



**UNIVERSIDADE ESTADUAL DA PARAÍBA  
CAMPUS III  
CENTRO DE HUMANIDADES  
CURSO DE BACHARELADO EM DIREITO**

**JEFFERSON GALDINO DA COSTA**

**PROTEÇÃO DA PRIVACIDADE E DE DADOS PESSOAIS:**

Relações de consumo e coleta de dados por High Techs, redes sociais e internet.

**Guarabira/PB  
2021**

**JEFFERSON GALDINO DA COSTA**

**PROTEÇÃO DA PRIVACIDADE E DE DADOS PESSOAIS:**

Relações de consumo e coleta de dados por High Techs, redes sociais e internet.

Trabalho de Conclusão de Curso de Graduação em Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharel em Direito.

**Área de concentração:** Direito do Consumidor e Direito Penal.

**Orientador:** Profa. Dra. Hérika Juliana Linhares Maria

**GUARABIRA/PB**

**2021**

**JEFFERSON GALDINO DA COSTA**

**PROTEÇÃO DA PRIVACIDADE E DE DADOS PESSOAIS:** Relações de consumo e coleta de dados por High Techs, redes sociais e internet.

Trabalho de conclusão de curso (Artigo) apresentado ao Departamento do curso de Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de concentração: Direito do Consumidor. Direito Penal.

Aprovado em: 26/05/2021.

**BANCA EXAMINADORA**



---

Prof<sup>a</sup>. Dr. Hérica Juliana Linhares Maia (Orientadora)  
Universidade Estadual da Paraíba (UEPB)



---

Prof. Me. Felipe Viana de Mello  
Universidade Estadual da Paraíba (UEPB)



---

Prof. Esp. Kleyton César Alves da Silva Viriato  
Universidade Estadual da Paraíba (UEPB)

É expressamente proibida a comercialização deste documento, tanto na forma impressa, como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano do trabalho.

C837p Costa, Jefferson Galdino da.  
Proteção da privacidade de dados pessoais [manuscrito] :  
relações de consumo e coleta de dados por High Techs, redes  
sociais e internet / Jefferson Galdino da Costa. - 2021.  
31 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) -  
Universidade Estadual da Paraíba, Centro de Humanidades ,  
2021.

"Orientação : Profa. Dra. Herika Juliana Linhares Maia ,  
Coordenação do Curso de Direito - CH."

1. Direito do consumidor. 2. Privacidade. 3. Proteção  
dedados. 4. Rede social. I. Título

21. ed. CDD 343.071

## **AGRADECIMENTOS**

O desenvolvimento deste singelo trabalho contou a ajuda de diversos entes, entre os quais agradeço:

Primordialmente a DEUS por permitir tal feito e nos guardar constantemente a cada dia e pelas suas misericórdias infinitas em nossa vida.

A meus familiares, principalmente minha Mãe, Dona Célia que tem me ajudado sobre medida e sido meu porto seguro e inspiração.

A meu tio Nal que nos ajudou em cada empreitada com sua grande empatia.

A minha irmã Jacielly que sempre nos incentiva e suas palavras de apoio nos melhores e piores momentos.

A minha namorada Karla que me apoia constantemente, me ladeando nesse caminho de conquistas e nas lutas passageiras, a qual amo mais a cada dia.

Aos nossos companheiros de lida que nos apoiam sempre e demais contribuintes desta obra que de maneira direta ou indireta contribuíram na feitura deste ato, afinal: QUEM SOU EU SEM MEUS IRMÃOS?

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>07</b>
<b>2</b>	<b>AS RELAÇÕES DE CONSUMO E AS REDES SOCIAIS VIRTUAIS .....</b>	<b>08</b>
2.1	Os elementos caracterizadores da relação de consumo.....	08
2.2	A internet e os seus reflexos no ato de consumir.....	09
2.3	O consumo virtual e a violação à privacidade do consumidor .....	11
<b>3</b>	<b>COLETA DE DADOS NAS REDES SOCIAIS .....</b>	<b>15</b>
3.1	Inteligência e contra inteligência.....	15
3.2	Cibercrimes.....	17
3.3	Tipos de informações que são alvo e como se proteger.....	19
<b>4</b>	<b>A TUTELA DA PRIVACIDADE DO CONSUMIDOR E A LEI GERAL DE PROTEÇÃO DE DADOS – LEI 13.709/18 .....</b>	<b>21</b>
4.1	Objetivo da lei 13.709/18.....	21
4.2	MUDANÇAS PROPORCIONADAS PELA LEI.....	22
4.3	A LGPD E A PRIVACIDADE DO USUÁRIO .....	23
<b>5</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>24</b>
	<b>REFERÊNCIAS.....</b>	<b>27</b>

**PROTEÇÃO DA PRIVACIDADE E DE DADOS PESSOAIS:  
RELAÇÕES DE CONSUMO E COLETA DE DADOS POR HIGH TECHS, REDES  
SOCIAIS E INTERNET.**

**PROTECTION OF PRIVACY AND PERSONAL DATA:  
CONSUMER RELATIONS AND DATA COLLECTION BY HIGH TECHS, SOCIAL  
NETWORKS AND THE INTERNET.**

Jefferson Galdino da Costa <sup>1</sup>

**RESUMO**

O presente artigo aborda como tema central a privacidade dos cidadãos que utilizam de bens e serviços virtuais, sendo alvos de coletas de dados indevidas por empresas tecnológicas, afetando diretamente nas relações de consumo e na garantia de seus direitos fundamentais. Dessa maneira, foram utilizadas informações com a finalidade de informar e dar conhecimento às pessoas de modo que aumentem os cuidados no dia a dia na utilização desses produtos disfarçados de entretenimento, comunicação, entre outros. Destarte, foram discutidas relações sócio-tecnológico-jurídicas que se perfazem na internet, além de temas atuais como o cibercrime e seus perigos ao usuário desavisado. Também foi feita uma análise da Lei Geral de Proteção de Dados, Lei 13.709/2018 ou LGPD, com seus objetivos e algumas das mudanças angariadas. Assim, por meio de uma pesquisa qualitativa de caráter indutivo, bibliográfico e documental que se deu através de doutrinas, costumes societários e jurisprudências pátrias atualizadas acerca do tema foi constatado que há, de maneira clara, relações de consumo entre usuário (consumidor) e as redes sociais virtuais (fornecedor), além de seus reflexos na sociedade e na privacidade do indivíduo, demonstrando a efetiva necessidade de garantir mais proteção a parte hipossuficiente na relação supracitada.

**PALAVRAS-CHAVE:** Direito do consumidor. Privacidade. Proteção de dados. Rede social.

**ABSTRACT**

This article addresses as a central theme the privacy of citizens who use virtual goods and services, being targets of improper data collection by technological companies, directly affecting consumer relations and guaranteeing their fundamental rights. In this way, information was used with the purpose of informing and giving knowledge to people in order to increase care in the day-to-day use of these products disguised as entertainment, communication, among others. In this way, the socio-technological-legal relations that take place on the internet were discussed, in addition to current topics such as cybercrime and its dangers to the unformed user. An analysis was also made of the Lei Geral de Proteção de Dados, Lei 13.709 / 2018 or LGPD, with its objectives and changes raised. Thus, through a qualitative research of an inductive, bibliographic and documentary character that took place through doctrines, corporate customs and updated national jurisprudence on the theme, it

<sup>1</sup> Bacharelado em Direito pela Universidade Estadual da Paraíba. 1º Tenente e instrutor na Polícia Militar da Paraíba. Jeff007costa@gmail.com.

was found that there are, clearly, consumer relations between user (consumer) and the virtual social networks (supplier), in addition to their reflexes on society and the individual's privacy, demonstrating the effective need to guarantee more protection to the under-sufficiency part of the aforementioned relationship.

**KEYWORDS:** Consumer Rights. Privacy. Data Protection. Social network.

## 1 INTRODUÇÃO

Antes do século XXI, grupos sociais se traduziam em agrupamentos de pessoas que tinham algo em comum e que se encontravam presencialmente em local físico para construir uma relação de diversão, trabalho, ou o que quer que seja. Já, atualmente, os grupos em que a maior parte das pessoas faz parte se traduzem em formas de relacionamento social online. As barreiras do presencial foram quebradas e as redes sociais virtuais influem cada dia mais na forma como se vive o dia a dia.

O presente trabalho tem por desígnio atingir uma observação transdisciplinar, jurídica com aspectos sociológicos dos ambientes virtuais que oferecem serviços e produtos ao cidadão, elencando normativos que são reguladores das atividades fornecedoras supracitadas.

Neste contexto, os questionamentos que nortearam a elaboração deste trabalho foram: os termos de uso e de privacidade dos aplicativos e sites como facebook/instagram ou de empresas de tecnologia respeitam os direitos do consumidor e os direitos fundamentais como a liberdade na manifestação do pensamento, a segurança, a intimidade e a vida privada? A Lei Geral de Proteção de Dados, lei 13.709/18 ou LGPD, tem feito o seu papel de proteger o cidadão e o consumidor da força econômica e de manipulação das *High Techs*? Quais os tipos de informações expostas em redes sociais que facilitam o ataque de criminosos por meios virtuais?

A incumbência deste artigo é, justamente, ponderar sobre e problematizar a questão do tratamento das informações e dados pessoais no campo da sua utilização comercial e institucional, tendo como baldrame legal do consentimento dos titulares e proprietários dos mesmos. Não há, de tal forma, intenção de solucionar o tema ou esgotar as discussões que o permeiam, mas discorrer sobre nuances, situações fáticas e limites para o manuseio de tais dados em conformidade com as garantias individuais do tema.

Esta pesquisa tem como meta específica, entre outras, levantar se há uma relação de consumo realmente quando o usuário faz uso das redes sociais virtuais e de sites na internet e se ele está sendo respeitado quanto a sua privacidade e ao seu livre desígnio de aceitação para que outros usem seus dados e informações. Conhecer mais sobre temas como inteligência, contrainteligência e cibercrime, assim como aspectos da fragilidade do usuário de redes sociais virtuais. Conhecer os principais aspectos legais sobre o uso de dados dos usuários como armazenamento, tratamento e uso comercial ou não. Analisar e discorrer sobre a Lei Geral de Proteção de Dados, Lei 13.709/18 quanto a seu aspecto teleológico e algumas mudanças proporcionadas. Identificar e descrever padrões de hábitos que transformam as pessoas em alvos fáceis no mundo cibernético a criminosos.

