REVISTA ACADEMICA
Faculdade de Direito do Recife
Vol.93 N.02 - Anno CXXX

COOKIES PARA QUEM?
Entre o escambo digital e os direitos à privacidade e proteção de dados

COOKIES FOR WHO?
Between the digital barter and the rights to privacy and data protection

Mario Filipe Cavalcanti[1]

Recebimento em 15/03/2021
Aceito em 17/06/2021

RESUMO

A partir da ideia de escambo digital exposta como a troca de dados e informações pessoais pelos consumidores das plataformas, para acesso a conteúdos *on-line* dessas plataformas, busca-se analisar as lógicas e práticas de armazenamentos de ficheiros de pequenos dados (*cookies*) que, acumulando-se e sendo acessados por "terceiros invisíveis", podem permitir extensa influência sobre o comportamento humano. Para além disso, por intermédio de revisão bibliográfica, da análise de alguns sítios eletrônicos que se utilizam dessas ferramentas e das informações técnicas prestadas pela comunidade Mozilla no Brasil, visa-se escrutinar como se dá a funcionalidade desse tipo de ferramenta de captação de dados, e como tais lógicas de economia digital se relacionam com o aparato legal atualmente vigente no Brasil acerca da garantia dos direitos à privacidade e à proteção de dados dos indivíduos e, sobretudo, se há garantia da autodeterminação dos indivíduos e o exercício efetivo de seu consentimento na navegação *on-line* pelo uso dessas ferramentas ou se o tipo de escambo que é realizado é enviesado.

Palavras-chave: C*ookies.* Escambo digital. Privacidade. Proteção de dados.

ABSTRACT

From the idea of digital barter exposed as the exchange of data and personal information by the platform's consumers to access online content on these platforms, we seek to analyze the logic and practices of storing small data files (cookies) that, accumulating and being accessed by "invisible third parties", can allow extensive influence on human behavior. In addition, through a literature review, the analysis of some websites that use these tools and the technical information provided by the Mozilla community in Brazil, the aim is to scrutinize how the functionality of this type of data capture tool works, and how such digital economy logics relate to the legal apparatus currently in force in Brazil regarding the guarantee of the rights to privacy and data protection of individuals and, above all, if there is a guarantee of self-determination of individuals and the effective exercise of their consent in online browsing by using these tools or if the type of barter that is carried out is biased.

Keywords: Cookies. Digital barter. Privacy. Data protection.

[1] Mestrando em Ciências da Comunicação pela Universidade de São Paulo, Pesquisador Membro do Grupo de Estudos Semióticos em Comunicação, Cultura e Consumo (GESC3) da Universidade de São Paulo. Pesquisador Externo no IDP Privacy Lab do Centro de Direito, Internet e Sociedade (CEDIS-IDP). Bacharel pela Faculdade de Direito da Universidade Federal de Pernambuco. Advogado em Propriedade Intelectual, Privacidade e Proteção de Dados. Membro Efetivo da Comissão Especial de Direito Digital da OAB/SP. Perito Judicial em Propriedade Intelectual no Tribunal de Justiça de São Paulo. Escritor e editor de artes, Vencedor do 3º Prêmio Pernambuco de Literatura.

1 INTRODUÇÃO: DANDO NOME AOS RASTROS E EXPLORANDO OS SIGNIFICADOS

Custou-se a entender que como em um terreno arenoso nossos passos na *web* deixam marcas, pegadas digitais (SUMPTER, 2019, p. 57) que não se apagam facilmente. E não se apagam porque servem para outros. Saber por onde andamos e o que fazemos com esse direito que as Constituições democráticas nos dão é muito valioso para determinados atores sociais, muitas vezes ocultos nas interfaces coloridas dos dispositivos digitais. Como alertaram os professores Nick Couldry e Andreas Hepp (2020, p. 132):

> O espaço social tem sido transformado pela capacidade de outros invisíveis (ou sistemas invisíveis) de *nos ver* a uma distância variável, quer estejamos parados ou em movimento. Isso não se dá como na ficção científica, porque literalmente carregamos câmeras em nosso corpo, mas porque um *software* permite que os traços de texto e imagem que deixamos *on-line*, bem como os dados deles derivados, sejam capturados remotamente e fiquem disponíveis para novas trocas e novos processamentos.

Esses traços de texto e imagem costumeiramente ignorados e encarados como irrelevantes, ganham o curioso nome de *cookies* e são umas das inúmeras ferramentas de coleta de dados de navegação nos meios digitais, voltadas à identificação, perfilização, predição e, com isso, à modelação comportamental (ZUBOFF, 2020, p. 19).

Segundo Marcel Verrumo (2016), a explicação para esse tipo de denominação estaria no dito popular britânico, uma vez que "*cookie* é também uma gíria para 'pessoa de um determinado tipo'. Ou seja, uma figura ou estereótipo. E é exatamente essa a função dos *cookies* da internet: moldar um perfil determinado do usuário".

Por mais que a função desempenhada pelos *cookies* seja também de perfilização, não podemos deixar de pensar que a denominação, por si mesma, é construída para a realização de um efeito psicológico sobre nós. A ideia é fazer entender que se trata de coisa pequena, irrelevante, de "biscoitos", como aqueles que se dá com naturalidade a um pequeno cão que se sai bem em uma tarefa.

Percebe-se, portanto, que o efeito significante desse tipo de linguagem sobre o usuário das plataformas digitais é preocupante, tendo em vista que este é levado a pensar que se trata de algo irrelevante, de "biscoitos" dados aos provedores e desenvolvedores de plataformas, *sites* e *Apps* pra facilitar o acesso aos conteúdos e maximizar a experiência *on-line*. Esse raciocínio favorece um novo tipo de troca, de dados por acesso a conteúdo *on-line*, a que chamamos escambo digital.

Para os atores econômicos trata-se, de fato, de uma simples troca de mercadorias, sendo proveitosa para eles a divulgação dos dados como "o novo petróleo" (LEMOS, 2018) ou as "novas *commodities*". Emprega-se, assim, por meio da linguagem economicista uma redução de complexidade que nos leva a pensar que nessa troca de dados por navegação, os primeiros custam pouco. Mas o que, exatamente, custa tão pouco?

