[29] KOTLER, Philip; KARTAJAYA, Hermawan; SETIAWAN, Iwan. **Marketing 4.0: do tradicional ao digital.** São Paulo: Sextante, 2021. p. 95.
[30] Ibid.,p. 98.
[31] RIBEIRO, Júlio César de Souza; FERNANDES, Gustavo. **Gestão da Privacidade de Dados Pessoais**. São Paulo: Novatec, 2019. p. 117.
[32]MICELI, André L. **Marketing Digital & E-commerce**. São Paulo: Atlas, 2019. p. 227.
[33] LEONARDI, Marcel. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento.** São Paulo: RT, 2021. p. 68.

> organizacionais para proteger os dados pessoais contra acessos não autorizados e outros riscos.

Portanto, é importante que as empresas sejam transparentes com o consumidor quanto ao uso e proteção de seus dados pessoais, para garantir a confiança e a segurança no processo de coleta e tratamento de dados.

3 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) é uma legislação brasileira que estabelece as regras para o tratamento de dados pessoais, com o objetivo de garantir a privacidade e a segurança desses dados. Sua história no Brasil está relacionada a uma série de discussões e avanços na área de proteção de dados e privacidade.

A preocupação com a proteção de dados no Brasil começou a ganhar destaque no início dos anos 2000, com a aprovação de leis específicas para setores como o de telecomunicações e o de serviços financeiros. No entanto, ainda não havia uma legislação abrangente que regulamentasse de forma ampla o tratamento de dados pessoais.

Houve o surgimento de ações que levantaram questionamentos sobre as práticas de algumas empresas, e diversas decisões reforçavam a importância da proteção dos direitos dos consumidores. Um exemplo notório foi a decisão divulgada em dezembro de 2019, na qual a Ministra Nancy Andrighi, atuando como relatora, concedeu uma indenização por danos morais ao consumidor. Essa decisão pode ser embasada, por haver o vínculo cliente x empresa, em leis já existentes, como o Código de Defesa do Consumidor e a Lei do Cadastro Positivo, entre outras normas relevantes.

> Evidentemente, quando o consumidor fornece seus dados para a realização de uma compra no comércio ele não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais.
> Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos.[34]

Em 2010, foi criado o Projeto de Lei nº 5276/2010, que ficou conhecido como "Projeto de Lei de Proteção de Dados Pessoais". Esse projeto foi elaborado

[34]BRASIL. Superior Tribunal de Justiça. Recurso Especial no 1.758.799 - MG (2017/0006521-9). Recorrente:PROCOB S⁄A. Recorrido:JOSÉ GALVÃO DA SILVA. Relator:Ministra NANCY ANDRIGHI. Julgamento em: 12 de Novembro de 2019. Número do processo: REsp 0039441-55.2013.8.13.0693 MG 2017/0006521-9.

com base em discussões realizadas em uma comissão de juristas e tinha como objetivo principal estabelecer os princípios e diretrizes para a proteção de dados pessoais no Brasil.

Após diversos debates e audiências públicas, o Projeto de Lei foi aprovado na Câmara dos Deputados em maio de 2018. No entanto, antes de sua entrada em vigor, foi realizada uma série de negociações e ajustes para sua aprovação no Senado Federal.

Finalmente, em agosto de 2018, a LGPD foi sancionada pelo então presidente Michel Temer, através da Lei nº 13.709/2018. A lei estabelece princípios, direitos e deveres para o tratamento de dados pessoais, além de prever sanções e penalidades em caso de descumprimento.[35]

A LGPD entrou em vigor em setembro de 2020, após um período de adaptação para que as empresas e organizações se adequassem às novas exigências. Desde então, a Autoridade Nacional de Proteção de Dados (ANPD) foi criada como órgão responsável pela fiscalização e aplicação da lei.

> A privacidade já é uma garantia constitucional reafirmada em mecanismos legais de proteção, com destaque para o Marco Civil da Internet (Lei n. 12.965/2014) e a Lei do Consumidor (Lei n. 8.078/1990). Entretanto, é importante notar que a privacidade se distingue de proteção de dados, e que mesmo um dado público deve ser protegido. É nesse contexto que, em 2018, foi criada a Lei Geral de Proteção de Dados Pessoais (a LGPD, Lei n. 13.709/2018), que estabelece uma estrutura legal com foco específico na proteção de dados. A LGPD inclui a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP), estruturas ligadas à presidência da República e exclusivamente dedicadas ao tema. [36]

A conjuntura política favoreceu a promulgação da lei, pois o Brasil pleiteava uma cadeira na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), ao mesmo tempo que inflamaram as discussões sobre as informações constantes no projeto Cadastro Positivo, e ainda o escândalo da Cambridge Analytica e o Facebook[37] que merecem menção devido às proporções que o caso

---

[35] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

[36] GARCIA, Fábio. **Privacidade e proteção de dados: Um estudo sobre a Lei Geral de Proteção de Dados Pessoais (LGPD).** In: FELIX, Rafael (Org.). Manual de Direito Digital e Compliance. 1. ed. São Paulo: Thomson Reuters, 2019. p. 63.

[37] O escândalo envolveu a coleta indevida de dados pessoais de milhões de usuários do Facebook pela empresa de consultoria política Cambridge Analytica. Esses dados foram usados para criar perfis

tomou ante ao cenário global no tocante a manipulação de dados.

A Lei Geral de Proteção de Dados (LGPD) teve influência da General Data Protection Regulation (GDPR), regulamento do direito europeu, sobre a privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Económico Europeu. Que ao entrar em vigor em Maio de 2018 afetou consideravelmente os negócios em âmbito mundial.

O prazo de *vacatio legis*[38], acabou por oportunizar as adequações consideráveis que o mercado brasileiro precisaria fazer. Neste estudo o enfoque será nos meios digitais, na qual as agências de marketing sentiram maior impacto, por conta da captação e do monitoramento no Funil de Vendas, em específico, na captação de leads utilizada no inbound marketing.

Sua definição encontra-se no artigo 1º ‘’Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.’’[39]

Às partes envolvidas neste novo controle conforme o artigo 5° da referida Lei são: O controlador, Pessoa Física ou Jurídica a quem competem as decisões referentes ao tratamento de dados pessoais; O operador, Pessoa Física ou Jurídica que realizam o tratamento de dados pessoais em nome do Controlador; O Titular, Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. E para zelar, implementar e fiscalizar o cumprimento a Autoridade Nacional de Proteção de Dados (ANPD).

Sobre o dado pessoal, temos duas divisões: O dado pessoal, cujo informação está relacionada a pessoa natural identificada ou identificável. Exemplos de dados pessoais “comuns”: consentimento, cumprimento de obrigação legal ou regulatória, execução de contrato, processo judicial, administrativo ou arbitral, legítimo interesse,

---

psicográficos detalhados e influenciar o comportamento dos usuários durante as eleições presidenciais dos Estados Unidos em 2016. Esse caso trouxe à tona questões importantes sobre privacidade, segurança de dados e manipulação política. Além desse caso, a Cambridge Analítica atuou no Brexit, que levou o Reino Unido a sair da União Europeia. Fonte: LIMA, Ana Paula Moraes Canto de, et al. **LGPD - Lei Geral de Proteção de Dados: sua empresa está preparada**.p.19

[38] Vacatio legis: termo em latim que significa vacância da lei, ou seja, o tempo entre a promulgação da lei e sua entrada em vigor.

[39] Lei nº 13.709/2018. **Lei Geral de Proteção de Dados**. Brasília, DF, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23 de maio de 2023.

proteção do crédito, execução de políticas públicas ,estudos por órgãos de pesquisa, tutela da saúde, proteção da vida.

O outro tipo de dado pessoal, é o sensível - origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, saúde, vida sexual, genética ou biometria. Alguns exemplos de dados pessoais sensíveis são: Consentimento, Cumprimento de obrigação legal ou regulatória, Execução de políticas públicas, Estudos por órgãos de pesquisa, Exercício regular de direitos, Proteção da vida, Prevenção à fraude e À segurança do titular. Fontes nas bases legais do artigos 7º e 11º.

De acordo com a Lei Geral de Proteção de Dados (LGPD), dado pessoal é qualquer informação relacionada a pessoa natural identificada ou identificável. Isso pode incluir nome, CPF, endereço, e-mail, número de telefone, entre outros dados.

Diversos doutrinadores do direito têm se dedicado a definir e explicar o conceito de dado pessoal na LGPD. Seguem algumas citações:

Para Bruno Bioni, especialista em proteção de dados, "dado pessoal é qualquer informação que permita a identificação direta ou indireta de uma pessoa natural"[40]

Já para Márcio Cots, professor de direito e especialista em privacidade e proteção de dados, "dado pessoal é toda e qualquer informação relativa a pessoa natural, identificada ou identificável"[41]

Na visão de Danilo Doneda, professor de direito e um dos principais elaboradores da LGPD, "dado pessoal é qualquer informação que se refira a uma pessoa natural identificada ou identificável."[42] Essas são apenas algumas das definições possíveis de dado pessoal na LGPD, mas todas elas convergem para a ideia de que se trata de qualquer informação que possa ser relacionada a uma pessoa natural identificada ou identificável. A LGPD diferente do Marco Civil da Internet, aborda tanto o cenário Online quanto Offline, e analisa todas as relações de fluxos de dados pessoais. No que diz respeito ao marketing inbound, normalmente apenas os dados pessoais costumam ser captados para que seja estabelecida a

---

[40] BIONI, Bruno. LGPD: **Lei Geral de Proteção de Dados Pessoais Comentada**. 1ª ed. São Paulo: Revista dos Tribunais, 2020. p. 77

[41] COTS, Márcio. **Comentários à Lei Geral de Proteção de Dados Pessoais.** 1ª ed. São Paulo: Revista dos Tribunais, 2020. p. 43.