O presente trabalho trata-se de uma pesquisa bibliográfica, a qual segundo Lakatos e Marconi (1991), procura a explicação de um problema a partir de referências teóricas publicadas em documentos. Ainda, de acordo, busca conhecer e analisar as contribuições culturais ou científicas existentes sobre um determinado assunto, tema ou problema. Envolve toda a bibliografia já publicada com ligação ao tema estudado, que vai desde publicações isoladas, jornais, revistas, livros, monografias, teses, artigos, material cartográfico e meios de comunicação como rádio, gravações em fita magnética e audiovisual como filmes ou televisão.

O método de abordagem utilizado foi o indutivo, pois segundo Rodrigues (2007) se refere a um processo mental que, através de dados particulares, satisfatoriamente averiguados, entende-se uma verdade total ou universal, não contida nas partes estudadas. Assim busca-se base para a pesquisa em sites, aplicativos, termos de contrato de uso de empresas de tecnologia, legislações nacionais e internacionais, trabalhos sobre o tema, além de tantas outras fontes.

Em momentos que a imagem humana é tratada por diversos meios, tantas maneiras e levada como meio de capitalização por empresas multinacionais se figura altamente relevante que a privacidade e outros direitos sejam discutidos e sintetizados em garantias. Portanto, urge a importância em se discutir o tema para que não se esqueça em nenhum campo que a privacidade é resguardada pelos normativos nacionais de mais expressão como a Constituição Federal de 1988 e outras legislações.

## **2. AS RELAÇÕES DE CONSUMO E AS REDES SOCIAIS VIRTUAIS**

A modernidade trouxe consigo mudanças expressivas na maneira de relacionamento entre as pessoas, criando conexões tão profundas que aproximou as relações na mesma medida em que as afastou. O advento das redes sociais virtuais tornou-se uma saída rápida e atraente em um mundo onde se está sempre com pressa, fornecendo aos seus usuários um acesso rápido, grátis, por tempo indeterminado e de onde quer que se encontrem. Seguindo a idéia das High techs, como demonstrou Maidique e Hayes (1984), quer seja a busca da excelência nos processos tecnológicos. Entretanto, o questionamento que surge é: qual o preço que se paga por tamanha facilidade desse tipo de serviço?

### **2.1. Os Elementos caracterizadores da Relação de Consumo**

Existem vários serviços *on-line* que são oferecidos ao consumidor, mesmo sem nenhuma forma de pagamento aparente. Vários desses serviços aparecem comumente na forma de redes sociais, oferecendo armazenamento de fotos, vídeos e textos enganosamente grátis.

Para Fabrício Bolzan de Almeida (2013, p. 74) a relação de consumos e vislumbra classificada como a: “relação firmada entre consumidor e fornecedor, a qual possui como objeto a aquisição de um produto ou a contratação de um serviço”. Para tratar sobre a relação de consumo entre o usuário e as redes sociais é preciso trazer os conceitos dos elementos que perfazem essa ligação. Sendo os elementos subjetivos: o consumidor e o fornecedor e os objetivos: o produto ou o serviço.

Primeiramente, em se tratando dos elementos subjetivos da relação, deve-se caracterizar o consumidor, quer seja, conforme a lei 8.078/90: “consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final” ou “a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo”, conforme elenca o artigo 2º do CDC e o seu parágrafo único. Também, por equiparação, define a lei em seu artigo 17: “todas as vítimas do dano causado pelo fato do produto e do serviço” e no artigo 29: “todas as pessoas determináveis ou não, expostas às práticas nele previstas”. Assim, a lei adota quatro conceitos da figura do consumidor, que são distintos, mas coesos entre si, integrando um conjunto de situações em que alguém pode gozar da tutela protecionista confeccionada pelo CDC (BRASIL, 1990).

Num segundo momento, encontramos a definição de fornecedor no artigo 3º do CDC como sendo:

Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços (BRASIL, 1990).

Ou conforme elenca João Batista de Almeida (2017), fornecedor é não apenas quem produz ou fabrica, industrial ou artesanalmente, em estabelecimentos industriais centralizados ou não, como também quem vende, ou seja, comercializa produtos nos milhares de pontos de venda espalhados no território nacional.

E quanto aos elementos objetivos da relação de consumo temos que o produto se define como “qualquer bem, móvel ou imóvel, material ou imaterial. Já serviço é “qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista”, como trouxe o Código de Defesa do Consumidor (BRASIL, 1990).

Ainda, segundo o entendimento doutrinário, pode-se elencar outro elemento, o finalístico, assim, em uma perspectiva teleológica em que o consumidor é o destinatário final do produto ou serviço (AGNE, DOS SANTOS, NOVACKI, 2016).

Consolida-se a cada dia uma espécie de mineração que busca, através da ação dos internautas e usuários, conseguir o máximo de informações e dados pessoais que possam influenciar nas relações de consumo, seja mostrando as preferências de certos públicos de consumidores ou realmente as necessidades individuais que são expostas no acesso particular e privado de cada pessoa. A LGPD (2018), em seu artigo 5º, define como dado pessoal qualquer informação relacionada à pessoa natural, identificada ou identificável.

Desse modo o usuário se caracteriza como consumidor enquanto faz uso dos serviços de armazenamento de dados, plataformas de pesquisa de pessoas, assuntos ou produtos como usuário final. Serviços que por sua vez são oferecidos pelas empresas de rede social virtual como, por exemplo: Facebook, Instagram, Whatsapp, Youtube, etc. Havendo como remuneração, por tal serviço prestado, a venda de informações dos usuários para quaisquer tipos de empresas, invadindo os espaços privados em detrimento das garantias fundamentais como se mostrará neste trabalho.

## **2.2 A Internet e os seus reflexos no ato de consumir**

A nova era estabelece um modelo social, técnico e econômico novo que rescinde o modelo de produção já constituído por Henry Ford, por meio da evolução tecnológica vinda com a internet e de novas tecnologias digitais, chamadas “da informação” ou TI. Dessa forma a informação gera mais informação e este é o produto do meio que obtém cada vez mais valor do mercado, por meio do seu tratamento adequado para o fim desejado, dentro de um contexto de consumo crescente e da movimentação de bens sob o aspecto globalista (BOFF; FORTES; e FREITAS, 2018, p. 16 *apud* FONSECA e NOGUEIRA *in* GROSSI, 2020).

O faturamento do comércio eletrônico no Brasil passou de 18,7 pra 41,3 bilhões de reais entre 2011 e 2015 conforme demonstra relatório *webshoppers*

divulgado pela empresa E-bit (2016). Dados que mostram um elevado crescimento do número de compras online na atualidade. Fatos que são vistos através da facilidade da compra online por diversas maneiras: débito, crédito, boleto, entrega a cobrar, como também do acesso cada vez mais frequente de crianças e adolescentes comprando online, tanto para si, como para adultos com pouca habilidade.

Todos os sites não governamentais ou que não sejam de instituições sem fins lucrativos são permeados por *pop-ups*, aqueles balões de anúncios, ou outros meios de propagandas online. Também a maioria esmagadora dos aplicativos que são usados pela população cotidianamente possui esses anúncios que buscam atrair os consumidores para todo tipo de compra ou aquisição de serviços. Isso quando não conseguem se tornar o próprio produto ou serviço, quando oferecem o conteúdo interno “sem propagandas” ou através de alguma prestação pecuniária. Assim quando não são o produto em si, passam a anunciar “parceiros” que pagam pela propaganda repetitiva.

Várias são as experiências dos internautas que buscando algum serviço ou informação online e tiveram que lutar contra vários balões de anúncios que surgiram do nada e passaram a tapar quase toda a tela de navegação, dificultando o acesso ao objetivo final do usuário.

Assim, o uso corriqueiro de sites e aplicativos, quaisquer que sejam, se torna em um passeio por vitrines online que tentam pescar o utente de alguma forma, chamando sua atenção. Acomodando, de tal maneira, os três elos de uma relação de consumo, sendo, um consumidor que é o internauta ou usuário de aplicativo, um fornecedor que é o próprio aplicativo, seu desenvolvedor, o site ou o anunciante e o produto que pode ser o site oferecendo acesso livre, ou acesso sem anúncios, como também o aplicativo com suas funcionalidades plenas, sem anúncios ou limitadas com anúncios. Relações de consumo estas que ocorrem no meio virtual por entre os sites e aplicativos ligados a rede mundial de computadores.

Em tempos permeados pela ubiquidade computacional que se dá através da presença ininterrupta da computação no dia a dia moderno, a ciência mercadológica promove o agenciamento segmentado e personalizado dos bens de consumo. Assim, os dados pessoais se tornam um bem estratégico para a garantia de sucesso comercial. Destarte, surge um novo exemplo de negócio, onde os consumidores deixam de contra prestar em pecúnia e passam a submeter em troca os seus dados e informações sensíveis sobre seus hábitos e suas intenções ou preferências.

Surge assim a publicidade comportamental que é levada através da força motriz da informação direcionada, traduzindo-se em um consumo direcionado, que se encaixa nas vontades do cliente. Ela é mantida pelos bancos de dados que são alimentados pelos cookies, além de outras ferramentas online. De tal forma que quase infalivelmente, de posse das preferências do usuário, se veiculam mensagens publicitárias que atingirão seus objetivos. Tornando-se assim, o consumidor, em mais uma peça chave que deixa o polo passivo da relação para influir diretamente no processo, sendo um agente de criação de forma instantânea (NOGUEIRA e FONSECA *apud* GROSSI, 2020).

Dessa forma, para entender o contexto atual, buscam-se aspectos históricos, os quais apontam que por influência do liberalismo, que já aparecia no Código Civil de 1916, surgiram vários temas como a liberdade de contratar, a autonomia da vontade e o *pacta sunt servanda*, entre outros.

Após a segunda guerra mundial o capitalismo ditou as regras para o modo de produção industrial, que passou a ser cada vez mais veloz, com tecnologia de ponta,

ou *High Techs* – como são chamadas as empresas de tecnologia -, automação industrial, satélites ligando o mundo, computação, como afirma Frieden (2008). No início do século XX, objetivos como diminuir os custos de produção, aumentar a oferta e captar uma maior parte da população, fizeram surgir o modelo de produção em massa que implica em uma padronização dos produtos oferecidos.

Chegando a meados do século XXI com a ideia da globalização em pleno vigor e influenciando cada vez mais nações que passaram a unificar e mesclar diversos costumes, ideias e formas de consumir. Surgiram assim os contratos de adesão (antes chamados de contratos-padrão) que seguindo a ideia de produção em massa, massificação do direito e o seu cultivo, possuindo caráter unilateral e de simples aceitação pelos consumidores que fossem adquirir os produtos ou serviços à época (GORENDER, 1997).