Nos últimos anos temos testemunhado o esforço no desenvolvimento de ferramentas tecnológicas digitais para que, por meio de algoritmos gerenciados por *Big techs*, os nossos *clicks* sejam registrados, cada acesso a *websites*, cada movimento nas *webpages*, cada deslocamento geográfico, tudo isso salvo em nossos próprios computadores e celulares inteligentes por intermédio do navegador de *internet* que usamos (ALVES, 2018) e para que fiquem à disposição do Google e de um "exército" de empresas que adquirem anúncios nas plataformas, como alertou o professor da Universidade de Uppsala:

> Enquanto você está *on-line*, o Google coleta informações dos *sites* que você visita e usa esses dados para decidir que anúncios lhe mostrar. (...) Todas as grandes empresas da *internet* – incluindo Google, Yahoo, Facebook, Microsoft e Apple –

> constroem um quadro personalizado de nossos interesses e o utilizam para decidir que anúncios nos mostrar. (SUMPTER, 2019, p. 20-21)

Esse quadro personalizado, perfis *on-line* de nosso eu, espécies de arquétipos do consumo como temos dito (CAVALCANTI, 2020a), nos pintam não como somos, mas o que importa em nós: como nossas informações podem ser utilizadas de modo vigilante e eficaz para exercer controle sobre nós, tanto do ponto de vista político, quanto do estímulo ao consumo.

Para a completa realização dessa lógica mais e mais dados são necessários (MOROZOV, 2018, p. 39), tendo em vista que não são eles, pura e simplesmente, que interessam aos agentes econômicos, mas os dados são o caminho pavimentado para o conhecimento e é, justamente, o conhecimento sobre seus titulares (BIONI, 2021, p. 10-11) – que pode ser obtido a partir desses dados, mediante a utilização de técnicas de *Big data* –, que interessa às plataformas.

Não há ética possível nesse desiderato sem uma efetiva, ampla e global regulação do setor, inclusive de uma regulação que reflita não somente o passado e o presente, mas também o futuro, considerando os novos tempos acelerados em que vivemos e a constante disrupção das tecnologias digitais. Isso porque, como lecionaram Couldry e Hepp (2020, p. 170), citando Bowker:

> Uma base de dados possui um tipo de poder organizador com base em um "princípio de exclusão" que determina o que pode e o que não pode ser armazenado de uma determinada forma. O que não é classificado se traduz como invisível.

Esse poder da invisibilidade e da invisibilização tem sido atribuído a algoritmos construídos por cientistas da computação, voltados ao atendimento das lógicas econômicas que justificam a sua implementação industrial, sem qualquer reflexividade sobre a complexidade das ontologias humanas ou das relações sociais.

Isso porque, se de um lado essas ferramentas prosseguem como "caixas-pretas" (MARTINS; SCHOR, 2021, p. 1) invisíveis não somente ao olho, mas também à compreensão dos atores sociais que não possuem conhecimento de computação e nem são os agentes econômicos que detém a propriedade industrial dessas ferramentas, de outro lado acabam por perpetuar em meio digital determinados *standards* de invisibilidade e discriminação já encontrados nas conflituosas relações sociais.

Para além desses aspectos, invisível também é a intangibilidade humana por trás dos dados. Não interessaria a tais agentes econômicos as assimetrias, opacidades e negatividades que fazem parte dos aspectos ontológicos de nossa construção como seres humanos (HAN, 2017, p. 11), mas apenas as nossas pegadas digitais, isto é, o que fazemos *on-line* e o que nos motiva a votar ou a comprar.

São, portanto, os nossos dados que movem a nova economia digital (SRNICEK, 2017, p. 4) e é isso que faz pairar no ar a pergunta do professor Jean Tirole (2020, p. 422):

> Poderemos controlar o acesso aos nossos próprios dados, bem como sua confidencialidade, ou seremos prisioneiros de uma empresa, uma profissão ou um Estado guardando ciosamente o controle do acesso a esses dados?

O presente artigo visa, portanto, a partir do breve escrutínio desse escambo digital, lançar luz sobre as lógicas e práticas de armazenamento de ficheiros de pequenos dados que, acumulando-se e sendo acessados por terceiros invisíveis, podem permitir extensa influência sobre o comportamento humano. Por intermédio de revisão bibliográfica e da observação de alguns sítios eletrônicos que se utilizam dessas ferramentas e das informações técnicas prestadas pela comunidade Mozilla no Brasil, visa-se escrutinar como se dá a funcionalidade desse tipo de ferramenta de captação de dados, e como tais lógicas de economia digital se relacionam com o

aparato legal atualmente vigente no Brasil acerca da garantia dos direitos à privacidade e à proteção de dados dos indivíduos e, sobretudo, se há garantia da autodeterminação dos indivíduos e o exercício efetivo de seu consentimento na navegação *on-line* pelo uso dessas ferramentas ou se o tipo de escambo que é realizado é enviesado.

2 ENTENDENDO QUE TIPO DE ESCAMBO É O ESCAMBO DIGITAL

Conforme pudemos ver em linhas gerais acima, entendemos que a relação de troca de dados por acesso a conteúdo *on-line*, portanto, à navegação, tem se mostrado como um novo tipo de permuta econômica a que denominamos escambo digital.

Por escambo entende-se historicamente todo e qualquer **sistema de trocas direta de uma mercadoria por outra**, sem qualquer mediação monetária (AULETE, 2004, p. 325). Tal sistema em voga nos recônditos da idade média europeia antes da criação e fortalecimento dos sistemas bancários, pôde ser observado de forma ampla no Brasil quando dos primeiros contatos entre os conquistadores europeus, à época "traficantes de pau-brasil" e "guarda-costas" (MARCHANT, 1943, p. 36), com os povos originários da terra.

No primeiro caso, temos a operação do escambo de modo pleno, onde as populações trocavam mercadorias que possuíam por aquelas de que necessitavam, sendo este um sistema econômico onde o valor dos produtos e serviços se baseava no nível de escassez e de necessidade, imperando, portanto, o binômio necessidade / possibilidade, bem como a plena ciência de todas as partes envolvidas (boa-fé), quanto à natureza desse binômio.