[42] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 2ª ed. Rio de Janeiro: Renovar, 2013. p. 121.

primeira comunicação.

3.1 Leis Regulamentadoras Setoriais

Anteriormente ao surgimento da LGPD no Brasil, existia um cenário regulatório complexo onde vigoravam, conflitantes e sem uniformidade, diversas leis regulamentadoras setoriais no tocante à privacidade, dados, comunicação e ciberespaço. Entre elas, relativas aos setores:

Setor financeiro, a Resolução do BACEN 9 n 4.658 - 2018, em seu artigo 2 e seguintes:

> Para fins desta resolução, considera-se:
> [...]
> X - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> [...]
> As instituições financeiras devem adotar medidas de segurança, administrativas e técnicas em padrões compatíveis com a natureza, o porte, a complexidade, a quantidade e a sensibilidade dos dados armazenados, bem como com as atividades por elas desenvolvidas, de modo a proteger os dados contra acesso não autorizado, destruição, perda, alteração, comunicação ou difusão.
> [...]
> O tratamento de dados pessoais pelas instituições financeiras deve observar as disposições da Lei nº 13.709, de 14 de agosto de 2018, e demais normas que regulamentem a proteção de dados pessoais.[43]

Este trecho da Resolução do BACEN nº 4.658/2018 destaca a definição de dado pessoal presente na LGPD, além de determinar que as instituições financeiras devem adotar medidas de segurança para proteger os dados pessoais e observar as normas de proteção de dados pessoais, conforme estabelecido na Lei nº 13.709/2018 (LGPD).

Sobre o sigilo das operações de instituições financeiras na Lei Complementar 105/2001 , prevê nos artigos 5 e 8:

> É vedada a utilização das informações obtidas nos termos desta Lei Complementar para fins diversos daqueles previstos nesta Lei Complementar, inclusive para instruir processo administrativo ou

[43] BANCO CENTRAL DO BRASIL. **Resolução nº 4.658, de 26 de abril de 2018.** Dispõe sobre o processo de supervisão e o processo administrativo sancionador na atuação regulatória do Banco Central do Brasil. Diário Oficial da União, Brasília, Seção 1, p. 24-26, 27 abr. 2018.

> judicial, sem prévia autorização do responsável pela guarda da informação.
> [...]
> As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais documentos, livros e registros forem considerados indispensáveis pela autoridade administrativa competente.
> [...]
> A inobservância do disposto neste artigo sujeita o infrator a processo administrativo-disciplinar, sem prejuízo das sanções penais e civis cabíveis.[44]

A Lei Complementar nº 105/2001 estabelece as regras para a utilização das informações obtidas a partir das instituições financeiras, determinando que essas informações só podem ser utilizadas para fins previstos na lei e mediante autorização do responsável pela guarda da informação. Além disso, a lei prevê que as autoridades fiscais só podem examinar documentos e registros das instituições financeiras em caso de processo administrativo ou fiscal em curso e quando esses documentos forem considerados indispensáveis pela autoridade competente. A inobservância dessas regras sujeita o infrator a processo administrativo-disciplinar, sanções penais e civis cabíveis.

Referente ao setor da saúde o Conselho Federal de Medicina com a Resolução 1.821/2007 em seus artigos 2, 7 e 8:

> É vedado ao médico:
> [...]
> V - permitir o acesso e/ou fornecer informações sobre pacientes a empresas, seguradoras, auditorias médicas, ou a qualquer outra instituição ou terceiros, salvo mediante autorização expressa do paciente ou quando amparado por legislação específica;
> [...]
> É vedado ao médico:
> [...]
> VIII - fornecer laudo, parecer ou atestado sem ter praticado ato profissional que os justifique, que não correspondam à verdade, que configurem fraude ou que favoreçam interesses ilegítimos;
> [...]
> O médico deverá zelar pelo sigilo profissional a fim de proteger a

[44] BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Diário Oficial da União, Brasília, 11 jan. 2001.

> privacidade do paciente, permitindo que somente pessoas autorizadas pelo paciente ou por lei possam ter acesso às informações sobre o seu estado de saúde.[45]

Este trecho da Resolução CFM nº 1.821/2007 trata da regulamentação do uso de dados médicos e estabelece que é vedado aos mesmos permitir o acesso ou fornecer informações sobre pacientes a empresas, seguradoras, auditorias médicas ou a qualquer outra instituição ou terceiros, salvo mediante autorização expressa do paciente ou quando amparado por legislação específica. Além disso, é vedado fornecer laudo, parecer ou atestado que não correspondam à verdade ou que configurem fraude. O médico também deve zelar pelo sigilo profissional e proteger a privacidade do paciente, permitindo que somente pessoas autorizadas pelo paciente ou por lei possam ter acesso às informações sobre o seu estado de saúde.

Referente ao Indivíduo temos a Declaração Universal dos Direitos do Homem, de 1948 que apesar de não fazer menção direta à regulamentação do uso de dados. Em seu artigo 12 estabelece o direito à privacidade:

> Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.[46]

Estabelece o direito à proteção da vida privada e da correspondência de todo indivíduo, sendo assim, pode ser relacionado à proteção dos dados pessoais, que são informações sensíveis que também devem ser protegidas pela lei para garantir a privacidade e a intimidade das pessoas.

Na Constituição Federal do Brasil 1988 no artigo 5:

> [...]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.[47]

---

[45] CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.821, de 23 de novembro de 2007.** Dispõe sobre as normas éticas para a utilização das técnicas de reprodução assistida. Diário Oficial da União, Brasília, 3 dez. 2007.
[46] ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Paris: ONU, 1948. Disponível em: http://www.dudh.org.br. Acesso em: 18 mar. 2023.
[47] BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.

Estabelece que a intimidade, vida privada, honra e imagem das pessoas são invioláveis, garantindo o direito a indenização em caso de violação desses direitos. Isso inclui a proteção dos dados pessoais das pessoas, já que o uso indevido desses dados pode violar sua privacidade e honra.

Ainda no Estatuto da Criança e do Adolescente da Lei 8.069/1990 nos artigos 16, 17, 143 e 248:

> O direito à privacidade, à honra e à imagem das crianças e dos adolescentes será respeitado em consonância com o disposto na Constituição Federal e na lei.";
> O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais.";
> É obrigatório o registro, no prontuário clínico, dos dados concernentes à saúde da criança e do adolescente, observados os princípios éticos e as normas expedidas pelos Conselhos Federal e Regionais de Medicina.";
> A divulgação de ato infracional poderá ser feita, excepcionalmente, quando necessária à identificação ou localização do infrator ou à apuração de infrações semelhantes.[48]

Esses artigos indicam a importância de respeitar a privacidade, honra, imagem e integridade física, psíquica e moral de crianças e adolescentes, assim como a necessidade de proteger seus dados pessoais, inclusive no âmbito da saúde. O artigo 248, por sua vez, permite a divulgação de ato infracional apenas em casos excepcionais, visando proteger a identidade e privacidade dos adolescentes envolvidos. Outro caso com enfoque na proteção da privacidade e dos dados pessoais de crianças e adolescentes.

Na Lei do Habeas Data - Lei 9.507/1997, o artigo 3:

> Qualquer cidadão é parte legítima para propor ação de habeas data que vise a proteger o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, ou para corrigir dados pessoais incorretos e obter a certificação de que as correções foram efetuadas.[49]

Através dela, o cidadão pode obter informações sobre si mesmo que

---

[48] BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Estatuto da Criança e do Adolescente. Diário Oficial da União, Brasília, DF, 16 jul. 1990.
[49] BRASIL. **Lei nº 9.507, de 12 de novembro de 1997**. Lei do Habeas Data. Diário Oficial da União, Brasília, DF, 13 nov. 1997.

estejam armazenadas em bancos de dados de entidades governamentais ou de caráter público, bem como corrigir dados pessoais incorretos. Em suma, o Habeas Data é uma importante ferramenta para garantir o direito à privacidade e à proteção de dados pessoais, além de contribuir para a transparência e *accountability*[50] de entidades que lidam com informações pessoais.

No Código Civil da Lei 10.406/2002[51] é onde estabelece uma série de direitos fundamentais que estão diretamente relacionados à proteção de dados pessoais, tais como o direito à privacidade (art. 21), o direito ao nome (art. 16), o direito à imagem (art. 20) e o direito à honra (art. 186).

A importância desses dispositivos é fundamental para garantir a proteção de dados pessoais, uma vez que eles estabelecem direitos básicos dos indivíduos em relação à sua identidade, intimidade e privacidade. Esses direitos têm sido cada vez mais valorizados e protegidos, principalmente no contexto atual em que a tecnologia e a informação estão cada vez mais presentes na vida das pessoas.

Além disso, o Código Civil também prevê a responsabilidade civil por danos causados a terceiros, o que inclui danos causados por violações de privacidade e uso indevido de dados pessoais (art. 927). Esse dispositivo é importante porque estabelece a responsabilidade dos indivíduos e das empresas em relação ao uso de dados pessoais, garantindo que haja consequências para quem desrespeitar a privacidade e a proteção de dados pessoais.

Em suma, embora o Código Civil não possua um trecho específico que trate da regulamentação do uso de dados, seus dispositivos relacionados à privacidade, imagem, honra e responsabilidade civil são fundamentais para garantir a proteção de dados pessoais e a responsabilização daqueles que desrespeitam esse direito.