Acostando-se as primeiras décadas do século XXI com o consumo virtual massificado em meio à sociedade, como supracitado, e fazendo parte da cultura moderna surgiram às redes sociais virtuais que oferecem compartilhamento e armazenamento de dados como fotos, vídeos, áudios e mensagens com diversos círculos de relacionamento. Mesmo assim, nos dias de hoje, não houve o abandono dos contratos de adesão pelas grandes empresas de tecnologia como Google, Samsung, Facebook, que não dão alternativas ao cidadão para consumir o seu “produto” de outra forma a não ser a preestabelecida nos termos de uso, que da maneira com que são postas, violam as garantias individuais.

### **2.3. O consumo virtual e a violação à privacidade do consumidor**

As empresas que detém o controle das redes sociais virtuais se enquadram perfeitamente no conceito da pós-modernidade, que conforme afirmou Bauman (1999, p.30), “vivem num estado de permanente pressão para se despojar de toda interferência coletiva no destino individual, para desregular e privatizar.” Recaindo assim, toda essa definição nas características que se encontram nas relações de consumo no cyber espaço, com amplo grau de privatização e uma desregulamentação sem tamanho, ferindo exacerbadamente alguma proteção que se possa pensar para o consumidor, polo vulnerável e, às vezes, hipossuficiente da relação de consumo.

Um excelente ponto de ancoragem, quanto à privacidade, foi publicado em 1948. A Declaração Universal dos Direitos Humanos (DUDH), e estabeleceu em seu artigo 12º, que “ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (BRASIL, 2018).

É impossível usar um *smartphone* ou alguma rede social como Facebook, Instagram, Whatsapp, TikTok, LinkedIn, etc, sem concordar com os seus termos de uso ou sem permitir que eles “usem os dados dos usuários para melhorar os serviços”, entre outras coisas, pois ao querer resguardar os seus dados pessoais cotidianos, não é possível aceitar os termos preestabelecidos, por que não há opções de meio termo. Não há opções de se abster em compartilhar informações privadas diariamente, ininterruptamente. Assim, os serviços oferecidos por tais empresas são vinculados a troca ou paga com dados pessoais, gerando assim, a cada dia, mais ilusão de gratuidade – pois é pequena a parcela da população que realmente lê os termos de uso daquelas empresas acima - e mais lucro pelas informações íntimas e privadas de parcelas gigantescas da sociedade. Lucro que é

gerado na troca por informações do consumidor no direcionamento das empresas por um público que demonstrou de alguma forma um interesse por certo tipo de produto ou serviço.

A exposição do indivíduo deve ser harmonizada, como consequência basilar desse fato estudado, intrínseco ao uso da internet, devendo primar pela proteção da privacidade, tendo como linha mestra que orienta a resolução dessas demandas o princípio da finalidade na qual foram cedidas as informações e dados pessoais dos usuários. Havendo normativos que corroboram com o posicionamento anterior exposto. Pode-se, então, antever que ainda brotarão diversos outros litígios de grande complexidade envolvendo a utilização de serviços on-line, que provocarão os estudiosos a encontrar soluções. Enquanto não resta dúvida de que tais serviços oferecem ao fornecedor uma remuneração ou lucro indireto, mesmo quando não pagos pelo consumidor diretamente, que atrai o manto do Código de Defesa do Consumidor e outras normas ulteriores (KONDER & DE SOUZA, 2019).

Faz-se necessário, então, um trabalho dedicado da dogmática jurídica para conceituar novos assuntos que passam a serem temas marcantes no cotidiano do indivíduo pós-moderno. Tendo a dogmática o papel de ligar-se ao direito lhe dando interpretação, permitindo sua completa aplicabilidade e construindo um sistema conceitual completo e coerente (ARNAUD e DULCE, 2000, p.15), assim qual nome se daria a esses tipos de contratos de adesão que, por lei não são permitidos, mas se perpetuam ilesos?

Os contratos de adesão foram regulados inicialmente no CDC de 1990, embora já possuíssem previsão legal anterior. São contratos escritos pelo fornecedor e que não abrem margem para que o consumidor tenha oportunidade de discutir ou modificar substancialmente o seu teor. Monteiro (2001, p.3), traz as características básicas dos contratos standard, como também podem ser chamados:

Todas as características dos contratos de adesão em sentido amplo: a predisposição, a unilateralidade, a rigidez, a generalidade e a indeterminação. Alguém, normalmente uma empresa, elabora previamente as cláusulas (ou "condições") que irão fazer parte de todos os contratos que vier a celebrar, seja com quem for. Isto não impede, naturalmente, eventuais negociações entre as partes quanto a alguns aspectos do contrato - no essencial, porém, ele será regido, no todo ou em parte, pelas cláusulas previamente formuladas, sem que o aderente possa alterá-las. Tais cláusulas não são, pois, o resultado das negociações - pelo contrário, elas antecedem eventuais negociações, são elaborados antes e independentemente de quaisquer (hipotéticas) negociações.

Tais institutos ferem o inciso III do artigo 4º do CDC que assim indica como princípio de proteção ao consumidor a “harmonização dos interesses dos participantes das relações de consumo [...] sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores” (BRASIL,1990). Assim, perpetrando violações ao CDC.

A Constituição Federal de 1988 previu em seu artigo 5º, inciso IV que: “é livre a manifestação do pensamento” (BRASIL,1988), mas como pode ser livre o pensamento ou de que maneira se pode expressar a vontade quando se pretende compartilhar informações, fotos e vídeos com amigos e familiares por meio das redes sociais virtuais sem poder fazer reserva dos seus dados pessoais, íntimos e privados?

Embora seja um tema recente e com pouco conteúdo, quantas pessoas já não se sentiram vigiadas por estar perto de celulares *smartphones*? As invasões que ocorrem a cada dia na vida privada do cidadão são perceptíveis por grande parte da população. Quem nunca se perguntou por que estava conversando sobre um determinado produto ou serviço com o celular na mão ou próximo e, logo após, ao usar serviços como Instagram, Facebook ou navegar em sites, viu que anúncios com o tipo de produto que havia falado apareceu repetidamente? São anúncios direcionados por captação de pesquisa feita no aparelho celular do cidadão ou por meio de voz, mesmo sem haver pesquisa alguma, apenas com conversas o aparelho celular recebe do usuário autorização em algum momento para captar áudio e a maneira com que é usado passa a servir interesses comerciais, perfazendo mais uma vez a tríade: fornecedor (empresa), consumidor (usuário), serviço (armazenamento e conexão social), além do lucro gerado por vender as vontades, como se pode dizer, do indivíduo. “O objetivo dessa vigilância é fazer manipulação psicológica para te persuadir a comprar produtos”, diz o criptógrafo americano Bruce Schneier, autor de 12 livros sobre segurança digital (GARATTONI, LEONARDI e SKLARZ, 2018).

A Constituição Federal de 1988, externa em seu artigo V, inciso X, que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988). Mas grande parte da vida privada do cidadão é exposta como forma de produto pelas empresas como Facebook, Instagram, que invadindo a vida privada do indivíduo, captam dados de uso e de acesso para vender como produto a intimidade das pessoas quando se interessam por determinado assunto ou passam mais tempo vendo tal notícia ou tipo de produto na internet. De tal forma, ajudam os fornecedores a guiar o consumo das pessoas. Criam um mercado de dados, assim a empresa que pagar mais terá acesso a informações de consumidores que estão pesquisando sobre determinado produto ou serviço, garantindo para si vantagem financeira e de mercado.

Por se tratar de normas de ordem pública os ditames que são abrigados pelo Código de Defesa do Consumidor (lei 8.078/90) não podem ser afastados por convenção entre as partes, assim qualquer contrato que venha a ferir ou se oportunizar da vulnerabilidade do consumidor, lhe trazendo danos, não pode ser considerado legítimo, legal ou ético (BRASIL, 1990). Desta forma, pode o juiz, de ofício, reconhecer algumas cláusulas como abusivas por se tratar de norma de interesse público. Com exceção, conforme trata a Súmula 381 do STJ, de relações de consumo em contratos bancários, assim impera ao impetrante que requisiute do juiz a abusividade de alguma cláusula contratual, não podendo o julgador conhecer de ofício a arbitrariedade das cláusulas (BRASIL, 2009).

Black Mirror, uma série da Netflix, empresa de entretenimento, que exemplifica em alguns de seus episódios tipos de vigilância extrema por sistemas informacionais como vemos, em um futuro possível, como o Google. Possui um determinado episódio chamado de “Toda a sua história”, onde a população tem todas as suas memórias gravadas em um implante e um certo personagem mostra como todos podem ter acesso a suas memórias, a exemplo de uma simples viagem que ele pretende embarcar e para tal é requisito o acesso a seus últimos atos do dia a dia que se encontram armazenados em um banco de dados dentro do chip em sua cabeça. Em certo momento a personagem lida com sérias invasões de privacidade entre seus relacionamentos e chega a tomar atitudes irracionais. Tal episódio mostra

como um produto que invade a privacidade de uma pessoa pode submeter à dignidade e a privacidade do consumidor a níveis rasteiros.

A CF/88, com ímpeto, descreveu em seu art.1º, III que “a dignidade da pessoa humana é um bem intangível” (BRASIL, 1988).

No mesmo sentido, o Código Civil de 2002 quanto ao direito de imagem que é um bem pessoal como o direito a privacidade trouxe:

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais (BRASIL, 2002).

A política de dados do Facebook (2021), que é dono também do Instagram e Whatsapp, traz o seguinte conteúdo:

Coletamos o conteúdo, **comunicações** e outras informações que você fornece quando usa nossos Produtos[...]isso pode incluir informações presentes ou sobre o conteúdo que você fornece (como **metadados**), como a **localização de uma foto ou a data em que um arquivo foi criado**. Isso pode incluir também **o que você vê** por meio dos recursos que fornecemos, como nossa câmera, de modo que possamos realizar ações como sugerir máscaras e filtros de que você pode gostar, ou dar dicas sobre o uso de formatos da câmera. **(grifo nosso)**

[...]as **pessoas com quem você mais se comunica** ou os grupos dos quais você faz parte. Também coletamos informações de contato se você optar por carregar, sincronizar ou importá-las de um dispositivo (como uma **agenda de contatos, registro de chamadas ou histórico de SMS**) [...]