No segundo caso temos um escambo lastreado no deslumbre e no engodo. Isso porque, a troca, por exemplo, de centenas de milhares de toras de pau-brasil extremamente caras ao comércio de tecidos e estamparias europeu da época, por bugigangas de latão, espelhos e machados, chamados *matihi* (adornos) pelos povos originários (KOPENAWA; ALBERT, 2015, p. 408) não parece se lastrear no binômio acima, nem na boa-fé. Note-se que, como alertado pelo historiador estadunidense Alexander Marchant (1943, p. 39-41), nessas trocas estava incluso o trabalho braçal de corte e carregamento pelo continente até o litoral de centenas de milhares de toras tão largas e altas de pau-brasil, que os europeus nunca conseguiriam transportar sem o emprego de centenas de nativos por meio desse engodo.

Vê-se, portanto, que acessória à compreensão do escambo está a constatação de que tipo de escambo se está falando e do nível de independência e, para se utilizar uma terminologia atual, de autodeterminação há em ambos os lados da troca econômica. Ambos os fatos históricos apontados acima se tratam de sistemas econômicos de troca. O primeiro seria aprovado pelos ordenamentos jurídicos democráticos atuais, caso se implantasse – e tem retornado a partir da crise de 2008, através do que se tem chamado "escambo corporativo" (GRAGNANI; VOLPINI, 2013) –, já o segundo, não seria aprovado, considerando que lastreado no engodo da parte hipossuficiente da relação de troca.

Tal compreensão é importante ao objeto desse estudo, porque o escambo digital mais se afigura ao segundo exemplo que ao primeiro, isto é, suas lógicas e práticas parecem se galgar mais no engodo e na oportunidade do que na autodeterminação e no consentimento livre, pleno e desimpedido dos cidadãos, mais nos critérios de deslumbre e desconhecimento, do que no binômio necessidade / possibilidade.

Nesse sentido, entendemos que os *cookies*, como uma das ferramentas representativas das lógicas de captação de variados dados, acumulação de grandes volumes e tratamento em alta velocidade desses dados, portanto, integrante direta da lógica de *Big data* (LANEY, 2001), é exemplificativo do efeito de sentido sobre as pessoas e de quão determinante é a lógica do escambo do engodo, que é o escambo digital.

Razão disso, primeiramente discorreremos sobre a sua lógica de funcionalidade, inclusive por meio da observação de alguns sites que os utilizam, em seguida explicaremos as razões para chegarmos à conclusão brevemente adiantada acima.

3 A LÓGICA DOS *COOKIES*

Numa matéria que repete o título de dezenas de outras que abordam o assunto, ilustrada com a reprodução fotográfica de um biscoito com gotas de chocolate de 17 por 15 cm, Gabriel Gugik (2008) explica:

> Basicamente, um *Cookie* é um arquivo de texto muito simples, cuja composição depende diretamente do conteúdo do endereço *Web* visitado. Por exemplo, a maioria dos sites armazenam informações básicas, como endereços IP e preferências sobre idiomas, cores, etc. Contudo, em portais como o Gmail e o Hotmail, nomes de usuários e senhas de e-mail também fazem parte dos *Cookies*.

O que Gurgik não explica é que muito mais informações pessoais de um usuário ficam armazenadas como dados de navegação de rede pelos *cookies*, e esses dados são geridos segundo o crivo do provedor, sem nenhuma participação consciente, livre, informada e inequívoca do usuário, conforme determinado pelo art. 5º, inciso XII da Lei Geral de Proteção de Dados Pessoais brasileira (LGPD).

O *site* do Tribunal Regional do Trabalho da Segunda Região, por exemplo, divulga o seguinte anúncio sobre as informações coletadas do usuário que navega por suas páginas:

> Quando um usuário acessa o site do TRT da Segunda Região, são registradas as seguintes informações:
> - data e hora dos acessos;
> - páginas visitadas;
> - tipo de browser;
> - Endereço de IP - Internet Protocol (nº associado ao computador sempre que um usuário se conecta à Internet);
> - ação que o usuário tentou executar (download de um documento, por exemplo) e se obteve êxito;
> - endereço de outro site, caso o acesso ao site do TRT da Segunda Região se dê por meio de link.
>
> Podem ser registradas as seguintes informações relativas a mensagens eletrônicas (e-mails):
> - endereço eletrônico;
> - nome do usuário;
> - assunto;
> - conteúdo da mensagem. (BRASIL, 2021).

Não se pode ignorar o quantitativo de informações armazenadas, com destaque para data e hora de acessos, páginas visitadas e conteúdo dos eventuais e-mails trocados. Em resumo, não há garantias de privacidade. Veja-se que estamos falando do *site* de um dos Tribunais Regionais que compõem o Poder Judiciário federal.

A página colaborativa de programadores da comunidade Mozilla no Brasil, dá a seguinte definição técnica para *cookies*:

> Um *cookie* HTTP (um *cookie web* ou *cookie* de navegador) é um pequeno fragmento de dados que um servidor envia para o navegador do usuário. O navegador pode armazenar estes dados e enviá-los de volta na próxima requisição para o mesmo servidor. Normalmente é utilizado para identificar se duas requisições vieram do mesmo navegador — ao manter um usuário logado, por exemplo. Ele guarda informações dinâmicas para o protocolo HTTP sem estado (MOZILLA, 2021).

Expondo a sua operacionalização oculta ao usuário da rede, os programadores da comunidade Mozilla, explicam:

> Ao receber uma requisição HTTP, um servidor pode enviar um cabeçalho '*Set-Cookie*' com a resposta. O *cookie* normalmente é armazenado pelo navegador, então o *cookie* é enviado com as requisições feitas para o mesmo servidor dentro do cabeçalho HTTP *Cookie*. Uma data de expiração ou duração pode ser especificada, e após esta data o *cookie* não é mais enviado. Adicionalmente, restrições para um domínio específico e caminho podem ser configuradas, limitando para onde o *cookie* é enviado. (MOZILLA, 2021).