Na lei de Acesso à informação - Lei 12.527/2011[52], artigo 6:

> Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação, utilizando todos os meios e instrumentos legítimos e

[50] “um processo fundamental para a governança democrática, destacando a importância da prestação de contas dos governantes às partes interessadas e da responsabilização por suas ações e políticas.” tradução nossa. Fonte: BOVENS, Mark. **Analysing and assessing public accountability: a conceptual framework.** European Journal of Political Research, v. 37, n. 4, p. 391-412, 2000.
[51] BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002.
[52] BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação. Diário Oficial da União, Brasília, DF, 18 nov. 2011.

> disponíveis, ressalvadas as hipóteses de sigilo e as informações pessoais protegidas pela Lei.

A Lei de Acesso à Informação é uma lei federal que estabelece as regras para o acesso às informações públicas. Ela tem como objetivo principal garantir o direito fundamental de acesso à informação, previsto na Constituição Federal, e promover a transparência e a *accountability* dos órgãos públicos.

O trecho estabelece a obrigação dos órgãos e entidades do poder público de assegurar a gestão transparente da informação, garantindo amplo acesso e divulgação das informações públicas. É importante destacar que a lei também prevê a proteção de informações pessoais, respeitando os direitos fundamentais à privacidade e à proteção de dados pessoais.

A Lei de Acesso à Informação é fundamental para garantir a transparência e *accountability* dos órgãos públicos e para o exercício do direito fundamental de acesso à informação por parte da sociedade. Além disso, a Lei também contribui para o fortalecimento da democracia, uma vez que permite que a população possa participar de forma mais ativa e informada nas decisões públicas.

É importante ressaltar que a Lei de Acesso à Informação também pode ser utilizada como ferramenta para o controle social e para a prevenção e combate à corrupção, uma vez que garante o acesso a informações públicas que podem ser utilizadas para identificar irregularidades e práticas ilícitas.

Referente ao Estado o crime de inserção da dados falsos em sistemas de informação pública - Lei 9.983/2000 em seu artigo 1:

> Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano será punido com reclusão de 2 (dois) a 12 (doze) anos e multa.[53]

Essa lei é fundamental para a garantia da integridade das informações públicas, uma vez que prevê penalidades para aqueles que inserem dados falsos em sistemas de informação pública ou alteram ou excluem dados corretos com o fim de obter vantagem indevida ou causar dano. A penalização desses comportamentos

[53] BRASIL. **Lei nº 9.983, de 14 de julho de 2000**. Dispõe sobre o processo administrativo no âmbito da Administração Pública Federal. Diário Oficial da União, Brasília, DF, 17 jul. 2000.

ilegais contribui para a promoção da transparência e da *accountability* dos órgãos públicos, além de prevenir possíveis danos à sociedade decorrentes da divulgação de informações falsas ou manipuladas.

Além disso, a Lei 9.983/2000 também contribui para a proteção da privacidade e dos dados pessoais, uma vez que a inserção ou alteração indevida de dados pessoais em sistemas de informação pública pode ter graves consequências para as pessoas afetadas. Portanto, a penalização dessas práticas também contribui para a proteção dos direitos fundamentais à privacidade e à proteção de dados pessoais.

No Cadastro único para programas sociais do Governo Federal pelo Decreto 6.135/2007 em seu artigo 22:

> As informações constantes do Cadastro Único serão utilizadas pelos órgãos e pelas entidades da administração pública federal, estadual, distrital e municipal, respeitadas as competências e as atribuições legais, para fins de seleção, monitoramento e avaliação de programas, projetos e benefícios sociais, bem como para a implementação de políticas públicas.[54]

A utilidade dessa regulamentação é fundamental para garantir a proteção dos dados pessoais dos usuários do Cadastro Único e para assegurar que essas informações informações socioeconômicas das famílias brasileiras em situação de vulnerabilidade sejam utilizadas apenas para fins legais e específicos, relacionados à seleção, monitoramento e avaliação de programas, projetos e benefícios sociais e à implementação de políticas públicas. Além disso, a regulamentação também contribui para a transparência e a *accountability* do Estado, uma vez que estabelece regras claras para a coleta, armazenamento e uso desses dados.

Censo Anual da Educação - Decreto 6.425/2008 em seu artigo 6 prevê:

> As informações coletadas pelo Censo Escolar e pelo Censo da Educação Superior serão utilizadas para fins exclusivos de estatística, planejamento e avaliação, não podendo ser objeto de comercialização ou uso diverso do previsto neste Decreto.[55]

---

[54] BRASIL. **Decreto nº 6.135, de 26 de junho de 2007.** Regulamenta a Lei nº 8.742, de 7 de dezembro de 1993, que dispõe sobre a organização da Assistência Social. Diário Oficial da União, Brasília, DF, 27 jun. 2007.

[55] BRASIL. **Decreto nº 6.425, de 4 de abril de 2008.** Regulamenta o Censo Anual da Educação Básica. Diário Oficial da União, Brasília, DF, 7 abr. 2008.

Fundamental para garantir a proteção dos dados pessoais dos estudantes e profissionais da educação e para assegurar que as informações coletadas sejam utilizadas apenas para fins específicos e legítimos, relacionados à estatística, planejamento e avaliação do sistema educacional brasileiro. Além disso, a regulamentação também contribui para a transparência e a *accountability* do Estado, uma vez que estabelece regras claras para a coleta, armazenamento e uso desses dados.

Política de Dados Abertos do Governo Federal - Decreto 8.777/2016: Tem como objetivo promover a abertura de dados públicos e a sua disponibilização em formato aberto para a sociedade, visando ampliar a transparência, a participação cidadã, a inovação e o desenvolvimento econômico e social.

> Art. 8º Os dados abertos disponibilizados pelos órgãos e entidades da administração pública federal direta, autárquica e fundacional devem ser disponibilizados em formato aberto, estruturado e processável por máquina, objetivando sua plena utilização pela sociedade.
> § 1º A disponibilização de dados abertos deve observar as normas e padrões técnicos definidos pela Infraestrutura Nacional de Dados Abertos - INDA.
> § 2º A disponibilização de dados abertos não implica em autorização para sua comercialização, direta ou indireta, salvo nos casos em que exista previsão legal.[56]

Essa regulamentação é fundamental para garantir a transparência e a *accountability* do Estado, uma vez que estabelece regras claras para a disponibilização de dados públicos em formato aberto e estruturado, permitindo que a sociedade possa acessar, analisar e utilizar esses dados para os mais diversos fins, incluindo a tomada de decisões informadas, a inovação e o desenvolvimento de novas soluções e serviços.

Além disso, a regulamentação também contribui para a promoção da transparência ativa e para o cumprimento dos princípios da Lei de Acesso à Informação[57] , uma vez que obriga os órgãos e entidades da administração pública federal a disponibilizarem dados públicos de interesse coletivo em formato aberto,

---

[56] BRASIL. Decreto nº 8.777, de 11 de maio de 2016. Dispõe sobre o Prazo de Recolhimento e a Atualização Monetária dos Débitos Inscritos em Dívida Ativa da União. Diário Oficial da União, Brasília, DF, 12 maio 2016.
[57] BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Diário Oficial da União, Brasília, DF, 18 nov. 2011.

estruturado e processável por máquina.

No setor de Comunicações a Lei 9.296/1996 de Interceptação Telefônica e Telemática regulamenta no artigo 10:

> Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
> § 1º Na mesma pena incorre quem:
> I - divulga, transmite a outrem ou utiliza abusivamente as informações obtidas na forma deste artigo;
> II - utiliza o serviço de radiocomunicação ou o de informática, ou se aproveita deles, sem autorização ou em desacordo com determinação legal ou regulamentar.[58]

Acima, a regulamentação busca garantir o direito à privacidade e à intimidade das pessoas, impedindo a realização de interceptações ilegais de comunicações telefônicas, de informática ou telemáticas. Além disso, a regulamentação visa proteger as informações obtidas por meio dessas interceptações, evitando a divulgação, transmissão ou uso abusivo dessas informações, o que poderia prejudicar a imagem e a reputação das pessoas envolvidas.

Fundamental para proteger os direitos fundamentais das pessoas, garantindo que a obtenção, a utilização e a divulgação de informações sigilosas sejam realizadas de forma legal e autorizada, de acordo com os princípios da legalidade e da proporcionalidade.

A Lei Geral de Telecomunicações de nº 9.472/1997, no artigo 3:

> A disciplina dos serviços de telecomunicações tem como objetivo a promoção do desenvolvimento das telecomunicações do País, em regime de competição, com liberdade de escolha pelo usuário e com plena observância das normas legais e regulamentares aplicáveis, em especial das normas relativas à defesa da concorrência e à proteção dos direitos dos consumidores.
> § 1º Para atender ao objetivo previsto no caput, a disciplina dos serviços de telecomunicações tem como diretrizes:
> (....)
> III - garantia do direito à privacidade, inviolabilidade da intimidade e da vida privada, bem como do sigilo de suas comunicações privadas

[58] BRASIL. Lei nº 9.296, de 24 de julho de 1996. Dispõe sobre as interceptações telefônicas. Diário Oficial da União, Brasília, DF, 25 jul. 1996.

> e dados pessoais, nos termos da lei;
> (....)[59]

A utilidade dessa regulamentação é garantir o direito à privacidade, intimidade e sigilo das comunicações pessoais, bem como a proteção dos dados pessoais dos usuários de serviços de telecomunicações. A LGT estabelece a obrigatoriedade das empresas de telecomunicações em proteger esses direitos, promovendo o desenvolvimento do setor em regime de competição.