[...]o **tipo de conteúdo que você visualiza ou com o qual se envolve**; os recursos que você usa; as ações que você realiza; as pessoas ou contas com que você interage; e **o tempo, frequência e duração das suas atividades**[...]nós também coletamos informações sobre como você usa recursos como nossa **câmera**.

[...]nós **coletamos informações sobre a compra ou transação**. Isso inclui informações de pagamento, como o seu número do cartão de crédito ou débito e outras informações sobre o cartão; outras informações de conta e autenticação; detalhes de cobrança, entrega e contato.

[...]os **recursos que você vê quando usa nossos Produtos** em outro dispositivo, como seu laptop ou tablet, ou para avaliar se você, em resposta a um anúncio que exibimos em seu telefone, realizou uma ação em um dispositivo diferente.

[...]informações **sobre operações e comportamentos realizados no dispositivo, tais como se uma janela está em primeiro ou segundo plano, ou movimentos do cursor** (que podem ajudar a distinguir humanos de bots).

[...]sinais de Bluetooth e informações sobre pontos de acesso de Wi-Fi nas proximidades, beacons e torres de celular.

**[...]informações que você permite que nós recebamos por meio das configurações do dispositivo que você ativa, como o acesso à sua localização GPS, câmera ou fotos. (grifo nosso)**

Primeiramente, a empresa coleta informações direta ou indiretamente por meio dos metadados que são uma descrição de conjuntos de dados ou conforme a definição original de Jack E. Myers que usou nos anos de 1960, um “conjunto de dados” (ALVES, 2010). Tal conjunto é aquele que está ligado a fotos, vídeos ou outros arquivos de forma não aparente, nas informações intrínsecas do arquivo como localização de fotos, de vídeos ou horários em que foram feitos como demonstra o próprio Facebook na sua política de dados. Além de utilizar, como supracitado, o que o usuário vê na sua câmera enquanto usa o aplicativo ou site, sem nenhuma restrição a empresa invade esse espaço que deveria caber só ao consumidor.

Quando o Facebook cita “tempo, frequência e duração” das atividades, ele está mapeando o comportamento do consumidor e isso é usado para sugerir “mais do mesmo”. As sugestões que são feitas, são repetitivas e persuasivas gerando um ciclo vicioso que fere o princípio do livre desenvolvimento da personalidade da pessoa natural, disposto na Lei Geral de Proteção de Dados (2018).

As informações financeiras que são coletadas são imensas e generalistas, deixando um grande vácuo do que realmente é armazenado. Informações outras de cartões ou de conta e autenticação podem inferir em possíveis capturas de senhas de autenticação, senhas de conta e acesso e códigos dos mais variados sobre a conta pessoal do usuário. Geralmente isso acontece quando se permite salvar senhas ou dados de acesso pelo Facebook ou outra empresa ou aplicativo qualquer, sem descartar a possibilidade de que esses dados possam ser capturados sem a ciência do consumidor de alguma forma.

Resumidamente, pode-se interpretar que a empresa Facebook elencou basicamente quase todas as formas com que ela pode coletar as informações pessoais do consumidor. Até com pronomes e substantivos generalistas para abarcar o máximo possível de dados que possam acessar.

Além do Facebook existem outras empresas como Samsung, Apple, Xiaomi, entre outras que restringem acesso aos seus serviços e aparelhos dos consumidores que não optem por aceitar compartilhar suas informações pessoais da maneira com que é disposto nas políticas de uso gerando assim um conflito que deve ser regulamentado.

### **3 COLETA DE DADOS NAS REDES SOCIAIS**

Não é novidade que os escândalos mundiais envolvendo o vazamento de informações pessoais de usuários estão cada vez mais frequentes, necessitando até mesmo de intervenção por parte das autoridades. É sob esta ótica que a lei geral de proteção de dados vem, com intuito de responsabilizar empresas, dando o mínimo de segurança para a parte hipossuficiente na relação consumerista.

É importante frisar que cabe também ao consumidor se resguardar e manter o máximo de atenção, uma vez que, ao passo que as novas tecnologias vêm para beneficiar, podem ser prejudiciais. Dessa forma, métodos capazes de ensinar os riscos, bem como quais são os crimes que pairam no mundo tecnológico são de extrema importância, além de informar os meios de proteção são tão indispensáveis como maneiras de solucionar a problemática, haja vista que prevenir é sempre o melhor caminho.

### 3.1 Inteligência e Contraineligência

Há uma proliferação imensa de ameaças - que não são só virtuais e crescem junto à alta tecnologia e as “*high tech companies*” ou empresas de alta tecnologia como a Google - dentro dos espaços da rede mundial de computadores que impactam diretamente na segurança das pessoas e de dados (MARCIANO e MARQUES, 2006). Assim a cada dia se revelam ações de inteligência (prioritariamente busca) e de contraineligência (principalmente defesa).

Coelho, Rasma e Morales (2013, p.37) definem dado como:

Qualquer elemento identificado na sua forma bruta, que por si só não conduz a uma compreensão de um determinado fato ou tema. Ao passo que por informação, entende-se como um conjunto de dados articulados entre si, que depois de trabalhados ou processados, produzem um determinado sentido ou significado sobre um assunto.

Além de todos os dados coletados e armazenados pelas empresas de rede social virtual, com objetivos comerciais principalmente, há vários tipos de coletas que são feitas por hackers solitários na rede mundial de computadores e pelos atores protagonistas de 4º geração dos conflitos armados. Esses atores são, como elencou Dunnigan (2008, p.10), “organizações não estatais armadas integradas por forças irregulares de diferentes matizes, sejam elas: separatistas, anarquistas, crime organizado, entre outros”. No caso do Brasil se percebe grande atuação do crime organizado, principalmente no tráfico de armas e de drogas.

Esses protagonistas utilizam de operações de inteligência criminosa para difundir, atingir, obscurecer, dissuadir e alcançar seus objetivos, quaisquer que sejam, desde o tráfico de informações, estelionato e golpes a execuções e ameaças a agentes ou a sociedade civil. Para tanto, são utilizadas ações de inteligência quer sejam: ações de coleta que acontecem quando realizadas ostensiva ou secretamente, com o fim de conseguir dados depositados em fontes disponíveis, quer sejam oriundas de indivíduos, órgãos públicos ou privados, tendo como exemplo dados de redes sociais abertas; ou ações de busca que são feitas por um elemento de operações a fim de reunir dados protegidos e/ou negados em um universo antagônico, por exemplo, informações de perfis restritos (BRASIL, 2015).

A Diretriz Nacional de Inteligência de Segurança Pública, DNISP (2015, p.43) definiu como inteligência:

O ramo voltado para a produção de conhecimento de interesse da Segurança Pública, de imediata ou potencial influência sobre o processo decisório nas ações de prevenção e repressão a atos de qualquer natureza, que atentem à ordem pública, à incolumidade das pessoas e do patrimônio.

A inteligência de Segurança Pública ou ISP, como um ramo de trabalho informativo possui como objetivos principais desenvolver ações com o desígnio de assistir o processo decisório por meio de conhecimentos sobre os assuntos relacionados à Segurança Pública e à defesa social, em seus níveis diretos de atuação - política, estratégica, tática e operacional, mediante os processos de produção e proteção de conhecimentos como também produzir conhecimentos nas diversas áreas de atuação dos órgãos integrantes do sistema de Segurança Pública

e Defesa Social, consubstanciados em ações que busquem prever, prevenir, neutralizar e reprimir quaisquer ações que atentem à ordem pública, à incolumidade das pessoas e do patrimônio (BRASIL, 2015, p.43).

Já a contrainteligência é definida como:

Se destina proteger a atividade de Inteligência e a instituição a que pertence, mediante a produção de conhecimento e implementação de ações voltadas a salvaguarda de dados e conhecimentos sigilosos, além da identificação e neutralização das ações adversas de qualquer natureza (BRASIL, 2015, p.45).

A contrainteligência possui alguns segmentos que são: “a segurança orgânica, segurança de pessoal, segurança da documentação, segurança das instalações, segurança de material, segurança das operações, das comunicações e da tecnologia da informação” (BRASIL, 2015, p.47). De tal forma se torna um campo vasto para atuação das organizações estatais, mostrando para o público civil que é algo de extrema importância e que requer um zelo elevado a proteção de informações e dados de quaisquer atores.

Assim, a inteligência usada pelas organizações criminosas visa à produção de conhecimento de interesse da Orcrim que possua influencia na tomada de decisão e na vantagem tática no planejamento de ações criminosas. Assim tendo conhecimento sobre o nível de organização e capacidade que uma Orcrim pode conter o cidadão ou principalmente funcionários públicos podem tomar atitudes que diminuem os riscos e as chances de serem alvos de tais práticas delitivas.

### 3.2 Cibercrimes

A modernidade trouxe grande avanço tecnológico e consigo o avanço das modalidades de crimes e suas formas. Novos tipos de crimes e o progresso de tantos outros geram uma grande preocupação. Quando acessamos quaisquer sites na rede de computadores estamos sujeitos a sermos alvos de algum tipo de ataque por vírus ou hacker malicioso com intuito de acessar dados pessoais ou informações chaves para cometer algum crime através da internet, já não bastasse isso, as empresas colhem nossos dados e vendem aleatoriamente e sem regulação. Assim o cibercrime se torna altamente comum na sociedade informatizada.

Simas (2014, p.12) trouxe o conceito de Cibercrime como:

O conceito de criminalidade informática, ou cibercrime, como hoje conhecemos não é unânime, nem tão pouco exacto. Alguns entendem que é considerada como “todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto de crime.

Também são termos utilizáveis: Crime informático, crime cibernético, e-crime, em inglês, cibercrime, crime eletrônico ou crime digital que conforme definido se baseia em toda a atividade criminosa que se utiliza de um computador ou uma rede de computadores como instrumento ou base de ataque (NASCIMENTO, 2019). Assim a sociedade que vive conectada a *smartphones* na maior parte do cotidiano ou na tela de computadores, vive uma geração que está diretamente exposta a tais crimes informáticos.

O crime virtual engloba todas as atividades criminosas realizadas por meio de computadores ou da internet. Podem ser empregados diversos métodos e ferramentas, tais como *phishing* (roubo de identidade ou de contas), vírus, *spyware* (software espião que captura dados pessoais), *ransomware* (software malicioso que bloqueia arquivos) e engenharia social, geralmente com o objetivo de roubar dados pessoais ou praticar fraudes.