Portanto, o pronto acesso a um *website* já permite ao servidor utilizado pelo usuário registrar os seus rastros, armazenando informações básicas, mas também complexas e específicas da atividade de navegação que, acumuladas, podem oportunizar um acesso irrestrito a aspectos íntimos da privacidade do indivíduo, como o conteúdo de sua navegação *on-line*.

E fático também é que, para além das possibilidades de configurações de *cookies* de sessão (sem "*Expires"* ou "*Max-Age*")[2], havendo restauração de sessão (funcionalidade permitida pelo Google e outros navegadores *web* para recuperação de páginas fechadas não intencionalmente, por exemplo), os *cookies* podem ser novamente resgatados, estendendo sua validade também para terceiros que exerçam monitoramento dos traços de rede.

Doutro lado, *cookies* permanentes estabelecem "*Expire"* e *"Max-Age"*, todavia, com datas de validade e duração frequentemente ignoradas por completo pelos usuários, permitindo acesso contínuo do navegador utilizado ou mesmo de terceiros completamente estranhos à relação de acesso, aos dados e informações de tráfego *on-line*, independente da atividade efetiva do usuário no momento da captação dos dados.

Os programadores da comunidade Mozilla (2020) explicam que os *cookies*, em específico:

> São usados principalmente para três propósitos:
> **Gerenciamento de sessão**
> Logins, carrinhos de compra, placar de jogos ou qualquer outra atividade que deva ser guardada por um servidor.
> **Personalização**
> Preferências de usuário, temas e outras configurações.
> **Rastreamento**
> Registro e análise do comportamento de um usuário.

Vê-se que o risco na utilização de *cookies* se dá, justamente, nos aspectos da personalização – e do nível de personalização que é gerada e com quais finalidades –, e do rastreamento, aspecto que rompe todos os limites da privacidade.

Em seu livro entusiástico das soluções trazidas pela mediação algorítmica na era digital, os matemáticos estadunidenses Brian Christian e Tom Griffiths (2017, p. 18) confessam que:

> Hoje em dia, o projeto de algoritmos envolve não só a ciência da computação, matemática e engenharia, mas também campos correlatos como estatística e pesquisa operacional. E ao considerar que algoritmos projetados para máquinas podem ter relação com mentes humanas, também precisamos dar uma olhada em ciências cognitivas, psicologia, economia, e muito mais.

O que os pesquisadores estadunidenses não dizem é que esse "dar uma olhada em ciências cognitivas, psicologia, economia e muito mais", esconde uma profundidade alarmante: a da

[2] Tratam-se de *cookies* sem data específica de expiração que deveriam expirar com o fechamento das páginas da *web* ao fim do acesso.

invasão da privacidade dos indivíduos e da manipulação comportamental gestada a partir das lógicas mais íntimas do *Big data*, cujos variados mecanismos de captação e mineração de dados também perpassam os *cookies*.

Vemos, portanto, que não há nada de "pequeno" e irrelevante nos *cookies*, muito pelo contrário, estes se tornaram uma espécie de ferramenta imperativa do escambo digital, na qual para se ter acesso a serviços *on-line*, os consumidores repassam além de suas informações, autorizações à monitoração dos seus passos *on-line*, ainda que sem saber.

O que há, portanto, é um novo tipo de escambo, um escambo digital, no qual, tal como se dava com os ameríndios há mais de quinhentos anos, informações absolutamente relevantes são trocadas diariamente por miçangas e espelhos.

Diante da importância das informações repassadas pelos usuários da *internet*, o acesso a determinados serviços é que se mostra irrelevante e percebemos que, se considerarmos por *cookies* a lógica da "coisa pequena", da "coisa pouca", que parece se querer encucar, só poderíamos concluir que essas coisas pequenas não são os dados repassados (sem saber) pelos usuários às plataformas digitais, mas sim, o acesso a essas plataformas de conteúdo *on-line*.

4 DOS *COOKIES* COMO FERRAMENTAS REPRESENTATIVAS DAS LÓGICAS DO ESCAMBO DIGITAL

Vê-se, portanto, que os *cookies* são os fenômenos mais elementares das práticas de captação de dados do novo estágio do que se veio a chamar "capitalismo de vigilância" (ZUBOFF, 2018, p. 89).

Isso porque, se de um lado, o uso dos *cookies* permitiu uma experiência mais personalizada de navegação nas redes (SALESFORCE, 2020), inclusive nas plataformas de *streaming*, garantindo o armazenamento de dados de acesso, sem que se tenha de repetir atos de *login* ou refazer operações já realizadas, permitindo uma rememoração pela máquina dos caminhos trilhados pelo usuário e garantindo, assim, maior comodidade na navegação – tal se observa com facilidade nas funcionalidades da plataforma Netflix, por exemplo –, de outro lado, esse tipo de comodidade não é gratuita e o custo é demasiado alto: a nossa privacidade, considerando que a mesma máquina que aprende o que fazemos é a máquina que aprende como funcionamos e remete aos agentes econômicos (de forma oculta) informações valiosas que serão utilizadas para predição e modelagem comportamental (ZUBOFF, 2020).

Como alertaram Hannes Grassegger e Mikael Krogerus:

> Tudo o que fazemos, tanto *on-line* como *offline*, deixa vestígios digitais. Cada compra que fazemos com nossos cartões, cada busca que digitamos no Google, cada movimento que fazemos quando nosso celular está em nosso bolso, cada *link* é armazenado. Especialmente cada *like*.

Esses vestígios digitais têm o objetivo claro de não se limitarem no tempo, de não serem poucos ou tangenciáveis, a lógica de *Big data* é de acumulação de informações para a garantia de maior computação que permita, com as análises probabilísticas, acumulação financeira e a construção de espécies de consumidores que perdem cada dia o controle da racionalidade sobre o ato de consumir, tornando-se verdadeiros "drogados do consumo" (LIPOVETSKY; SERROY, 2015, p. 31).