Com essa regulamentação, os usuários dos serviços de telecomunicações no Brasil têm a garantia de que suas informações pessoais e comunicações estarão protegidas contra o uso indevido por terceiros, incluindo as empresas prestadoras de serviços de telecomunicações. Além disso, a regulamentação também estimula a concorrência entre as empresas do setor, garantindo a liberdade de escolha dos usuários e a oferta de serviços de qualidade.

Referente ao setor de Consumo e Crédito temos o Código de Defesa do Consumidor sujo antes da Lei Geral de Proteção de Dados Pessoais (LGPD), o Código de Defesa do Consumidor (CDC)[60] não possuía um trecho específico sobre a regulamentação do uso de dados pessoais pelas empresas. No entanto, o CDC estabelece princípios fundamentais para a proteção dos direitos dos consumidores, que também se aplicam ao tratamento de dados pessoais pelas empresas.

O CDC estabelece, por exemplo, que as empresas devem respeitar a privacidade e a intimidade dos consumidores, bem como garantir a transparência e a informação adequada sobre os produtos e serviços oferecidos. Esses princípios são fundamentais para o tratamento de dados pessoais, pois garantem que os consumidores sejam informados e tenham controle sobre as informações coletadas sobre eles.

Além disso, o CDC também estabelece que as empresas são responsáveis por eventuais danos causados aos consumidores em decorrência de práticas comerciais abusivas ou de produtos e serviços defeituosos. Essa responsabilidade se estende ao tratamento de dados pessoais, pois a empresa é responsável por garantir a segurança e a proteção dos dados dos consumidores.

---

[59] BRASIL. **Lei nº 9.472, de 16 de julho de 1997**. Lei Geral de Telecomunicações. Diário Oficial da União, Brasília, DF, 17 jul. 1997.
[60] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Código de Defesa do Consumidor. Diário Oficial da União, Brasília, DF, 12 set. 1990.

No entanto, apesar de estabelecer princípios fundamentais para a proteção dos direitos dos consumidores em relação ao tratamento de dados pessoais, o CDC não era suficiente para regular de forma abrangente e específica o tratamento de dados pessoais pelas empresas.

Sobre o Decreto 6.523/2008 acerca do Serviço de SAC está estabelecido algumas disposições que visam garantir a proteção dos dados dos consumidores. Dentre essas disposições, destacam-se os artigos 15 e 29, que abordam a obrigação das empresas de manterem registros das demandas dos consumidores e a proibição da solicitação excessiva ou indevida de informações pessoais, respectivamente.

> As empresas prestadoras de serviços regulados ficam obrigadas a manter serviço de atendimento ao consumidor, que deverá ser adequado para atender às demandas e esclarecer as dúvidas dos consumidores.
> § 1o O serviço de atendimento ao consumidor funcionará, por meio de ligação telefônica gratuita, durante 24 (vinte e quatro) horas por dia.
> § 2o O serviço de atendimento ao consumidor deverá estar apto a receber e processar as demandas dos consumidores por todos os meios de comunicação disponíveis.
> § 3o As demandas dos consumidores devem ser resolvidas em até 5 (cinco) dias úteis, contados da data de registro, podendo este prazo ser prorrogado mediante justificativa.
> § 4o As empresas prestadoras de serviços regulados devem manter registros das demandas dos consumidores por um período mínimo de 2 (dois) anos, que deverão estar disponíveis para consulta pelos consumidores.[61]

O artigo 15 determina que as empresas devem manter registros das demandas dos consumidores por um período mínimo de dois anos, com a finalidade de viabilizar o acompanhamento e o controle da qualidade do atendimento prestado pelo SAC. Essa medida tem como objetivo garantir a transparência no atendimento aos consumidores, permitindo que eles tenham acesso ao histórico de suas demandas e à avaliação da empresa em relação ao atendimento prestado.

> É proibida a exigência de informações pessoais do consumidor para a realização de atendimento, exceto aquelas estritamente necessárias à prestação do serviço ou fornecimento do produto.
> § 1o O consumidor que se sentir lesado por ter fornecido informações pessoais indevidas poderá exigir a imediata correção, devendo o fornecedor dos serviços arcar com as despesas

[61] BRASIL. **Decreto nº 6.523, de 31 de julho de 2008**. Dispõe sobre o Serviço de Atendimento ao Consumidor (SAC). Diário Oficial da União, Brasília, DF, 1º ago. 2008.

> decorrentes.
> § 2o As informações pessoais dos consumidores obtidas em virtude da prestação dos serviços de atendimento ao consumidor deverão ser utilizadas exclusivamente para os fins a que se destinam e poderão ser armazenadas em banco de dados, observado o disposto na legislação aplicável.[62]

Já o artigo 29 proíbe a solicitação de informações pessoais do consumidor de forma excessiva ou indevida, respeitando a privacidade e a intimidade do titular dos dados. O objetivo dessa medida é proteger os direitos fundamentais dos consumidores, impedindo que as empresas coletem informações desnecessárias ou abusivas e garantindo que os consumidores tenham controle sobre o uso de suas informações pessoais.

Dessa forma, os artigos 15 e 29 do Decreto 6.523/2008 tinham como função estabelecer algumas medidas básicas para a proteção dos dados dos consumidores no contexto do atendimento ao SAC.

Na Lei do Cadastro Positivo, Lei 12.414/2011 temos o artigo 5 que estabelece a finalidade do Cadastro Positivo, que é a de registrar informações positivas e negativas do histórico de crédito dos consumidores, a fim de fornecer dados relevantes para as análises de risco de crédito e decisões de concessão de crédito por parte das instituições financeiras e demais empresas que operam no mercado de crédito.

> O Cadastro Positivo tem por finalidade armazenar e gerir informações necessárias para a análise de risco de crédito. O compartilhamento de informações constantes do Cadastro Positivo será efetuado mediante consentimento prévio, informado e específico do cadastrado.[63]

No artigo 7 é estabelecido as condições para o compartilhamento dos dados do Cadastro Positivo, que deve ser feito mediante o consentimento prévio, informado e específico do titular dos dados.

Esses artigos visam garantir que o uso dos dados no Cadastro Positivo seja feito de forma responsável e respeitando os direitos dos consumidores. Ao estabelecer a finalidade do Cadastro Positivo e as condições para o compartilhamento dos dados, a lei busca proteger a privacidade e a intimidade dos

---

[62] Ibid.
[63] BRASIL. **Lei nº 12.414, de 9 de junho de 2011.** Dispõe sobre a proteção ao crédito. Diário Oficial da União, Brasília, DF, 10 jun. 2011.

titulares dos dados, bem como garantir a transparência e a segurança no uso dessas informações pelas empresas que operam no mercado de crédito.

A regulamentação do uso de dados no Cadastro Positivo tem como objetivo principal fomentar a oferta de crédito e reduzir a inadimplência, contribuindo para o desenvolvimento econômico e social do país.

A Lei 7.962/2013 do Comércio Eletrônico também conhecida como "Lei do E-commerce"[64], estabelece regras para proteger os consumidores nas compras realizadas por meio eletrônico e regulamenta o uso de dados pessoais. O Artigo 7º da referida lei prevê que é obrigatória a disponibilização de informações claras e precisas sobre o tratamento de dados pessoais pelo fornecedor, incluindo a finalidade, forma e duração do tratamento, além da identificação do responsável pelo tratamento.

Essa disposição tem uma grande importância no âmbito da proteção de dados pessoais e privacidade do consumidor. A disponibilização de informações claras e precisas sobre o tratamento de dados pessoais pelo fornecedor permite que o consumidor tenha controle sobre a sua informação pessoal e possa decidir sobre a sua divulgação. Ademais, a identificação do responsável pelo tratamento de dados pessoais facilita a aplicação de medidas de responsabilização em caso de uso indevido ou não autorizado desses dados.

A Resolução 245/2007 DENATRAN[65] relativo aos setores de Internet ou eletrônicos, regulamenta o acesso e compartilhamento de informações sobre veículos, condutores e infrações de trânsito entre os órgãos de trânsito e demais entidades autorizadas. O artigo 2º da resolução determina que o acesso às informações é restrito aos órgãos e entidades autorizadas e somente deve ser realizado para fins específicos previstos em lei ou regulamento.

Essa disposição é fundamental para garantir a proteção dos dados pessoais dos proprietários de veículos e condutores, bem como a segurança no trânsito. Ao estabelecer regras claras para o acesso e compartilhamento de informações, a resolução contribui para evitar o uso indevido ou não autorizado dessas informações, o que poderia prejudicar a privacidade dos indivíduos envolvidos e até

---

[64] BRASIL. **Lei nº 7.962, de 15 de março de 2013.** Dispõe sobre a proteção do consumidor no comércio eletrônico. Diário Oficial da União, Brasília, DF, 18 mar. 2013.
[65] BRASIL. Departamento Nacional de Trânsito. **Resolução nº 245, de 27 de julho de 2007.** Estabelece normas para o transporte de produtos perigosos. Diário Oficial da União, Brasília, DF, 30 jul. 2007.

mesmo gerar riscos à segurança no trânsito.

A Lei 12.737/2012[66], também conhecida como Lei Carolina Dieckmann, dispõe sobre a tipificação criminal de delitos informáticos, como a invasão de computadores e a violação de dados pessoais. O artigo 154-A, incluído pela referida lei, tipifica a conduta de invadir dispositivo informático alheio, conectado ou não à internet, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou de sua responsável legal.

Representou um avanço significativo na proteção dos direitos fundamentais à privacidade e à proteção de dados pessoais. Ao tipificar a conduta de invasão de dispositivos informáticos, a lei busca coibir práticas ilegais e criminosas que possam colocar em risco a privacidade e a segurança dos dados pessoais dos usuários. A criminalização dessas práticas tem como objetivo promover a proteção dos direitos fundamentais dos usuários de dispositivos informáticos, bem como a segurança e a confiabilidade das informações que são armazenadas e compartilhadas nesses dispositivos.