O termo engenharia social parece ser algo que não conota em malefício ao ser humano ou a alguma instituição, conforme a junção das palavras do termo. Peixoto (2004) traz o significado dos termos em que a engenharia é a arte de aplicar conhecimentos científicos, empíricos a criação de estruturas, dispositivos e processos que convertem recursos naturais em formas de atendimento as necessidades humanas e o social relativo à sociedade de fato. Já Eiras (2004) *apud* Coelho, Rasma e Morales (2013) revela que a engenharia social é uma terminação empregada para determinar a área que estuda as técnicas e práticas utilizadas para a obtenção de informações importantes ou sigilosas de uma organização, através das pessoas, funcionários e colaboradores de uma corporação ou de uma sociedade. Essas informações podem ser obtidas por ingenuidade ou confiança.

Também Hadnagy e Maxwell (2009) trazem que a engenharia social revela-se na conjuntura da segurança quanto ao uso de tecnologias de informação e comunicação nas ações exercitadas para alcançar e dissolver o valor da informação. Também para conseguir dados relevantes e sigilosos, através da exploração da confiança de pessoas, que são provenientes de organizações e/ou sistemas computacionais.

Existem como Nascimento (2019) elencou dois tipos de sujeitos ativos dos cibercrimes que são eles os *Hackers* e os *Crackers*, os primeiros são usuários experientes que invadem sistemas de computadores para provar suas capacidades e o segundo conceito são invasores que tem objetivo de roubar informações dos sistemas, como também causar danos as vítimas além de favorecerem a pirataria destruindo a proteção de softwares.

Há na rede de computadores ambientes virtuais que se assemelham a mercados negros, como são chamadas as redes de internet Deep Web e Dark Web que segundo alguns autores podem chegar a representar 90% da rede de internet. São formadas por sites de acesso negado a buscadores comuns como Google ou Bing e não estão disponíveis no que é chamado de *SurfaceWeb* ou a internet de superfície. A *DeepWeb* ou web oculta opera através da internet, é um sistema hipertextual e possui todo o conteúdo restrito a usuários comuns na rede por meio do uso aberto e normal, já a *DarkWeb* ou web negra, possui toda a parte imoral, ilegal e violenta da rede como tráfico de armas, drogas e outros crimes.

Há no Senado Federal a Lei 236/2012, que possui a finalidade de instituir um novo Código Penal Brasileiro e tratar de assuntos ainda com lacunas legislativas presentes, como o cibercrime.

Hoje o principal meio de obtenção de informações pelas organizações criminosas é a internet. Por meio de ações de inteligência elas buscam dados de diversos tipos de pessoas como população civil, funcionários públicos, entre outros. Podemos então citar como organização criminosa (Orcrim), como definiu a lei 12.850 de agosto de 2013:

A associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações

penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional (BRASIL, 2013).

Tais Ocrim podem visar a prática de estelionato ou fraude, extorsão (art. 158), entre outros crimes quando tem a chance de apropriar-se dos dados de algum cidadão, seja dado exposto ou negado. Dado exposto é aquele em que há extrema facilidade na sua coleta e o negado é quando há alguma barreira para a coleta deste tipo de conhecimento (BRASIL, 2015).

Todos podem ser alvo de uma organização criminosa, mas algumas pessoas tendem a ser mais atacadas como por exemplo: autoridades de estado, policiais, empresários, comerciantes, membros da classe média alta.

Há atualmente a lei 12.737/2012 que dispõe sobre a tipificação criminal de delitos informáticos, uma legislação recente que surgiu a partir do projeto de Lei nº 2.793/2011, tendo sido aprovado após a situação fatídica que envolveu a atriz Carolina Dieckmann que foi alvo de crackers, que conseguiram furtar imagens pessoais e da sua família, inclusive com imagens íntimas da atriz que após acessar um e-mail infectado com um *spyware* teve diversas fotos capturadas pelos criminosos. De início foi pensado que teria ocorrido o fato onde a atriz teria consertado seu computador, mas após foi verificado que foram indivíduos do interior de Minas Gerais e São Paulo que praticaram o ato.

Os criminosos exigiram R\$ 10.000,00 reais para que não fossem divulgadas as fotos nas mídias sociais. A atriz registrou boletim, tendo sido feitas investigações, após dispersão das imagens. O enquadramento dos fatos foi feito por furto, extorsão qualificada e difamação (SILVEIRA, SOUZA e MELO, 2017).

Após esse fato surgiram tipificações como: invasão de dispositivo informático; Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e também falsificação de documento particular e de cartão. Nesse ano de 2021 foi sancionada a Lei 14.155 que altera o Código Penal, agravando penas como fraude, furto e estelionato com invasão de dispositivos eletrônicos. O crime de invasão de dispositivo informático, por exemplo, com pena anterior de 3 meses a 1 ano passou para 1 a 4 anos de reclusão (BRASIL, 2021).

### **3.3 Tipos de informações que são alvo e como se proteger**

Primeiramente, como o caso supracitado da atriz Carolina Dieckmann, se podem elencar fotos pessoais e íntimas como um tipo de objeto alvo, que possuem um valor emocional grande para a vítima. Quem é alvo desse tipo pode sofrer extorsões em troca de dinheiro ou de favores sexuais. Assim no caso de e-mails infectados é interessante manter um antivírus atualizado que possua capacidade para escanear a caixa de entrada e o e-mail do usuário, assim como arquivos que são recebidos e a criação de um hábito de não abrir ou acessar e-mails aleatórios e de fontes sem procedência.

Brandão (2020) elenca informações importantes que são expostas pelos usuários, quer sejam: 98,33% dos pesquisados mostram a imagem do rosto; 40% mostram a data de nascimento completa; 5% revelam o endereço completo e 71,66% mostram sua cidade; 85% expõem seus familiares; 78,33% expõem sua profissão como policial militar e 80% mostram sua rotina em rede social principalmente com situações sobre viagens, festas, trabalho e esportes. Esses dados revelam que mesmo profissionais que lidam com o crime diariamente estão

desatentos quanto ao uso das redes sociais e deixam a desejar quanto ao aspecto da segurança das suas informações pessoais.

Ter um perfil privado pode ajudar sobremaneira na exposição de informações a desconhecidos, a exemplo dos dados mencionados acima, como também filtrar as pessoas e perfis que possuem acesso ao ciclo de seguidores ou amigos nas redes sociais. Mesmo assim, ter um criterioso ciclo de amizades ou seguidores em rede social é recomendado, pois mesmo com restrição do perfil pode-se estar sendo monitorado pela “loira de vermelho da matrix”. Uma personagem chamativa que possuía no filme um objetivo sorrateiro.

Outro ponto que pode ser alvo são os álbuns de fotografias ou vídeos, pois municiam o invasor de informações sobre endereços, rotinas, veículos, escolas e locais de tratamento de saúde, entre outras informações sensíveis a segurança individual ou familiar. Também existe o “**Check-in**” do Facebook que é primordial quanto à segurança, pois mostra em tempo real o local exato onde o usuário se encontra, geralmente sendo usado em bares, restaurantes, praias, entre outros (BRANDÃO, 2020).

Garattoni, Leonardi e Sklarz (2018) assealam que a captura de informações do usuário começou com a Netscape, quando o americano Lou Montulli lançou um dos primeiros navegadores. O problema era que os sites não se lembravam dos usuários, tendo que informar senhas de acesso todas vezes que forem acessados. Assim Lou inventou o “*Cookie*” que com apenas uma linha de código seria lançado pelos sites para o computador, para não mais necessitar de informar a senha do site, lembrando do usuário. O nome do arquivo foi feito para ser simpático. Assim o comércio usou para criar os carrinhos de compra, porque agora os sites lembraram-se dos usuários através do computador reconhecido pelo *cookie*, tendo cada site seu próprio arquivo, não podendo vigiar o navegante pela internet.

Em 1996, a empresa Doubleclick criou os supercookies e distribuiu para mais de 30 sites, assim conseguindo monitorar a navegação de usuários online. Conseguia também traçar um perfil comercial e psicológico e agora exibir anúncios personalizados para os internautas. Funcionava assim que a pessoa lesse um texto ou pesquisa sobre um super herói, por exemplo a empresa mostrava anúncios de brinquedos, filmes ou fantasias do herói de quadrinhos. Houveram nos Estados Unidos da América processos contra a empresa Doubleclick, pois então eles podiam vigiar as pessoas, mas os demandantes não tiveram êxito. Já em 1998 o Google foi criado como uma ferramenta de busca e passou a crescer desde que inseriu anúncios em sua tela, quando em 2008 adquiriu a Doubleclick por mais de US\$ 3 bilhões. Assim a Google passou a controlar a publicidade online e a nutri-la cada vez mais.

Alguns passos podem ser seguidos para diminuir o acesso que empresas têm sobre os dados do usuário que são: 1- barrar o monitoramento do Chrome desativando o item “*atividade da web*” e desativar as sugestões de pesquisa na aba avançada das configurações; 2- revisando os aplicativos em configurações, aplicativos e na aba ativos e expirados se pode deletar os apps que não se usa; 3- diminuir a vigilância do Facebook instalando o plugin “PrivacyBadger” que bloqueia cookies e rastreadores que espionam a atividade na maioria dos sites. Além de usar navegadores fantasmas como o “Ghostery” ou usar abas fantasmas; 4- desativar o assistente de voz no aplicativo Google, na aba voz e desligando o “Voice match” ou detecção de ok Google. 5- Para ouvir o que o Google pode ter gravado basta acessar o link: [myaccount.google.com/activitycontrols](https://myaccount.google.com/activitycontrols), clicar em “outra atividade” e “informações do dispositivo”; 6- fotos sensíveis podem ser não enviadas para

aplicativos de sincronização como “icloud” ou “Google fotos” que possuem nuvens que são mais propensas a vazamentos ou acidentes como misturar fotos pessoais com arquivos de trabalho ou familiares (GARATTONI, LEONARDI e SKLARZ, 2018)

O histórico de localização do Google é outra ferramenta que tem um benefício que é ser usado como um meio de defesa criminal, um álibi ou prova, mas em contrapartida ele fornece ao Google toda sua trajetória, minuto a minuto de locais que foram visitados como lojas e tipos de ambientes que podem ser usados pela empresa ou por algum hacker para mapear a rotina do usuário. Assim desativar essa configuração é indicado para quem não quer compartilhar esse tipo de informação com o Google (GOOGLE, 2021).