E essa é a razão do avanço absolutamente gigantesco das novas interfaces tecnológicas do mundo digital conectadas à *internet*, afinal, como no dizer de Magrani (2018, p. 21) "quanto maior o número de dispositivos conectados, mais dados são produzidos" e assim o é porque "quanto mais *inputs* disponíveis, melhores as previsões serão" (SUMPTER, 2017, p. 49).

Todos esses dados não somente se apresentam como um risco, diante do que se pode descobrir sobre nós, mas também, do que se pode inveridicamente deduzir sobre nós ou nos fazer

crer que somos ou queremos. Os professores Nick Couldry e Andreas Hepp (2020, p. 173) já nos alertaram sobre esse processo de "tipificação" do humano, vejamos:

> Os próprios artefatos das bases de dados de hoje em dia operam para tipificar seres humanos principalmente para fins comerciais e de vigilância, para construir um mundo integrado e contínuo para o comércio e o controle.

Nessa mesma esteira também se debruçaram David Sumpter (2019, p. 63-76) – analisando as probabilidades de falhas desses sistemas probabilísticos que compõem os algoritmos, que tratam dados captados de variadas formas, inclusive por intermédio de *cookies*, e os efeitos sobre a vida política e social das pessoas – e Cathy O'Neil (2020, p. 46) – que vê os algoritmos como modelos matemáticos impregnados dos vieses dos cientistas de dados, seus criadores, e dos empresários, seus investidores/detentores.

A doutrina jurídica brasileira especializada na temática já demonstra a percepção da necessidade de impedir tais atos discriminatórios a partir de uma tutela dos dados com o fim de desestimular "práticas autoritárias e de vigilância por parte de instituições públicas e privadas" (TEPEDINO; TEFFÉ, 2020, p. 282).

Portanto, a questão a que nos deparamos é: se a justificativa para a instalação automática dessas funcionalidades nos computadores e celulares inteligentes é a garantia de comodidade na navegação *on-line*, por que os *cookies* são programados também para rastrear e perfilar? Não bastaria que fossem somente gerenciadores de sessão?

A resposta a essas perguntas não prescinde da compreensão das lógicas do capitalismo de vigilância. Isso porque, se a troca realizada nos *cookies* se desse apenas para garantia da comodidade, teríamos um típico escambo de binômio, como visto acima, onde se troca bens de valores equiparáveis. No entanto, essa comodidade na navegação aqui figura como os adornos, espelhos e miçangas. Para que a lógica do mercado funcione e a mineração de dados gere receitas, é preciso que os *cookies* sejam muito mais que facilitadores da navegação *on-line*, é preciso que sejam ferramentas de espionagem e eis aqui, portanto, a natureza enganosa do escambo digital.

5 A RELEVÂNCIA DA REGULAÇÃO ESTATAL SOBRE O ESCAMBO DIGITAL

Nesse sentido que a regulação do assunto se mostra como único horizonte civilizatório possível para que os novos avanços tecnológicos, aqui também representados por essas ferramentas, não signifiquem a bancarrota da privacidade e de outros direitos da personalidade, como os de proteção de dados.

Ao contrário do quanto sugerido por Marcel Leonardi (2011, p. 187), não se afigura razoável entender que uma forma efetiva para a proteção da disseminação de dados na internet seja a autotutela. Isso porque, as ferramentas de captação de dados, *cookies* entre elas, são, muitas vezes, invisíveis ou mesmo disponibilizadas em linguagem de programação, longe de uma percepção compreendida do senso comum (BUCHER, 2020).

Desse modo, os atos de criptografia de dados, utilização de navegadores anônimos, etc., permitem uma possibilidade de sigilo de navegação, não uma garantia fática, sobretudo, levando-se em consideração o desenvolvimento diário de novas ferramentas e *upgrades* técnicos para a captação e mineração agressiva de dados.

A solução a médio prazo parece residir firmemente em uma regulação estatal global da matéria. Discorrendo sobre o papel do Estado na determinação do desenvolvimento tecnológico, Manuel Castells afirmou (2020, p. 70):

> O que deve ser guardado para o entendimento da relação entre a tecnologia e a sociedade é que o papel do Estado, seja interrompendo, seja promovendo, seja liderando a inovação tecnológica, é um fator decisivo no processo geral, à medida

> que expressa e organiza as forças sociais dominantes em um espaço e uma época determinados.

Nesse esteio, acerca da necessidade de implementação, pelos governos, de limites a um desenvolvimento tecnológico desenfreado que ponha em xeque a capacidade humana de lidar com as novas tecnologias e permita um mar de malferimentos a direitos fundamentais dos cidadãos ao redor do mundo, inclusive por meio de uma inutilização dos seres humanos em suas relações de trabalho e de interação social, o historiador israelense Yuval Noah Harari (2018, p. 58-59), leciona:

> Os governos podem decidir retardar o ritmo da automação para reduzir seu impacto e dar tempo para reajustes. A tecnologia nunca é determinista, e o fato de que algo pode ser feito não quer dizer que deva ser feito. A legislação pode bloquear com sucesso novas tecnologias mesmo se forem comercialmente viáveis e economicamente lucrativas. Por exemplo, durante muitas décadas tivemos tecnologia para criar um mercado de órgãos humanos completo, com "fazendas de corpos" humanos em países subdesenvolvidos e uma demanda quase insaciável de compradores abastados. Essas fazendas de corpos poderiam valer centenas de bilhões de dólares. Mas a lei proíbe o livre comércio de partes do corpo humano.

E é nesse cenário de necessidade de garantia dos direitos dos indivíduos humanos à privacidade e à proteção de seus dados que temos visto o desenvolvimento de regulações estatais e, portanto, uma onda de implementação de normas jurídicas voltadas ao balanceamento das relações na era da informação, entre cidadãos hipossuficientes e grandes conglomerados econômicos com suas lógicas e práticas de *Big Data*.

No que concerne aos *cookies*, por exemplo, como ferramentas de programação para captação de dados durante a navegação *on-line*, duas legislações brasileiras, em diálogo com a Carta Magna, estabelecem o entendimento dos aspectos jurídicos de proteção que não devem ser ignorados quando da compreensão de nossa regulamentação legal da matéria.

a. O Marco Civil da Internet no Brasil

Promulgada com o intento de estabelecer "princípios, garantias, direitos e deveres para o uso da internet" é fático que, sob esse desiderato, construiu-se em verdadeira disciplina legislativa da proteção de dados e da privacidade dos cidadãos no Brasil, sobretudo em sua relação de consumo *on-line*.