O Marco Civil da Internet - Lei 12.965/2014[67] estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. O artigo 7º, que trata da proteção aos registros, aos dados pessoais e às comunicações privadas, determina que a coleta, o uso, o armazenamento e a proteção de dados pessoais devem ser realizados de forma transparente e com respeito à privacidade, à intimidade, à honra e à imagem das pessoas.

Estabelece uma série de direitos e deveres para os usuários da internet e para as empresas e instituições que coletam e utilizam dados pessoais. Lembrando que a proteção dos dados pessoais é um direito fundamental e essencial para a garantia da privacidade e da liberdade de expressão dos usuários da internet. Além disso, a transparência na coleta e utilização dos dados pessoais é um princípio fundamental para o fortalecimento da confiança dos usuários na internet.

O Decreto 8.771/2016[68] é uma norma regulamentadora da Lei 12.965/2014,

---

[66] BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, DF, 3 dez. 2012.
[67] BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014.
[68] BRASIL. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 12 maio 2016.

que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. O decreto estabelece regras para a guarda, proteção e utilização de dados pessoais e comunicações privadas pelos provedores de conexão e de aplicações de internet.

O artigo 9º do Decreto 8.771/2016 determina que os provedores de aplicações de internet devem informar de forma clara e completa sobre a coleta, uso, armazenamento e tratamento de dados pessoais dos usuários, bem como sobre as finalidades específicas para as quais esses dados serão utilizados. Além disso, o decreto estabelece que os provedores de aplicações de internet devem obter o consentimento expresso do usuário para a coleta e utilização de seus dados pessoais, de forma destacada e específica para cada finalidade.

Estabelece um conjunto de obrigações que os provedores de aplicações de internet devem cumprir para garantir a privacidade e a proteção dos dados pessoais dos usuários. A informação clara e completa sobre a coleta e utilização de dados pessoais é essencial para que os usuários possam tomar decisões informadas sobre o compartilhamento de suas informações na internet. Já a exigência de consentimento expresso e destacado contribui para que os usuários tenham maior controle sobre seus dados pessoais, decidindo de forma consciente sobre a utilização dessas informações por terceiros.

Concluindo, vale destacar que as diversas Leis, Decretos e Regulamentações acima colacionados também contribuíram para a implementação da Lei Geral de Proteção de Dados (Lei 13.709/2018), uma vez que estabelece punibilidades e regras claras para a anonimização, manutenção e a proteção de dados pessoais que possam ser disponibilizados em formato aberto.

3.2 Big Data

Datificar é o processo que transforma “comportamentos humanos complexos, sentimentos, relacionamentos e motivações em formas de dados digitais” [69]. Esse processo é considerado um meio legítimo de monitorar, acessar e entender o comportamento humano[70].

---

[69] LUPTON, Deborah. (2016). **The quantified self: A sociology of self-tracking.** John Wiley & Sons.
[70] VAN DIJCK, José. (2014). **Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology.** Surveillance & Society, 12(2), 197-208.

> O big data atua como a peça final do quebra-cabeça. A tecnologia de IA exige um volume maciço e uma ampla variedade de dados para que a máquina seja treinada e o algoritmo seja progressivamente aprimorado. Isso é propiciado pelo uso diário de navegadores na web, e-mails, redes sociais e aplicativos de mensagens, principalmente em telefones celulares. Os dados externos complementam os dados internos de transações, gerando padrões comportamentais e psicográficos. A melhor coisa em relação aos dados com base na internet é que, ao contrário dos dados de pesquisas de mercado tradicionais, eles podem ser coletados on-line, em tempo real e na escala desejada. Além disso, o custo do armazenamento de dados vem caindo, e a capacidade vem aumentando em ritmo mais rápido – facilitando a gestão de grandes volumes de informações. [71]

O big data, o qual pode ser resumido como o conjunto de dados coletados, em larga escala, a partir de todas as origens (entradas) disponíveis, deve ser categorizado e tratado por algoritmos específicos a fim de garantir melhores resultados às estratégias de marketing.

> O advento do big data transformou a face da segmentação e da seleção de mercados-alvo. A amplitude e a profundidade dos dados sobre os consumidores estão crescendo exponencialmente. Dados de mídia, dados sociais, dados da web, dados de pontos de venda, dados da internet das coisas e dados de engajamento formam, juntos, um perfil riquíssimo de clientes individuais, permitindo que o profissional pratique o marketing de “segmentos de um”[72]

Novas tecnologias de extração, tratamento e armazenagem de dados reduziram os custos da datificação de atividades cotidianas e seu registro. Associados ao crescente uso do ambiente digital como meio de comunicação e consumo, o volume de dados produzido tornou-se inconcebível. No entanto, as empresas tradicionais não estavam preparadas para explorar tais fontes e tiveram que evoluir suas atividades de extração e uso de dados.

Todavia esta novidade e exclusividade de mercado, agora inteiramente personalizadas, ofereciam um risco inerente à forma como esses dados seriam transacionados e armazenados. Os riscos à informação pessoal nos provedores de serviço são diretamente proporcionais à quantidade de atributos coletados dos

---

[71] KOTLER,Philip et al. **Marketing 5.0: tecnologia para a humanidade.** Rio de Janeiro: Sextante, 2017. e-book. p.108

[72] Ibid. p. 156-157

indivíduos[73].

> O JSON Web Token (JWT) utiliza de um objeto de padrão JSON para definir um modo compacto e independente, que pode ser enviado junto à uma requisição de acesso e conter as informações do usuário, para a transmissão segura de informações entre cliente e servidor. O token gerado pelo JWT é salvo no dispositivo do usuário e suas informações podem ser verificadas a cada solicitação, pois são criptografadas utilizando um segredo, através de um par de chaves públicas e privadas, garantindo assim a sua confiabilidade. [74]

Podendo ser utilizados tanto para autenticação de usuários, que é o cenário mais trivial, sendo enviados a cada requisição de rota, serviço ou recurso, quanto na transmissão segura de informações, uma vez que com base em sua assinatura criptografada é possível verificar se o conteúdo não foi adulterado.

Evidenciando, o novo desafio da era digital que inclui questões como: a segurança dos dados, fraudes e privacidade dos usuários. A adequação torna-se um diferencial positivo para diversos provedores de aplicação no Brasil e no mundo, que passaram a adotar mecanismos sofisticados de criptografia forte como o padrão básico de segurança em seus serviços.

> A privacidade pode ser alcançada por leis, técnicas e mecanismos (ou políticas). A finalidade é permitir que indivíduos exerçam controle sobre seus dados pessoais. A importância de proteger dados pessoais mereceu a criação de normas internacionais, como a iniciativa da Organisation for Economic Co-operation and Development (OECD) (OECD, 1980), que estabeleceu oito princípios gerais. Esses princípios nortearam a criação de leis, regulamentos e frameworks para proteção aos dados pessoais em diversos países.[75]

As comunicações digitais, tipicamente atravessam fronteiras e um mesmo serviço de comunicação costuma ser utilizado em diversos países. Ao considerar essas características nota-se como a falta de regulação da criptografia em um país pode criar uma falha de segurança que afete todos os demais utilizadores de um

---

[73] CAMERON, Kim. **The laws of identity.** 2005. Disponível em: <http://myinstantid.com/laws.pdf>. Acesso em: 15 jun. 2022.
[74] JONES, Michael B. (2011) **“The emerging JSON-based identity protocol suite”**. W3C workshop on identity in the browser.
[75] CAMILLO, Gerson Luiz. **Privacidade no controle de acesso em sistemas de gerenciamento de identidade para a Web** / Gerson Luiz Camillo ; orientadora, Carla Merkle Westphall, 2018.

mesmo sistema de comunicação. Se um país proíbe criptografia eficaz ou impõe vulnerabilidades aos serviços existentes em seu território, então a comunicação oriunda deste país ou que trafegue por sua infraestrutura será, necessariamente, menos segura. Nesse sentido, pode-se afirmar que um sistema de comunicação internacional será tão seguro quanto, o país mais restritivo envolvido, permitir que ele seja.[76]

[76] SWIRE, Peter; AHMAD, Karim. **Encryption and Globalization.** Science and Technology Law Review, [S. l.], v. 13, n. 2, 2012. DOI: 10.7916/stlr.v13i2.3964. Disponível em: <https://journals.library.columbia.edu/index.php/stlr/article/view/3964>. Acesso em: 6 jul. 2022.

4 SEGURANÇA JURÍDICA

Sobre a gestão de incidentes de segurança, com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Alguns exemplos de incidentes de segurança são: código malicioso (vírus) na rede de computadores da organização, indisponibilidade de *e-commerce* e o vazamento de dados confidenciais da empresa após ataque cibernético. Evidenciando a importância da elaboração do plano de resposta (ou contenção) a incidentes de privacidade.

Vale saber que gastos com LGPD, para empresas optantes pelo regime tributário do lucro real, podem gerar créditos de PIS/Cofins.

> No caso, o advogado que assessora a tng, Leonardo Mazzillo, fez questão de deixar muito claro na petição inicial o quanto esse tratamento de dados é fundamental. “em toda atividade econômica, o momento da venda é o mais importante. e nessa hora, o caixa pergunta ao cliente se quer ou não cpf na nota, ou seja, o varejista é obrigado a lidar com esses dados[77]

A LGPD instituiu uma série de obrigações para as empresas em relação ao manuseio e a guarda de informações de terceiros – clientes, fornecedores e colaboradores. E como se trata de obrigação, sem a qual a empresa não poderia exercer sua atividade, acrescenta, deve ser considerada insumo e ter direito a créditos de PIS e Cofins.