Outro meio de conseguir informações pessoais é por meio de disfarce, com um perfil falso, entrando em contato com a vítima e se fazendo parecer com o sexo oposto na maioria das vezes. Buscam informações privadas diretamente da pessoa e muitas vezes conseguem marcar encontros pessoalmente, então filtrar as pessoas que tem acesso ao perfil é essencial.

Quando no cadastro procura-se que não se veicule informações não obrigatórias como estudo, trabalho, cidade, família e outros itens que falem sobre sua vida, pois são as informações mais sensíveis e procuradas. Como também ter muito cuidado nas Configurações de privacidade de dados pessoais e no que se publica, pois se pode ter um controle maior sobre quem pode ver tais informações (BRANDÃO, 2020).

Atitudes como não mostrar localização de atividades, não mostrar rotina ou horários são imprescindíveis, além de revisar todas as fotos e vídeos que são veiculados para não mostrar informações que não estão tão aparentes a primeira vista. Também é indicado, se for preferível postar fotos de locais após ter se ausentado e não gerar frequência.

## **4 A TUTELA DA PRIVACIDADE DO CONSUMIDOR E A LEI GERAL DE PROTEÇÃO DE DADOS – LEI 13.709/18**

A exemplo do que ocorre em Portugal e nos Estados Unidos, onde o primeiro segue uma política mais positivada sobre a proteção de dados e o segundo adota uma maior liberalidade do tratamento, deixando a cargo das partes a regulação e do setor privado a geração de certificados de segurança. O Brasil seguiu uma política mais parecida com Portugal ou da União Europeia, possuindo normativos que regem o tema buscando legislar de forma exaustiva essa proteção (SIMAS, 2014).

### **4.1 Objetivos da Lei 13.709/18**

A humanidade nos dias atuais está arraigada pela dependência do uso da tecnologia e pela influencia digital. As crianças não passeiam mais por praças como antes e se contentam em ficar na frente de uma tela escutando sons e vendo imagens coloridas. Assim, surgem legislações que positivam a proteção que deve ser disposta a quem se dispõe a consumir produtos virtuais ou está sendo alvo do serviço de alguma empresa ou dispositivo tecnológico que é controlado por uma empresa de tecnologia. A Lei Geral de Proteção de Dados ou Lei 13.709/2018 busca resguardar o titular ou dono originário das informações que são captadas e coletadas de diversas formas (BRASIL, 2018).

A LGPD apareceu com o intuito de resguardar os dados pessoais e seu tratamento, mostrando uma evolução do Marco Civil da Internet no aspecto de abrir

um leque de possibilidades para que também às empresas possam efetivamente coletar dados mesmo sem o consentimento do titular, assim trazendo dúvidas quanto a sua eficácia.

O objetivo principal que é trazido no artigo 1º da Lei 13.709/18 diz que a lei disporá 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 (BRASIL, 2018).

Tal trecho versa sobre o tratamento de dados feito de forma virtual e material, abrangendo maiores campos de atuação e compreendendo todos os tipos de pessoas, quer sejam naturais, jurídicas e de direito privado ou público, protegendo os direitos fundamentais de liberdade, privacidade e a livre formação da personalidade da pessoa humana, elencados na Constituição de 1988.

Conforme a SERPRO (2021) - empresa líder no mercado nacional de tecnologia da informação para o setor público e privado e que trabalha também com os principais órgãos da Administração Pública Federal como Banco do Brasil, DENATRAN, Receita Federal e Ministério da Economia - a LGPD foca sua aplicação nos dados relacionados à pessoa, brasileira ou não, que se situe no Brasil, ao tempo da coleta, como também dados tratados sob o território nacional, não importando o meio utilizado, e dados usados para o provimento de serviços ou bens.

Excetua-se os dados usados por pessoa natural com fins particulares e não econômicos, com fins jornalísticos, artísticos, acadêmicos, para segurança pública, defesa nacional, segurança do Estado e atividades de investigação ou repressão de infrações penais.

A lei em tela possui como fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Conforme o artigo 6º da LGPD (2018) busca-se no tratamento dos dados a boa-fé; uma finalidade legítima, específica, clara; o uso mínimo dos dados para seu fim; o livre acesso do titular; uma exatidão e atualização; a transparência das informações e de quem trata; a segurança dos dados e a prevenção contra danos; a não discriminação e a responsabilização do agente tratador.

## **4.2 Mudanças proporcionadas pela lei**

Em vários momentos do cotidiano os dados pessoais são alvos de tratamento. Quando uma loja usa os cookies (arquivos de memória de acesso) para enviar propagandas ou direcionar seu público alvo, quando um administrador de empresa ou público utiliza as fichas dos funcionários para folha de pagamento ou para selecionar um ou outro para determinada tarefa, quando se enviam arquivos, fotos ou vídeos para uma rede social ou drive de armazenamento ou quando imagens de um cidadão são gravadas por um sistema de monitoramento. São várias as formas de enquadramento em que a lei se aplica.

A principal evolução que foi proporcionada pela lei foi o acesso claro, facilitado e regulamentado dos dados pessoais que estejam sob a posse de qualquer empresa, mesmo que elas possam coletar esses dados de outras formas que não sejam com o consentimento claro do titular, segundo se identifica no artigo 7º, inciso IX, que informa maneira regulada em que se pode manipular dados:

Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018).

A criação da ANPD (Autoridade Nacional de Proteção de Dados) conforme o art. 55-A, órgão que tem por fim regular e fiscalizar o cumprimento da lei, além de tratar da política nacional de proteção de dados, é importante para que se tenha um órgão regulador que possa tomar a frente das questões estratégicas e de defesa do consumidor, como proporcionar o elencado no inciso VIII do artigo 55-J:

Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis (BRASIL, 2018).

O acesso a dados para tratamento, mesmo quando negado pelo titular, não pode ser alvo de conflito ou de sanção pelo controlador ou tratador, pois a livre escolha faz parte do exercício de direitos pela pessoa que detém os dados. Não podendo o titular ser prejudicado pela sua opção de aceitar ou rejeitar os termos sugeridos pelo agente de tratamento, pois o controle integral é um fundamento legal do tratamento de dados pessoais.

Nos dias atuais, após a promulgação da LGPD, quando se acessa um site qualquer se observa primeiramente um termo de contrato sobre a ação de cookies, muitos deles contratos de adesão sem possibilidade de ajuste pelo usuário/consumidor. Esses termos que autorizam a coleta e o armazenamento de informações pelos cookies se encaixam em mais um tratamento diverso do disposto no inciso I que é o consentimento do titular, pois ao acessar tais sites não se pode utilizar plenamente do serviço sem aceitar a ação dos cookies.

Vários serviços informacionais garimpam dados pessoais para atrair investimentos e gerar riqueza. Tal situação traz grandes questões jurídicas quando lidam com a privacidade, o tratamento desses dados e como são usados, gerando responsabilidade aos detentores (ANHAIA e SOARES, 2020). Assim se verificam várias mudanças que visam regular o uso dos dados de terceiros, no caso os titulares.

### **4.3 A LGPD e a Privacidade do Usuário**

A Lei em tela trata diretamente em seu nome sobre a proteção dos dados pessoais dos titulares que fornecem ou são captados de alguma forma, mesmo sem ciência do proprietário. De tal maneira que se pode perceber que o intuito principal da lei é a garantia da não violação da privacidade do usuário. Sendo opção deste a contribuição pela vontade expressa com suas informações para qualquer banco de dados de qualquer uma das mais diversas empresas de “*High Tech*”. De tal maneira

que aumentando a geração de informações, aumenta-se a preocupação com a segurança de tais informações (GONÇALVES, 2005).

A transnacionalidade de delitos que são cometidos através dos meios avançados de difusão de informações à distância, por intermédio de *hackers* e *crackers* (BITTAR, 2016, p.139), que geram grandes danos a sociedade na figura individual dos usuários da internet é uma preocupação que é tratada no campo da bioética e do biodireito, pois mostra uma essencial necessidade de normatização dos processos. Assim, a Lei 13.709/18 precisa ser encarada como um processo não findo e que busca olhares mais atraídos para ser alavancada em rumo a uma proteção mais ampla do cidadão.

Na conjuntura atual que trata sobre tecnologia da informação, a LGPD cumpre um papel de harmonização, de atualização de conceitos, mitigando riscos e esclarecendo regras para proteção de dados pessoais (MALDONADO; BLUM, coord. 2019, p. 23 *apud* FONSECA e NOGUEIRA in GROSSI, 2020, p.21), desta forma ela abre caminho para que novas normativas venham trazer mais e mais proteção ao usuário por meio de regulação das estruturas da internet e da atuação dos agentes de tratamento.

Nesse contexto há um novo tipo de cultura que se intitula como “cultura de consumo virtual” (BARRETO, 2011) que hoje em dia se desdobra em diversas demandas jurídicas, apontando novos atores em um cenário do que chamou Rad e Benyoucef (2010) de “social commerce”, que não representa apenas um comércio social, mas algo que não poderia acontecer sem as novas tecnologias e formas de interagir da sociedade. O termo utilizado trata de uma nova realidade que diferente de tempos passados, se mostra como um comércio realizado através das redes sociais virtuais como o Facebook, Instagram ou Whatsapp.

O *social commerce* é uma nova modalidade híbrida de comércio, assim como as diversas novas tecnologias, ele vem se desenvolvendo rapidamente e mudando formas de interagir com o público, no caso o consumidor/usuário. Assim a LGPD não possui profundidade de regulação nessas demandas, trazendo em um mundo que a cada dia muda seu modo social de interagir, apenas conceitos e fundamentos. Relações como essas em que dados são nos dias de hoje tratados como produtos ou como minério e transformados em capital.

Quanto à aquisição de produtos de telefonia como *smartphones* pelo titular de dados, a LGPD ainda não solucionou a problemática dos verdadeiros contratos de adesão que são dispostos na inicialização dos aparelhos, pois é claro e indubitável que se o consumidor não aceitar os termos elencados no acordo de uso dos atuais *smartphones* não poderá fazer uso dos produtos de forma normal ou de alguma forma sequer. Isso tem gerado um dano imensurável à liberdade de expressão e de opinião, ao desenvolvimento tecnológico e a defesa do consumidor protegidos no artigo 2º da Lei Geral de Proteção de Dados (2018), como também a privacidade, pois só se tem permissão de uso dos aparelhos citados, em sua maioria, com a permissão do titular/consumidor de que sejam utilizados seus dados conforme os termos do contrato ali dispostos.