Isso porque, ao estabelecer os princípios da disciplina do uso de redes digitais, aquele diploma legislativo garantiu o seguinte, senão vejamos:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei. (BRASIL, 2014)

Ora, a proteção dos dados pessoais tornou-se princípio básico expresso do diploma legal do Marco Civil da Internet (MCI), passando a regular as atividades de transmissão e transferências de informações em rede, assim como determinando a responsabilização dos controladores pelo desvio de tais princípios.

Indo mais longe, se de um lado estabeleceu que o acesso à internet seria "essencial para o exercício da cidadania", também determinou a inviolabilidade da intimidade do usuário da *web*

como direito e garantia fundamental, submetendo os seus infratores às indenizações para reparação dos eventuais danos morais ou patrimoniais decorrentes de sua violação, veja-se:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 2014)

Ainda nesse sentido, e certamente instituindo normativo completamente adequado, o MCI determinou nos incisos VII e VIII, do art. 7º, como assegurados os direitos dos particulares sobre a utilização dos dados na finalidade expressa pela contratação, salvo consentimento livre, expresso e informado:

> Art. 7º. (...) são assegurados os seguintes direitos:
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> justifiquem sua coleta;
> não sejam vedadas pela legislação; e
> estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais. (BRASIL, 2014)

Note-se que tal determinação legal advinda do MCI desde 2014 já demonstrava a necessidade de haver comunicação clara e inequívoca ao usuário da *web* acerca da captação de suas informações, expondo-se, inclusive, as finalidades de tal tratamento.

A essa determinação, e à sua posterior reafirmação a partir da promulgação da Lei Geral de Proteção de Dados Pessoais (2018) iniciou-se uma enxurrada de "avisos de *cookies*" em *webpages* com o intuito de capturar um "consentimento" formal dos usuários para a captação, armazenamento e transferências de *cookies*.

Todavia, como tal consentimento pode ser considerado efetivado, se o consumidor das *webpages* desconhece o que são *cookies*, quais suas funcionalidades exatas e quais as finalidades por trás de sua captação? Em outras palavras, como pode haver liceidade no escambo se não há boa-fé?

Ainda que inúmeros avisos abundem as páginas da internet, se não há compreensão livre e inequívoca dos usuários acerca de tais funcionalidades, haveria vício no consentimento diante dos direitos protegidos pelo ordenamento jurídico brasileiro. Ainda mais se considerarmos as dinâmicas e as novas lógicas de temporalidade acelerada trazidas pelas redes digitais (HAN, 2018, p. 66), nas quais a leitura de extensos "termos de privacidade" e "termos de uso de *cookies*", muitos deles repletos de jargão jurídico, impede de forma indireta o acesso à navegação, de modo que os usuários consentem sem ler, para poderem utilizar os serviços.

Ora, na Seção II do MCI, intitulada "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas", aquele diploma legal assim estabeleceu:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (BRASIL, 2014)

Portanto, vemos que a legislação brasileira segue um caminho de evolução de normas de garantia a direitos fundamentais à privacidade e à proteção de dados quando estabelece os regramentos acerca da captação e uso de dados pessoais de usuários da internet no Brasil, determinando que o tratamento válido de informações somente se dá dentro de determinados limites, respeitando-se a finalidades claras e previamente informadas, devendo o usuário decidir por anuir ou não de forma "consciente, livre e informada", constituindo, ainda, a responsabilização das plataformas nos casos de desvirtuamento de todos esses princípios e normativos legais.

b. A Lei Geral de Proteção de Dados Pessoais brasileira

Tal como na legislação federal supracitada, a LGPD assim determina quanto aos direitos dos cidadãos na garantia da proteção de seus dados, na inviolabilidade de sua intimidade, e vida privada etc.:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
>
> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. (BRASIL, 2018)

No campo dos regramentos ao tratamento dos dados, salta aos olhos as limitações impostas, vejamos:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
>
> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> (...)
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

> (...)
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados. (BRASIL, 2018)

Portanto, resta cristalino que a nova lei repisa determinações já há muito cogentes quanto à necessidade de consentimento prévio e consciente pelo titular dos dados, bem como da utilização dos dados em respeito da finalidade contratada, reascendendo a discussão acerca da efetividade do tipo de consentimento oportunizado pelas plataformas nas navegações.

O escambo digital é aqui, mais uma vez, posto à prova. Isso porque se "os donos dos dados são os donos do futuro" (HARARI, 2018, p. 102) e os donos dos dados são os cidadãos deles titulares, como se justifica que tais informações possam transitar livremente entre plataformas, prestadoras de serviços de internet, operadores de telefonia, mídias sociais, etc., gerando riquezas ao completo arrepio dos cidadãos titulares?

Quanto ao regramento e ao esclarecimento dos liames do consentimento do titular dos dados, a LGPD vai ainda mais longe que o MCI, deixando claramente firmadas a necessidade de consentimento expresso, direto, objetivo, consciente e para uma finalidade específica, como uma base legal ao tratamento de dados, senão vejamos:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
>
> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.
>
> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas. (BRASIL, 2018)

Cristalino, portanto, que o campo em questão está em plena disputa. Todavia, ainda mais cristalino que os normativos já presentes no ordenamento jurídico brasileiro, na mesma esteira de regulamentos os mais variados ao redor do mundo – como o Regulamento Geral de Proteção de Dados europeu ou o *Consumer Privacy Act* californiano – demonstram o enfoque e a predileção estatal pela regulamentação da matéria garantindo a proteção ao cidadão.

c. A proteção ao consumidor brasileiro no escambo digital

Nesse mesmo esteio, quando estamos tratando de captação de dados (por *cookies* ou outras ferramentas) a partir de relações de consumo *on-line* – seja de produtos de *e-commerce*, seja de serviços os mais variados como os prestados pelas próprias redes sociais digitais – resta cristalino que toda a disposição legal advinda das leis de proteção de dados, como o MCI e a LGPD, precisam ser interpretadas à luz do microssistema de proteção aos direitos do consumidor.