4.1 Aplicabilidade

A LGPD se aplica a empresas que ou têm estabelecimento no Brasil, e/ou oferecem produtos e serviços ao mercado brasileiro, e/ou coletam e tratam dados de

---

[77] LOPES CASTELO,***TNG obtém direito a créditos de PIS e COFINS sobre gastos com a LGPD***. *Lopes Castelo Advogados*. Disponível em: [https://lopescastelo.adv.br/tng-obtem-direito-a-creditos-de-pis-e-cofins-sobre-gastos-com-a-lgpd/#:~:te xt=A%20rede%20de%20lojas%20TNG,Prote%C3%A7%C3%A3o%20de%20Dados%20](LGPD). Acesso em: 23 maio 2023.

pessoas que estejam no país. Assim como às pessoas físicas que tratam dados pessoais com fins econômicos.

> [...] não estão sujeitos a ela (LGPD) os dados tratados por uma pessoa natural sem qualquer finalidade econômica, aqueles utilizados para fins artísticos, jornalísticos e acadêmicos. Ou, ainda, para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão a infrações penais – nesses casos, haverá legislação específica sobre o assunto e o banco de dados não poderá ser utilizado por empresa privada. Ela também exclui os dados que tenham origem fora do território nacional, desde que não haja nenhum compartilhamento, tratamento ou transferência no Brasil.[78]

Antes da LGPD os *leads* captados nas campanhas de *inbound marketing* não eram protegidos podendo ser utilizados para diversos fins não especificados. Além de que para o titular requerer a exclusão dessas informações muitas vezes não havia informações de contato disponíveis, ou pronta resposta para esta solicitação.

As novidades trazidas pela Lei Geral de Proteção de Dados quanto a este fluxo, são que a partir do primeiro contato, o visitante deve ter ciência que suas informações estão sendo tratadas: armazenadas e utilizadas. Para que fim serão operadas. Qual empresa terá acesso aos dados. E a criação de canais de contato para que a qualquer momento possa ser solicitado ao controlador, a exclusão completa das informações.

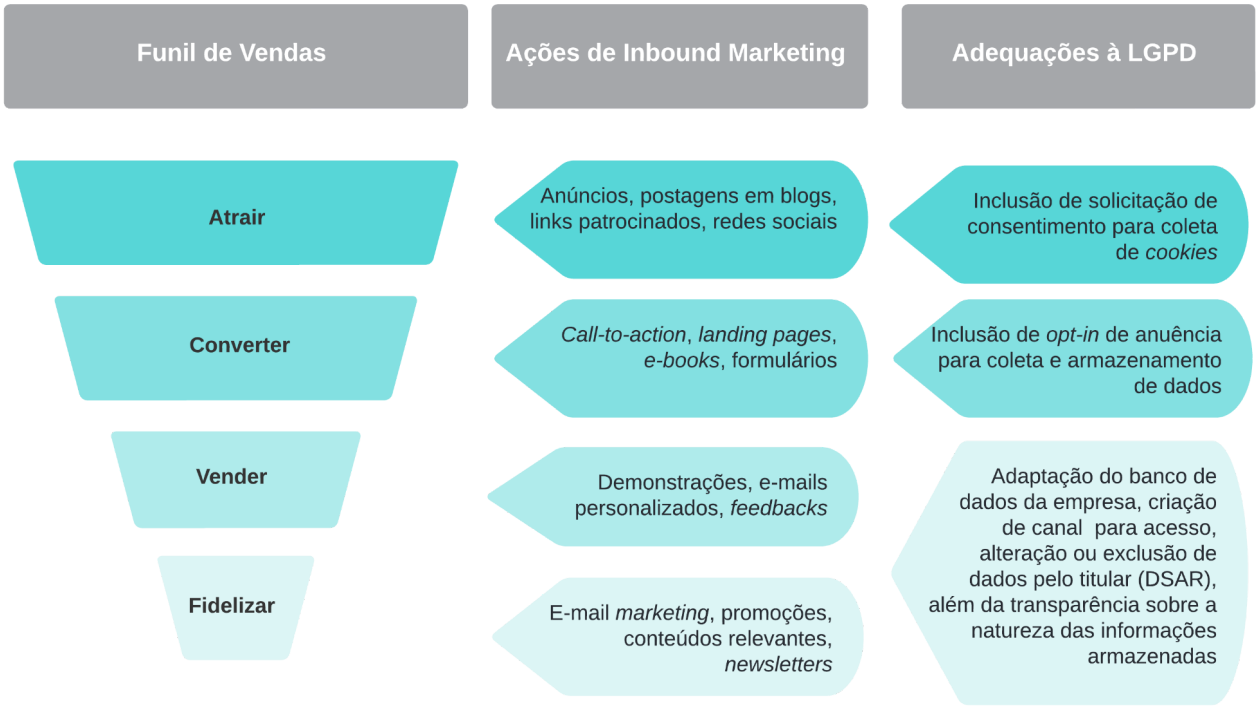
> Na União Europeia, tornou-se relativamente comum que os controladores, ali denominados responsáveis pelo tratamento, disponibilizem canais em seus portais ou plataformas para que os titulares formulem os seus requerimentos. Tal procedimento alinha-se com o esforço à facilitação, ao titular, para o exercício de seus direitos, o que também é esperado dos controladores que se submetem à legislação brasileira, que cuidou de prever, em sentido amplo, o incentivo à facilidade de controle sobre os dados, o que, por óbvio, inclui a própria possibilidade de exercício dos direitos.[79]

---

[78] GARCIA, Lara Rocha; AGUILERA-FERNANDES, Edson, et al. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação.** p.6

[79] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada**.p 265

Figura 4 - Inbound marketing adequações à LGPD



Fonte: Autora (2022)

No que tange a segurança da informação, os dados pessoais são tratados em várias operações de tratamento de dados do nosso dia a dia, e a segurança de informação deve ser garantida em todos os tipos de repositório e em todas as etapas do ciclo de vida do dado.

> Segurança em todo o ciclo de vida da informação: trata-se da preocupação dos sistemas de informação garantirem segurança, do ponto de vista técnico, ao dado pessoal desde o momento de sua coleta até o momento de seu descarte definitivo. Todas as etapas do ciclo de vida de uma informação, o qual pode contemplar coleta, armazenamento, processamento, uso, transmissão e destruição, merecem proteção.[80]

É importante colocar em prática ações que visam mitigar riscos para a empresa em razão do tratamento de dados. As ações prioritárias em um programa

[80] End-to-End Security — Full Lifecycle Protection. Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the fonte: CAVOUKIAN, Ann, Ph.D. **Privacy by Design: The 7 Foundational Principles**. Information & Privacy Commissioner Ontario, Canada, p. 2. Disponível em: [www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf]. Acesso em: 23 abr 2023.

de adequação à LGPD incluem: nomear um encarregado pela proteção de dados pessoais, estabelecer canais de contato para exercício de direitos dos titulares e processos para atendimento das demandas. Por fim, é de suma importância elaborar Políticas de Privacidade.

Se faz necessário uma adequação contratual, prever qual a definição das partes, a responsabilidade de cada uma. Estruturação do procedimento interno de recebimento e resposta à requisições de titulares; elaboração de mapeamento de dados Relatório de Impacto à Proteção de Dados(RIPD)[81] manter registro da gestão do ciclo dos dados; criação de campanhas educativas aos colaboradores; treinamento/capacitação dos colaboradores.

Também é interessante que sejam elaborados programas de conscientização, revisando e adequando todos os procedimentos internos que foram verificados riscos no mapeamento de Dados, por exemplo a coleta excessiva de dados. Alguns pontos chave para realizar este mapeamento, segundo Furtado[82], são: a observância do princípio de responsabilização e da prestação de contas; a necessidade de cumprimento das normas de fiscalização da Autoridade Nacional de Proteção de Dados (ANPD); a conformidade com o princípio da transparência; e a garantia do direito à confirmação do tratamento e do direito de acesso às informações. Para facilitar o registro dos dados pessoais, é recomendado seguir o roteiro a seguir como referência:

Figura 5 - Sugestão Mapeamento de Dados

[81] O RIPD é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). Fonte: **AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso 26 jun 2022

[82] FURTADO, Tiago Neves. **Registro das operações de tratamento de dados pessoais - data mapping - data discovery: porque é importante e como executá-lo**. In: VAINZOF, Rony; OPICE BLUM, Renato; FABRETTI, Henrique. Data Protection Officer: Teoria e Prática de Acordo com a LGPD e o GDPR. São Paulo: Revista dos Tribunais, 2020.

A. QUEM?

Quem envia a informação?	Banco, Hospital, *Site* de Compras, Seguradora, Comércio...
Direção do fluxo	Entrando ou saindo da empresa
Destinatário	Banco, Hospital, *Site* de Compras, Seguradora, Comércio...

B. O QUÊ?

Item dos dados	- Dados do paciente; nome/registro/ contatos... - Dados financeiros - Emissão de NF....
Tipo de conteúdo	- Dados pessoais - Dados pessoais sensíveis
Mídia	- Papel - Transferência *Internet* - Armazenamento digital

C. ONDE?

Onde estão os dados armazenados antes de serem enviados ou depois de terem sido recebidos?	- Pasta física - Disco Computador - Disco de *Backup* - Nuvem
Como o armazenamento de dados é protegido?	- Senha de usuário - Pasta protegida - Criptografado - Nenhum
Mídia	- Papel - Transferência *Internet* - Armazenamento digital

D. QUANDO?

Número de registros por transferência	Pode criar faixas que se adequem melhor à empresa
Método utilizado para a transferência	- *E-mail* - Transferência *Internet* - Dispositivos externos

Fonte: Lima (2020)[83]

Com este registro meticuloso dos dados armazenados, será possível conectar os procedimentos internos do programa de privacidade às políticas de segurança de dados e informações de usuários.