A segurança do usuário deve ser garantida como um preceito fundamental e não elencada apenas como direito. Deve, portanto, ser positivada com a maior quantidade de detalhes para que o consumidor não sofra prejuízos e danos elevados como o caso a seguir, acórdão proferido pelo Tribunal de Justiça do Rio grande do Sul (2007):

Empréstimo efetuado em nome de aposentado via internet. Ausência de comprovação de fraude. Fragilidade do sistema de contratação da instituição financeira, permitindo fosse atingido o benefício previdenciário do postulante. Situação que extrapola o mero dissabor ou o pequeno transtorno, gerando intranquilidade, **insegurança e invasão de privacidade. Dano à personalidade caracterizado.** Fixação do valor da indenização em quantia módica, ante ausência de demonstração de maior prejuízo. Sentença de improcedência a ser reformada. Deram provimento as recurso (recurso Cível nº71001166768, primeira turma recursal Cível, Turmas Recursais, TJ-RS. Relator: Heleno Tregnago Saraiva, julgado em 25/10/2007). **(grifo nosso)**

A proteção trazida no fundamento da autodeterminação informativa, disposto no artigo 2º inciso II da LGPD, não elencou maneiras com que o usuário possa controlar e proteger seus dados, deixando mais um espaço vago para regulamentação.

## 5. CONSIDERAÇÕES FINAIS

A LGPD se revela como um grande avanço na temática da proteção de dados no Brasil, trazendo diversas mudanças materiais e virtuais que ajudam a proteger o cidadão contra a força sem pudor do mercado de consumo e das empresas, mas há um caminho considerável para que se possa dizer que ela tem uma força expressiva na proteção do usuário ou consumidor tanto quanto possui o Código de defesa do consumidor com as suas garantias e direitos mais claros e práticos.

Verifica-se que há realmente uma relação de consumo entre os usuários e as redes sociais virtuais, pois há uma geração de lucro com o acesso dos consumidores, assim como nos sites e plataformas que acontece o mesmo fenômeno mercadológico. Não há um respeito pleno a privacidade do consumidor que acessa as redes sociais ou pretende utilizar plenamente os serviços e funcionalidades oferecidas pelos smartphones, pois para ele precisa concordar em ceder seus dados privados para poder usar o que lhe é oferecido, cedendo a um contrato de adesão totalmente rígido, fenômeno trazido pelas mudanças rápidas dos processos consumeristas. As políticas de uso devem ser revistas e regulamentadas sem ferir o direito do consumidor de livre dispor de seus dados pessoais.

O respeito à liberdade na manifestação do pensamento, a segurança, a intimidade e a vida privada não são, como mostrados, totalmente respeitados e colocados em primeiro plano. De maneira que nem sempre há a total aceção por parte do usuário dos termos de uso de forma livre e sem manipulação. Realmente, o faturamento é o que baseia as ações das grandes empresas, as High Techs. Dessa forma se faz necessário que haja uma profunda regulação das relações no ambiente do *social commerce*. Assim, a LGPD tem aberto um caminho menos sinuoso para que a proteção ao usuário/consumidor seja mais ampla, mas falta muito ainda para que seja considerado satisfatório esse amparo.

Constata-se que há uma enorme fragilidade para quem usa uma rede social como Facebook, Instagram, entre outras, de certa maneira que sem o conhecimento devido para proteger-se de ameaças virtuais e materiais, os consumidores se veem expostos na rede mundial ao cibercrime. Conhecendo os padrões aqui expostos, além de outros vários, o consumidor pode se proteger um pouco mais a cada dia.

O comércio realizado através das mais variadas redes sociais ou *social commerce*, deveria ser mais assistido quanto a estudos e análises para que os legisladores viessem a entender os nuances dos processos internos e inter relacionáveis para, assim, construir normas que efetivamente mantivessem harmonia entre consumidor e fornecedor, como também se mantivessem atuais, não trazendo prejuízos a qualquer parte da relação de consumo. Além de resguardar o usuário quanto a padrões e processos de vigilância.

## REFERÊNCIAS

AGNE, Karime; P. B., DOS SANTOS, P. R., NOVACKI, E. **O Consumidor na relação jurídica de consumo**. N° 8, JICEX, 2017. *E-book*.

ALMEIDA, Fabrício Bolzan de. **Direito do consumidor esquematizado**. São Paulo: Saraiva. 2013. *E-book*.

ALVES, Rachel Cristina Vesú, et al. **Metadados como elementos do processo de catalogação**. Faculdade de Filosofia e Ciências – Universidade Estadual Paulista. Marília. 2010. *E-book*.

ANHAIA, Vinicius Bardemaker. SOARES, Nadia pedroso. **O Direito à privacidade e sua proteção na era digital**. URCAMP. 2020. *E-book*.

APOSKITIS, L. Social Engineering: The absolute war in full development. JournalofHellenicNexus, dez. 2009. Disponível em: <<http://thegreek.hubpages.com/hub/Social-Engineering-The-absolute-war>>. Acesso em: 05 abr. 2021.

AQUINO JUNIOR. Geraldo Frazao de. **Contratos eletrônicos: a boa fé objetiva e a autonomia da vontade**. Curitiba: Juruá, 2002. *E-book*.

ARNAUD, Andre-Jean; DULCE, Maria José Fariñas. **Introdução à análise sociológica dos sistemas jurídicos**. Rio de Janeiro: Renovar, 2000. *E-book*.

BACKES, Lúcia Jacinta da Silva. **A Publicidade e suas Implicações com as Racionalidades de Consumo**. Gestão e Desenvolvimento, Novo Hamburgo, ISSN: 1807-5436, v. 2, n. 1, jan.-jun. 2005. Disponível em: [[www.redalyc.org/pdf/5142/514252206004.pdf](http://www.redalyc.org/pdf/5142/514252206004.pdf)]. Acesso em: 17.03.2020.

BARRETO, Ricardo Menna. **Direito, redes sociais e social commerce: pensando a proteção do consumidor**. Revista da Seção Judiciária do Rio de Janeiro, Rio de Janeiro, v. 18, n. 32, p. 145-162, 2011. *E-book*.

BAUMAN, Zygmunt. **O mal-estar da pós-modernidade**. Editora Schwarcz-Companhia das Letras, 1999. *E-book*.

BAUMAN, Zygmunt. **Vida para o consumo: a transformação das pessoas em mercadorias**. Rio de Janeiro: Zahar, 2008. *E-book*.

BITTAR, Eduardo C. B. **Curso de ética jurídica: ética geral e profissional.** São Paulo. 13. ed. Saraiva. 2016. *E-book*.

BÖGER, D. S.; BODEMÜLLER JUNIOR, R. **Segurança da Informação.** 2007. Disponível em: <[http://www.das.ufsc.br/~dsbogger/aula/07\\_1/ine5329-administracao\\_em\\_processamento\\_de\\_dados/transparencias\\_seguranca.pdf](http://www.das.ufsc.br/~dsbogger/aula/07_1/ine5329-administracao_em_processamento_de_dados/transparencias_seguranca.pdf)>. Acesso em 18 abr. 2021.

BRANDÃO, John Lennon dos Anjos. **As redes sociais e a exposição dos agentes de segurança pública.** Faculdade IPEP. 2020. *E-book*.

BRASIL. **Declaração Universal (DUDH).** Disponível em: <<https://www.gov.br/mdh/pt-br/centrais-de-conteudo/declaracao-universal-dudh>>. Acesso em: 06 mai. 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil.** Brasília, DF. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/2002/L10406compilada.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm)>. Acesso em: 17 mar. 2021.

BRASIL. Lei nº 12.850, de 02 de agosto de 2013. **Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências.** Brasília, DF. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/lei/l12850.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm)>. Acesso em: 12 mar. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 17 mar. 2021.

BRASIL. **Doutrina Nacional de Inteligência de Segurança Pública DNISP.** Brasília: MJ, 2015. *E-book*.

BRASIL. **Súmula nº381.** Disponível em: <[https://www.stj.jus.br/docs\\_internet/revista/eletronica/stj-revista-sumulas-2013\\_34\\_capSumula381.pdf](https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2013_34_capSumula381.pdf)>. Brasília: STJ, 2009. Acesso em 04 mai. 2021.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. **Engenharia Social: uma ameaça à sociedade da informação.** Exatas & Engenharias, 2013. Campos dos Goytacazes. Disponível em: <[https://ojs3.perspectivasonline.com.br/exatas\\_e\\_engenharia/article/view/87/59](https://ojs3.perspectivasonline.com.br/exatas_e_engenharia/article/view/87/59)>. Acesso em 28 abr. 2021.

CRAWFORD, Emma. **How much would it cost to use Facebook ad-free? A Vancouver digital marketing agency has uncovered some surprising results in its search to answer that question.** Business Vancouver, technology, Vancouver,

20 de dezembro de 2012. Disponível em: <[www.bi.com/article/2012/12/how-much-would-it-cost-to-use-facebook-ad-free/](http://www.bi.com/article/2012/12/how-much-would-it-cost-to-use-facebook-ad-free/)>. Acesso em: 12.03.2021

DE ALMEIDA, João Batista. **Manual de direito do consumidor**. Saraiva Educação SA, 2017. *E-book*.

DE BRITO, Dante Ponte; COSTA, Pedrita Dias. **Consumo pós-moderno, redes sociais e superendividamento**. Revista de Direito do Consumidor, p. 79-97, 2020. *E-book*.

DONEDA, Danilo. **A proteção da privacidade e de dados pessoais no Brasil**. Observatorio Itaú cultural, São Paulo, n.16, 2014. *E-book*.

DUNNIGAN, James F. **Ações de comandos: operações especiais, comandos e o futuro da guerra dos EUA**. Rio de Janeiro: Biblioteca do Exército Editora, 2008.

E-bit (2015). **RelatórioWebshoppers**. Ed. 32. 2015. Disponível em: <[http://img.ebit.com.br/webshoppers/pdf/32\\_webshoppers.pdf](http://img.ebit.com.br/webshoppers/pdf/32_webshoppers.pdf)>. Acesso em: 31.03.2021.

E-bit (2016). **RelatórioWebshoppers**. Ed. 33. 2016. Disponível em: <[http://img.ebit.com.br/webshoppers/pdf/33\\_webshoppers.pdf](http://img.ebit.com.br/webshoppers/pdf/33_webshoppers.pdf)>. Acesso em: 31.03.2021.

FACEBOOK, Inc. **Política de dados**. CA. Disponível em: <<https://www.facebook.com/privacy/explanation>>. Acesso em: 25.03.2021.