A própria LGPD possui disposição expressa nesse sentido, vejamos:

> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. (BRASIL, 2018)

Ora, o Código de Defesa do Consumidor (CDC) visa tutelar a relação de consumo e, nesse desiderato, impõe ao fornecedor a necessidade de prestar serviços sem falhas ou vícios, sob pena de responsabilização civil. Nesse sentido que, havendo defeitos relativos à prestação de serviço ou insuficiência nas informações prestadas ao consumidor, são responsáveis os fornecedores legalmente, conforme disciplina estampada no art. 14, *caput* do CDC, senão vejamos:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. (BRASIL, 1990)

Indo ainda mais longe, numa redação legislativa exemplar, o CDC expõe no parágrafo primeiro do art. 14, que o "serviço defeituoso" é aquele que não fornece ao consumidor a segurança que dele poderia esperar, senão vejamos:

> Art. 14.
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido. (BRASIL, 1990)

Nesse mesmo sentido, a LGPD, harmonizando-se com o dantes já previsto na norma consumerista, assim estabeleceu em seu art. 44:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - o modo pelo qual é realizado;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador[3] ou o operador[4] que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano. (BRASIL, 2018)

Há, portanto, plena harmonização entre a norma consumerista de 2002 e a norma de proteção de dados de 2018, estabelecendo para a violação de dados havida a partir da relação de consumo a responsabilidade objetiva do agente de tratamento. Sobre o assunto afirma Anderson

[3] Segundo o art. 5º, VI da LGPD, "Controlador", um tipo de "agente de tratamento de dados", é: "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

[4] Seguindo o art. 5º, VII da LGPD, "Operador", outro tipo de "agente de tratamento de dados", é: "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

Schreiber (2021, p. 26):

> É impossível deixar de notar que o art. 44 da LGPD exprime uma versão adaptada da noção de defeito do serviço, constante do art. 14§1º, do Código de defesa do Consumidor. Não seria absurdo coitar aqui de um 'tratamento defeituoso' dos dados pessoais, muito embora a LGPD não empregue explicitamente a noção de 'defeito' – como talvez devesse ter feito, em benefício de alguma coerência sistêmica, sem prejuízo da circunstância evidente de que a proteção de dados pessoais não se restringe às relações de consumo. O importante para o tema ora enfrentado é verificar que a LGPD emprega construção análoga nesta matéria àquela empregada na legislação especial que se ocupa da responsabilidade do fornecedor de produtos ou serviços, que consiste, como se sabe, em exemplo de responsabilidade objetiva, cuja configuração prescinde da verificação de culpa do causador do dano.

Portanto, além de haver nítida harmonia entre as normas que demonstra a proteção ao consumidor e a responsabilização objetiva do agente de tratamento que viola dados na relação de consumo, é inequívoco que a utilização dos dados para outras finalidades que não informadas inicialmente, ainda que por meio de violação da base de dados por terceiros, é suficiente para demonstrar quebra na expectativa do consumidor, como já aduzimos:

> Há quebra de confiança, portanto, e defeito na prestação do serviço, ainda que se fale em obrigação acessória, quando ocorre a desvirtuação da finalidade contratada, portanto, quando esses dados são utilizados para outras finalidades, inclusive por terceiros. (CAVALCANTI, 2021, p. 235)

Vê-se, portanto, que a lógica dos *cookies* tal como atualmente se desenha vai de encontro dos regramentos jurídicos de proteção de dados nas relações de consumo, uma vez que ao escambo digital, no qual as ferramentas sob análise se inserem como mecanismos de captação de dados, é imprescindível o deslumbre e o engodo e, portanto, não privilegia a autodeterminação plena dos cidadãos, uma vez que esse conhecimento pleno poderia gerar nítido *opt-out* que poria em cheque as lógicas de rastreamento, perfilização, predição e modelação comportamental que são caras ao capitalismo vigilante.

Há que se estudar a percepção dos cidadãos acerca da existência de *cookies* e inúmeras outras formas de capação e mineração de dados, mas o que já se pode depreender com assertividade é que o consumidor não acessa a *web* ciente de que precisa deixar algo em troca dos serviços, como o imaginário que já permeia a sua ida à farmácia – onde sabe que em troca do remédio, precisa deixar dinheiro. A lógica dos serviços *on-line* como serviços "gratuitos" e, mesmo, *freemium*, esconde o escambo e isso fere os regramentos de autodeterminação informativa do indivíduo, bem como permite a existência de quebra na expectativa e na confiança do consumidor.

Nesse sentido, a jurisprudência pátria tem reafirmado que o fornecedor que presta serviços eivados de falhas e vícios tem o dever de indenizar o consumidor, além de reparar tais falhas, também quando o assunto é a proteção de dados, portanto, a prestação de um serviço acessório ao principal, senão vejamos:

> APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE REPARAÇÃO POR DANOS MATERIAIS E MORAIS. FALHA NA PRESTAÇÃO DO SERVIÇO. WEB HOSTING. FALHA NA PRESTAÇÃO DE SERVIÇO. CONFIGURAÇÃO. Hipótese em que o conjunto probatório dos autos conforta a versão do autor, apontando para a ocorrência de falha na prestação de serviços prestados pela ré. Sentença mantida. (...) DANO MORAL. CONFIGURAÇÃO. Caso concreto em que a empresa autora teve sua imagem abalada, em razão da falha na prestação de serviço realizado pela ré, causando

> lesão à sua reputação e imagem. Caracterizado o dano moral puro, exsurgindo, daí, o dever de indenizar. Sentença mantida. *QUANTUM* INDENIZATÓRIO. MANUTENÇÃO. Na fixação da reparação por dano extrapatrimonial, incumbe ao julgador, atentando, sobretudo, para as condições do ofensor, do ofendido e do bem jurídico lesado, e aos princípios da proporcionalidade e razoabilidade, arbitrar quantum que se preste à suficiente recomposição dos prejuízos, sem importar, contudo, enriquecimento sem causa da vítima. A análise de tais critérios, aliada às demais particularidades do caso concreto, especialmente, os parâmetros comumente adotados por esta Câmara e pelo c. STJ, em situações análogas, conduz à manutenção do montante indenizatório em R$ 10.000,00 (dez mil reais). Sentença mantida. APELAÇÃO DESPROVIDA. (BRASIL, 2013)