[83] LIMA, Ana Paula Moraes Canto de, et al.(2020) **LGPD - Lei Geral de Proteção de Dados: sua empresa está preparada.** e-book

4.2 Penalidades

As penalidades previstas na Lei Geral de Proteção de Dados (LGPD) representam um mecanismo essencial para garantir o cumprimento das disposições da lei e a proteção adequada dos dados pessoais. A seguir será abordado todas as penalidades previstas na LGPD, detalhando suas características e impactos para as organizações.

A advertência é uma penalidade que pode ser aplicada pela Autoridade Nacional de Proteção de Dados (ANPD) em situações de infrações menos graves da Lei Geral de Proteção de Dados (LGPD). Essa medida consiste em uma notificação formal emitida pela ANPD à organização infratora, com o objetivo de alertar sobre as práticas inadequadas e fornecer orientações para a correção das irregularidades.

No que diz respeito às multas administrativas, elas representam as penalidades mais relevantes previstas na LGPD. A ANPD tem a autoridade para aplicar essas multas em casos de infrações mais graves da lei. O valor das multas pode atingir até 2% do faturamento da organização infratora, com um limite máximo estabelecido na legislação. Essa penalidade tem como finalidade desencorajar práticas inadequadas e garantir a conformidade com a LGPD.

A LGPD também estabelece a possibilidade de publicização da infração cometida pela organização. Nesse sentido, a ANPD pode divulgar publicamente informações sobre a infração, o infrator e a penalidade aplicada. Essa medida tem como propósito promover a transparência e conscientizar o público acerca da importância da proteção de dados pessoais.

Outra medida punitiva prevista na LGPD é o bloqueio dos dados pessoais. A ANPD tem a autoridade para determinar o bloqueio quando a organização infratora não está cumprindo as obrigações legais estabelecidas na LGPD. Esse bloqueio impede que os dados sejam tratados, mas preserva sua integridade e segurança. Essa penalidade visa garantir a proteção dos dados pessoais enquanto a organização se adequa às exigências da lei.

Em situações extremas de infração da LGPD, a ANPD pode determinar a eliminação dos dados pessoais que foram objeto da infração. Essa penalidade implica na exclusão definitiva das informações pessoais coletadas e tratadas de forma inadequada. A eliminação dos dados pessoais tem como objetivo proteger a privacidade e os direitos dos titulares dos dados.

Além disso, a LGPD prevê a possibilidade de suspensão parcial ou total das atividades de tratamento de dados pessoais realizadas pela organização infratora. A ANPD pode determinar a suspensão temporária das operações de tratamento de dados como medida punitiva. Essa penalidade tem como objetivo interromper as práticas inadequadas de tratamento de dados e garantir a proteção das informações pessoais.

Nos casos mais graves de infração da LGPD, a ANPD pode proibir a organização infratora de exercer atividades relacionadas ao tratamento de dados pessoais. Essa penalidade impede completamente a organização de realizar qualquer tipo de tratamento.

É importante ressaltar que as maiores penalidades relacionadas à proteção de dados geralmente são resultado de denúncias e incidentes de privacidade, não necessariamente de uma fiscalização ativa. Os principais fiscalizadores da LGPD são os titulares de dados, os clientes, parceiros de negócios e investidores.

A Autoridade Nacional de Proteção de Dados (ANPD) é responsável pela regulamentação, orientação e fiscalização do cumprimento da LGPD no Brasil desde 1º de agosto de 2021. A ANPD foi criada pela LGPD como um órgão autônomo e independente, vinculado à Presidência da República. Sua principal função é zelar pela proteção dos dados pessoais, garantindo sua utilização adequada por parte das organizações e promovendo a conscientização e a cultura de privacidade na sociedade.

Dentre as atribuições da ANPD, estão a regulamentação e elaboração de diretrizes complementares à LGPD, a fiscalização e aplicação de sanções previstas na lei, a orientação e educação sobre a LGPD, a cooperação nacional e internacional com outras entidades e autoridades, e a resolução de conflitos relacionados à proteção de dados, atuando como mediadora entre as partes envolvidas.

A defesa de uma infração à Lei Geral de Proteção de Dados (LGPD) ocorre por meio de um processo administrativo que é conduzido pela Autoridade Nacional de Proteção de Dados (ANPD). Quando a ANPD identifica uma infração à LGPD, ela inicia o procedimento de apuração e notifica a organização infratora, concedendo-lhe o direito à ampla defesa.

A organização notificada terá um prazo determinado pela ANPD para apresentar sua defesa, onde poderá apresentar argumentos, documentos e evidências que possam justificar ou mitigar a infração. É importante ressaltar que a organização deve se basear em fundamentos legais e técnicos para sustentar sua defesa, demonstrando que está agindo de acordo com os princípios e requisitos da LGPD.

Durante o processo de defesa, a ANPD analisará os argumentos apresentados pela organização, bem como todas as provas e documentos pertinentes ao caso. A autoridade poderá solicitar informações adicionais, realizar diligências ou perícias técnicas, se necessário, para fundamentar sua decisão final.

Após analisar todas as informações e a defesa da organização, a ANPD emitirá uma decisão administrativa. Essa decisão pode resultar na aplicação de penalidades previstas na LGPD, como multas, advertências, bloqueio de dados, eliminação de dados, suspensão de atividades relacionadas ao tratamento de dados ou até mesmo proibição do exercício de determinadas atividades.

É importante ressaltar que a defesa de uma infração à LGPD deve ser embasada em sólidos argumentos legais e técnicos, além de uma postura cooperativa e transparente perante a autoridade. É recomendado que as organizações busquem assessoria jurídica especializada em proteção de dados para auxiliá-las no processo de defesa, garantindo que todos os aspectos legais e regulatórios sejam adequadamente considerados.

É fundamental que as organizações estejam cientes das suas obrigações e responsabilidades previstas na LGPD, adotando medidas proativas de conformidade para minimizar o risco de infrações e garantir a proteção adequada dos dados pessoais que tratam. A prevenção e a conformidade contínua são essenciais para evitar situações de infração e as consequentes penalidades.

5 CONSIDERAÇÕES FINAIS

A LGPD implicou em impactos significativos no campo do *inbound marketing*, exigindo a obtenção de consentimento explícito dos consumidores, implementação de medidas de segurança e proteção de dados, respeito aos direitos dos consumidores e transparência nas políticas de privacidade. Apesar dessas exigências, o *inbound marketing* continua sendo uma estratégia valiosa para as empresas que optam por seguir utilizando-a em conformidade com a LGPD.

O *inbound marketing* é benéfico para os consumidores, uma vez que oferece conteúdo relevante e informativo, personalização das interações, maior engajamento, comunicação transparente e menor interrupção. A disponibilização de conteúdo valioso permite aos consumidores obter informações úteis para solucionar problemas e expandir seus conhecimentos. Além disso, a personalização das estratégias permite que os consumidores recebam conteúdos direcionados às suas necessidades e interesses específicos, o que resulta em uma experiência mais satisfatória.

A interação e o engajamento promovidos pelo *inbound marketing* permitem que os consumidores participem ativamente das ações de marketing, compartilhem opiniões e sintam-se parte de uma comunidade. Isso fortalece o relacionamento entre as empresas e os consumidores, proporcionando um ambiente de confiança e envolvimento.

A transparência na comunicação é um valor essencial dessa estratégia, garantindo que as empresas forneçam informações claras sobre seus produtos e serviços. Isso permite que os consumidores tomem decisões de compra mais informadas, evitando surpresas desagradáveis e construindo uma relação de confiança com as marcas.

Uma vantagem adicional do *inbound marketing* é a redução da interrupção na experiência do consumidor. Ao contrário das estratégias tradicionais de marketing que são intrusivas, o *inbound marketing* atrai os consumidores de forma não invasiva, permitindo que eles busquem informações quando desejarem, sem serem interrompidos por anúncios indesejados. Isso cria um ambiente mais positivo para o consumidor, que tem maior controle sobre o processo de compra.

Além disso, o *inbound marketing* oferece recursos gratuitos e cupons de desconto, proporcionando aos consumidores acesso a informações adicionais e

benefícios sem custo. Essa abordagem de compartilhamento gratuito de conhecimento demonstra o valor que as empresas podem oferecer aos consumidores antes mesmo de solicitar qualquer forma de reciprocidade.

Portanto, mesmo com os requisitos impostos pela LGPD, o *inbound marketing* continua sendo uma estratégia valiosa para as empresas que desejam estabelecer um relacionamento positivo com os consumidores. Ao seguir as diretrizes da LGPD, as empresas podem garantir a proteção dos dados dos consumidores e oferecer uma experiência de consumo personalizada, relevante e transparente, que atende às expectativas dos consumidores e fortalece a relação entre marcas e consumidores.

REFERÊNCIAS

AMBLER, Tim. **The new dominant logic of Marketing:** views of the elephant. London: Centre for Marketing of London Business School, 2004. Working Paper, n. 04-903.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.658, de 26 de abril de 2018.** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF, 27 abr. 2018. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/normativo.asp?numero=4658&tipo=Resolu%C3%A7%C3%A3o. Acesso em: 18 mar. 2023.