FERREIRA M.; ALEXANDRINO, O.; PELIN, R.; JARDIM, W. **Engenharia Social, a ação humana na prática ilegal de acesso à Informação**. 2010. Disponível em: <[http://fbvmanagersheet.googlecode.com/svn/trunk/ManagerSheet/ManagerSheet/Ambiente/Infraestrutura/Engenharia\\_Social\\_Paper.pdf](http://fbvmanagersheet.googlecode.com/svn/trunk/ManagerSheet/ManagerSheet/Ambiente/Infraestrutura/Engenharia_Social_Paper.pdf)>. Acesso em: 12 abr. 2021.

FERREIRA, M. **O que vem a ser segurança da informação?**. 2008. Disponível em: <<http://www.apinfo.com/artigo81.htm>>. Acesso em: 15 abr. 2021.

FRIEDEN, Jeffry A. **Capitalismo global: história econômica e política do século XX**. Editora Schwarcz-Companhia das Letras, 2008. Disponível em: <[https://books.google.com.br/books?hl=pt-PT&lr=&id=T3HTDwAAQBAJ&oi=fnd&pg=PT6&dq=hist%C3%B3ria+econ%C3%B4mica&ots=wIAX9uReuC&sig=Xg\\_mJRXLJWN1E\\_8-S58AmkOalgM#v=onepage&q&f=false](https://books.google.com.br/books?hl=pt-PT&lr=&id=T3HTDwAAQBAJ&oi=fnd&pg=PT6&dq=hist%C3%B3ria+econ%C3%B4mica&ots=wIAX9uReuC&sig=Xg_mJRXLJWN1E_8-S58AmkOalgM#v=onepage&q&f=false)>. Acesso em: 24 abr. 2021.

GARATTONI, B.; LEONARDI, A. C.; SKLARZ E.; **Como não ser espionado**. Super interessante. Abril. Disponível em: <<https://super.abril.com.br/especiais/como-nao-ser-espionado/>>. Acesso em: 04 mai 2021.

GERALDO, G.C.MAINARDES, E.W. **Estudo sobre os fatores que afetam a intenção de compras online**. REGE-Revista de Gestão.1 de Abril. 24(2):181-94. 2017. *E-book*.

GONÇALVES, L. R. O. **Um modelo para verificação, homologação e certificação de aderência a norma nacional de segurança da informação – NBR-ISSO / IEC-17799**. 2005. 189f. Tese (Mestrado em Ciências em Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro, COPPE – Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Rio de Janeiro. *E-book*.

GOOGLE. **Gerenciar o Histórico de localização**. Disponível em: <<https://support.google.com/accounts/answer/3118687?hl=pt-BR>>. Acesso em: 04 abr. 2021.

GORENDER, Jacob. **Globalização, tecnologia e relações de trabalho**. Estudos avançados, 1997. Disponível em: <[https://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0103-40141997000100017](https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40141997000100017)>. Acesso em: 24 abr. 2021.

GRAEF, Inge. **Market definition and market power in data: the case of online platforms**. Word Competition, Amsterdam, n.4, p.473-506, 2015. *E-book*.

GROSSI, Bernardo Menicucci. **Lei geral de proteção de dados. Uma análise preliminar da lei 13.709/2018 e da experiência de sua implantação no contexto empresarial**. Porto Alegre, RS: Editora Fi, 2020. *E-book*.

HADNAGY C.; MAXWELL, E. **Social Engineering Defined. Social engineering framework**. 2009. Disponível em: < [http://www.social-engineer.org/framework/Social\\_Engineering\\_Defined](http://www.social-engineer.org/framework/Social_Engineering_Defined) >. Acesso em: 05 abr. 2021.

KONDER, Carlos Nelson De Paula; DE SOUZA, Amanda Guimarães Cordeiro. **Onerosidade Do Acesso Às Redes Sociais**. Revista de Direito do Consumidor, 2020. *E-book*.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 3. ed. São Paulo: Atlas, 1991. *E-book*.

LIPOVETSK, Gilles. **A felicidade paradoxal: ensaio sobre a sociedade de hiperconsumo**. São Paulo: Companhia das Letras, 2007. *E-book*.

MAIDIQUE, M. A.; HAYES, R. H. **The art of high-technology management**. Sloan Management Review, 1984, 25.2: 17-31. Disponível em: < <https://books.google.com.br/books?hl=pt-PT&lr=&id=kgFgksillkYC&oi=fnd&pg=PR7&dq=high+technology&ots=wjbNWyaiuo&sig=zt5L0M-UMhq0BAzoVaulzLO36EY#v=onepage&q=high%20technology&f=false> > Acesso em 31 mai. 2021.

MARCIANO, J. L.; MARQUES, M. L. **O Enfoque Social da Segurança da Informação**. Revista Ciência da Informação, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006. *E-book*.

MARQUES, Claudia Lima. **Proteção do consumidor no comércio eletrônico a chamada nova crise do contrato: por um direito do consumidor aprofundado**. Doutrinas Essenciais do direito do consumidor, São Paulo: Ed. RT, 2014. *E-book*.

MARTINS, Grilherme Magalhaes. **Responsabilidade civil por acidente de consumo na internet**. 2. Ed. São Paulo: Ed. RT, 2014. *E-book*.

MARTINS, Grilherme Magalhães; LONGHI, João Victor Rozatti. **A tutela do consumidor nas redes sociais virtuais: responsabilidade civil por acidentes de consumo na sociedade de informação**. Revista de Direito do consumidor, São Paulo, a.20, v.78, p.191-220, abr-jun. 2011. *E-book*.

MELO, A. M. A. J., SILVEIRA N., SOUZA, M. L. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann**. 2017. Disponível em: <<https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann>>. Acesso em: 28 abr. 2021.

MONTEIRO, António Pinto. **Contratos de adesão e cláusulas contratuais gerais: problemas e soluções**. Estudos em Homenagem ao Prof. Doutor Rogério Soares, Studialuridica, v. 61, 2001. *E-book*.

MOREIRA, Diogo Rais Rodrigues; BARBOSA, Nathalia Sartarello. **O reflexo da sociedade do hiperconsumo no Instagram e a responsabilidade civil dos influenciadores digitais**. Revista Direitos Culturais, Santo Ângelo, ISSN 2177-1499, v. 13, n. 30, maio-ago. 2018. Disponível em: [<http://srvapp2s.urisan.tche.br/seer/index.php/direitosculturais/article/view/2706/1295>] . Acesso em: 30.03.2020.

NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais**. Disponível em: <<https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>>. Acesso em: 21.04.2021.

NETFLIX, Inc. **Black Mirror: todos os seus dados**. Disponível em: <<https://www.netflix.com/watch/70264856?trackId=13752289&tctx=0%2C3%2C52ac5911680db8825f3ed8de51caad55feaa900b%3A0b1e71e7d15771e332d0ae1bab1d68220dfe0680%2C52ac5911680db8825f3ed8de51caad55feaa900b%3A0b1e71e7d15771e332d0ae1bab1d68220dfe0680%2Cunknown%2C>>. Acesso em: 09.04.2021.

NUNES, Rizzatto. **Comentários ao Código de Defesa do Consumidor**. 8. ed. São Paulo: Saraiva, 2015. *E-book*.

PEIXOTO, Mário César Pintaui. **Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas organizações**. Monografia (Bacharelado)– Curso de Ciência da Computação – Pró-Reitoria de Ensino de Graduação do Centro Universitário do Triângulo. Uberlândia: Unitri, 2004. *E-book*.

PERLINGHERI, Pietro. **In tema ditipicita e atipicita Nei contratti. Il diritto dei contrattifra persona e mercato: problemi Del dirittocivile**. Napoli: ESI, 2003. *E-book*.

RAD, Amir Afrasiabi; BEYOUCEF, Morad. **A Model for understanding social commerce. Conference on information systems applid research**. V.3, n. 1.511. *E-book*.

NASHVILLE, 2010. **A model for understanding social commerce**. Disponível em: <[HTTP://proc.conisar.org/2010/pdf/1511.pdf](http://proc.conisar.org/2010/pdf/1511.pdf)>. Acesso em: 10 mai. 2021.

SERPRO. **OBJETIVO E ABRANGÊNCIA DA LGPD**. Disponível em: <<https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/objetivo-e-abrangencia-da-lgpd>>. Acesso em: 05 mai. 2021.

SIMAS, Diana Viveiros de. **O cibercrime**. Lisboa: Universidade Lusófona de Humanidades e Tecnologias. 2014. *E-book*.

STJ 4ºT. **REsp 844736** / DF, Rel. Min. Luis Felipe Salomão,j.27.10.2009. publ. Dje.02.09.2010.

TJSC. **RE219.7800**, rel. Min. Carlos Mário Velloso julgado em 13 de abril de 1999. MS 22.801, rel. Min. Carlos Alberto Menezes Direito, julgado em 17 de dezembro de 2007.

VERAS, Gésio de Lima; BRITO, Dante Ponte de. **Publicidade subliminar: violação dos direitos do consumidor e o direito à reparação por dano moral coletivo**. Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo, Minas Gerais.e-ISSN: 2526-0030, v. 1, n. 2, p. 45-61, jul.-dez. 2015. Disponível em: [<https://indexlaw.org/index.php/revistadgrc/article/view/86>]. Acesso em: 18.03.2020.

VERBICARO, Dennis; SILVA, Camille Barroso. **O assédio de consumo no âmbito da publicidade infantil**. Revista Direitos Sociais e Políticas Públicas (UNIFA-FIBE). ISSN 2318 -573. v. 5, n. 2, 2017. Disponível em: <[www.researchgate.net/profile/Dennis\\_Verbicaro/publication/322571640\\_O\\_ASSEDI\\_O\\_DE\\_CONSU-MO\\_NO\\_AMBITO\\_DA\\_PUBLICIDADE\\_INFANTIL/links/5a6a6f25458515b-2d0532b91/O-ASSEDIO-DE-CONSUMO-NO-AMBITO-DA-PUBLICIDADE-INFANTIL.pdf](http://www.researchgate.net/profile/Dennis_Verbicaro/publication/322571640_O_ASSEDI_O_DE_CONSU-MO_NO_AMBITO_DA_PUBLICIDADE_INFANTIL/links/5a6a6f25458515b-2d0532b91/O-ASSEDIO-DE-CONSUMO-NO-AMBITO-DA-PUBLICIDADE-INFANTIL.pdf)>. Acesso em: 17.03.2020.