BARTELS, Robert. **The History of Marketing Thought.** Ohio, 1976. Disponível em: https://people.missouristate.edu/chuckhermans/bartels.htm. Acesso em: 10 mai.2022

BIONI, Bruno. **LGPD: Lei Geral de Proteção de Dados Pessoais Comentada.** 1ª ed. São Paulo: Revista dos Tribunais, 2020.
BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Decreto nº 6.135, de 26 de junho de 2007.** Regulamenta a Lei nº 10.836, de 9 de janeiro de 2004, que cria o Programa Bolsa Família, e a Lei nº 10.689, de 13 de junho de 2003, que institui o Cadastro Único para Programas Sociais do Governo Federal, e dá outras providências. Diário Oficial da União, Brasília, DF, 27 jun. 2007. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/decreto/d6135.htm. Acesso em: 25 mar. 2023.

BRASIL. **Decreto nº 6.425, de 4 de abril de 2008.** Regulamenta o art. 11 da Lei nº 11.494, de 20 de junho de 2007, que regulamenta o Fundo de Manutenção e Desenvolvimento da Educação Básica e de Valorização dos Profissionais da Educação - FUNDEB, quanto à coleta, ao tratamento e à divulgação de dados fiscais e financeiros, e ao censo escolar da educação básica. Diário Oficial da União, Brasília, DF, 7 abr. 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6425.htm. Acesso em: 25 mar. 2023.

BRASIL. **Decreto nº 8.777, de 11 de maio de 2016.** Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações públicas, para tratar das normas sobre dados abertos. Diário Oficial da União, Brasília, DF, 12 maio 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8777.htm. Acesso em: 25 mar. 2023.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Diário Oficial da União, Brasília, DF, 11 jan. 2001. Disponível em:

http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp105.htm. Acesso em: 18 mar. 2023.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 18 mar. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 25 mar. 2023.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990.** Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, DF, 16 jul. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8069.htm. Acesso em: 18 mar. 2023.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996.** Lei de Interceptação Telefônica e Telemática. Diário Oficial da União, Brasília, DF, 25 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9296.htm. Acesso em: 25 mar. 2023.

BRASIL. **Lei nº 9.472, de 16 de julho de 1997.** Lei Geral de Telecomunicações. Diário Oficial da União, Brasília, DF, 17 jul. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9472.htm. Acesso em: 25 mar. 2023.

BRASIL. **Lei nº 9.507, de 12 de novembro de 1997.** Regulamenta o direito de acesso a informações e disciplina o rito processual do habeas data. Diário Oficial da União, Brasília, DF, 13 nov. 1997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9507.htm. Acesso em: 18 mar. 2023.

BRASIL. **Lei nº 9.983, de 14 de julho de 2000.** Altera dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, e dá outras providências. Diário Oficial da União, Brasília, DF, 17 jul. 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L9983.htm. Acesso em: 25 mar. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial no 1.758.799 - MG (2017/0006521-9)**. Recorrente:PROCOB S⁄A. Recorrido:JOSÉ GALVÃO DA SILVA. Relator:Ministra NANCY ANDRIGHI. Julgamento em: 12 de Novembro de 2019. Número do processo: REsp 0039441-55.2013.8.13.0693 MG 2017/0006521-9.

BOVENS, Mark. **Analysing and assessing public accountability: a conceptual framework.** European Journal of Political Research, v. 37, n. 4, p. 391-412, 2000.

CAMERON, Kim. **The laws of identity**. 2005. Disponível em:

http://myinstantid.com/laws.pdf. Acesso em: 15 jun. 2022.

CAMILLO, Gerson Luiz. **Privacidade no controle de acesso em sistemas de gerenciamento de identidade para a Web.** 2018. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Santa Catarina, Florianópolis, 2018. Orientadora: Carla Merkle Westphall.

CANEDO, Letícia Bicalho. **A Revolução Industrial.** Campinas: Editora Atual; Unicamp, 1998.

CAVOUKIAN, Ann, Ph.D. **Privacy by Design: The 7 Foundational Principles.** Information & Privacy Commissioner Ontario, Canada, p. 2. Disponível em: [www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf]. Acesso em: 23 set. 2022.

CHAUVEL, Marie Agnes. (2000). **Consumidores insatisfeitos: uma oportunidade para as empresas.** Rio de Janeiro: Mauad.

CHO, Chang-Hoan.; CHEON, Hongsik. **Why do people avoid advertising on the internet?** Journal of Advertising, v. 33, n. 4, 2004. DOI: 10.1080/00913367.2004.10639175.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.821, de 23 de novembro de 2007**. Dispõe sobre a vedação de indicação de tratamento de caráter experimental e terapias antineoplásicas de alta complexidade fora da modalidade hospitalar e dá outras providências. Diário Oficial da União, Brasília, DF, 6 dez. 2007. Seção 1, p. 199. Disponível em: http://www.portalmedico.org.br/resolucoes/CFM/2007/1821_2007.htm. Acesso em: 18 mar. 2023.

COTS, Márcio. **Comentários à Lei Geral de Proteção de Dados Pessoais.** 1ª ed. São Paulo: Revista dos Tribunais, 2020.

ALMEIDA, Lucas Rodrigo Santos de. **Repensar e reaprender na era pós-digital**. Revista de Administração de Empresas, São Paulo, v. 57, n. 5, p. 520-521, 2017. Disponível em: https://www.scielo.br/j/rae/a/g3GKyG9qKQH9FJWCb7QpJrM/?lang=pt. Acesso em: 09 set 2022.

DIJCK, José van. **Datafication, dataism and dataveillance: big data between scientific paradigm and ideology.** Surveillance and Society, v. 12, n. 2, 2014.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 2ª ed. Rio de Janeiro: Renovar, 2013,

DUARTE, Juliano Franco. **O livro proibido do marketing: Inbound Marketing,** Marketing de Conteúdo e Hacks para sua empresa crescer. Edição do Kindle. 2020.

ERBISTI, Marcos; SUAREZ, Maribel Carvalho. **Ad Blocking: Discursos de Adoção e de Anticonsumo da Publicidade.** Revista de Administração de Empresas, São

Paulo, v. 59, n. 3, p. 227-238, jun. 2019. Disponível em: <https://www.scielo.br/j/rae/a/dnbzhY8bZdyvjKzJTW5pNzR/?lang=pt>. Acesso em: 01 jun. 2019.

GABRIEL, Martha; KISO, Rafael. (2010). **Marketing na Era Digital: Conceitos, plataformas e estratégias**. Novatec Editora. Página 174.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação.** São Paulo: Blucher, 2019. 1 e-book.

HALLIGAN, Brian; SHAH, Dharmesh. **Inbound Marketing,** Revised and Updated. 2009. Wiley. e-book Kindle.

HAUK, Chris, **Browser Fingerprinting: What Is It And What Should You Do About It?** 2022. Disponível em: <https://pixelprivacy.com/resources/browser-fingerprinting/> Acesso em: 7 jun. 2022.

ITU. **International Telecommunication Union. Estatísticas da UIT.** [Online]. Disponível em: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Acesso em: 05 mai. 2023.

JONES, Michael. B. **The emerging JSON-based identity protocol suite.** W3C workshop on identity in the browser, 2011.

KOTLER, Philip., KARTAJAYA, Hermawan. & SETIAWAN, Iwan. (2017). **Marketing 4.0: Mudança do Tradicional para o Digital.** e-book.

KOTLER,Philip et al. **Marketing 5.0: tecnologia para a humanidade.** Rio de Janeiro: Sextante, 2017. e-book. p.108

KOTLER, Philip. **Marketing Insights from A to Z: 80 Concepts Every Manager Needs to Know. 2003**. e-book.

LAS CASAS, Alexandre Las. **Marketing: uma introdução. In: Marketing: Conceitos, Exercícios e Casos.** São Paulo: Editora Atlas, 2001.

LIMA, Ana Paula Moraes Canto de, et al.(2020) **LGPD - Lei Geral de Proteção de Dados: sua empresa está preparada.** e-book.

LUPTON, Deborah. **The Quantified Self.** Cambridge, UK: Polity Press, 2016.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada.** São Paulo: Revista dos Tribunais, 2020.

MARQUES, Humberto; LEVI, Renato. **Funil de Vendas: um jeito fácil para você realizar bons negócios.** Edição do Kindle. Editora Senac São Paulo, 2020.

OECD. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Organisation for Economic Co-operation and Development, September 1980. Disponível em:

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html. Acesso em: 22 jun. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** Paris: ONU, 1948. Disponível em: http://www.dudh.org.br. Acesso em: 18 mar. 2023.

PETERS, Richard; SIKORSKI, Robert. **"Cookie Monster?"** Science (American Association for the Advancement of Science) 278.5342 (1997): 1486-487. Web.

ROCHA, Angela. CHRISTENSEN, Carl., **Marketing, Teoria e prática no Brasil.** 2. Ed. São Paulo: Atlas, 1999.

SANTOS, Tatiani; LIMA, Mayana Virginia Viégas; BRUNETTA, Douglas Fernando; FABRIS, Carolina; SELEME, Acyr. **O desenvolvimento do Marketing: uma perspectiva histórica.** Revista de Gestão, v. 16, n. 1, art. 5, 2009.

SWIRE, Peter; AHMAD, Karim. **Encryption and Globalization. Science and Technology Law Review,** v. 13, n. 2, 2012. DOI: 10.7916/stlr.v13i2.3964. Disponível em: https://journals.library.columbia.edu/index.php/stlr/article/view/3964. Acesso em: 6 jul. 2022.

WEBSTER JR., Frederick. **Marketing in changing times.** Marketing Management, v. 11, n. 1, Jan.-Feb. 2002.

ZUIDERVEEN BORGESIUS, Frederik J. **"Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation."** The Computer Law and Security Report 32.2 (2016): 256-71. Web.