Portanto, cristalino que o ordenamento jurídico brasileiro protege o titular dos dados, mesmo em sua relação de consumo, diante da sua utilização desavisada, para finalidades não contratadas e com consentimento vicioso. É preciso repensar as lógicas e práticas do escambo digital, portanto.

d. Salvaguarda Constitucional e aval do Supremo Tribunal Federal

Nesse sentido e, por fim, útil trazer à análise a disposição da norma constitucional que garantiu *status* de direitos fundamentais àqueles atrelados ao sigilo de dados e da inviolabilidade da intimidade e da vida privada, senão vejamos:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. (BRASIL, 1988).

Ora, se a proteção aos direitos do consumidor revelou-se instituto jurídico moderno, derivado das necessidades de equiparar e balancear as relações de comércio realizados com partes hipossuficientes economicamente em relação a grandes empresas, a proteção aos dados dos particulares tem se demonstrado demanda exaustiva da sociedade civil nos novos tempos da tecnologia da informação, lastreada pela própria norma constitucional brasileira desde 1988.

Segundo o magistério do Ministro Alexandre de Moraes (2016, p. 74), a determinação constitucional da inviolabilidade do sigilo de dados deve ser entendida como complementar à previsão ao direito da intimidade e da vida privada, tendo em vista que:

> A defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos *relativos* à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional.

Nessa mesma esteira, relevante a decisão proferida pela maioria absoluta do plenário do Supremo Tribunal Federal no julgamento das ADIs nº. 6387, 6388, 6389, 6390 e 6393, que reconheceu a proteção e o sigilo de dados como direitos fundamentais da personalidade, como se pode ver do seguinte excerto tirado do Voto da Relatora, a Ministra Rosa Weber:

> Entendo que as condições em que se dá a manipulação de dados pessoais digitalizados, por agentes públicos ou privados, consiste em um dos maiores desafios contemporâneos do direito à privacidade.
> A Constituição da República confere especial proteção à intimidade, à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). O assim chamado direito à privacidade (right to privacy) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.
> A fim de instrumentalizar tais direitos, a Constituição prevê, no art. 5º, XII, a inviolabilidade do 'sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal. (BRASIL, 2020)

Portanto, vê-se que os direitos à privacidade e à proteção de dados, reconhecidos com o *status* de direitos fundamentais da personalidade humana demonstram a relevância da análise de como mecanismos de captação de dados como os *cookies* e as lógicas de mercado a eles inerentes, como o escambo digital, precisam ser pensados e analisados diante do atendimento das normas jurídicas reguladoras do assunto que, em última análise, garantem, não somente a proteção do indivíduo humano, mas de seu agrupamento social e, portanto, do próprio processo civilizatório em que nos encontramos.

6 CONCLUSÃO

Vê-se, portando, que se o escambo digital, no qual estamos imersos, traz na figura dos *cookies* a ideia de pequenos agrados dados pelos usuários às plataformas para acesso aos conteúdos *on-line*, a realidade demonstra justamente o contrário, que as plataformas digitais é que dão *cookies* (agrados) aos seus usuários em troca de relevantes informações pessoais que são utilizadas, costumeiramente, para finalidades nunca assimiladas pelos consumidores.

Essas lógicas e práticas das plataformas de internet precisam ser analisadas sob a régua dos regulamentos presentes no ordenamento jurídico pátrio sob o ponto de vista mais favorável ao consumidor e, portanto, às pessoas físicas titulares de dados.

Nesse sentido, ainda que haja divergências doutrinárias sobre o tipo de responsabilidade estampado pela LGPD brasileira, somos convictos que a responsabilidade do agente de tratamento que viola ou permite a violação de dados no âmbito da relação consumerista é plenamente objetiva o que se dá pela aplicação harmônica e sistemática da LGPD cumulada ao CDC e à norma constitucional.

É preciso, portanto, que haja reflexividade por parte dos agentes econômicos na operacionalização de ferramentas como *cookies*, entre outras. Isso porque, a lógica de deslumbre e de engodo que perpassa o escambo digital permite violações de direitos e garantias fundamentais da personalidade, como a autodeterminação do ser (inclusive informacionalmente), a privacidade e a proteção de dados. Em outras palavras, para que o escambo digital seja válido, é preciso que se dê em respeito à boa-fé e à autodeterminação dos titulares dos dados, isto é, pode até haver deslumbre, mas não pode haver engodo.

REFERÊNCIAS

AULETE, Caldas. **Dicionário contemporâneo da língua portuguesa**. Rio de Janeiro: Nova Fronteira, 2004.

ALVES, Paulo. O que são *cookies?* Entenda os dados que os sites guardam sobre você. **Techtudo.** Disponível em: https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml. Acesso em: 14/03/2021

BIONI, Bruno Ricardo. **Proteção de dados pessoais**. A função e os limites do consentimento. Rio de Janeiro, Forense, 2021.

BITTAR, Eduardo; ALMEIDA, Guilherme. **Curso de filosofia do Direito**. São Paulo: Atlas, 2001.

BRASIL. **Constituição da República Federativa do Brasil**, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 14 mar. 2021

BRASIL. **Lei Federal nº. 8.078/1990**, "Código de Defesa do Consumidor". Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 14 mar. 2021

BRASIL. **Lei Federal nº. 13.079/2018**, "Lei Geral de Proteção de Dados Pessoais". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 14 mar. 2021

BRASIL. **Lei Federal nº. 12.965/2014**, "Marco Civil da Internet no Brasil". Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 14 mar. 2021

BRASIL. Supremo Tribunal Federal. **ADI 6387/2020**. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em 14 mar. 2021

BRASIL. Tribunal Regional do Trabalho. (2. Região). **Política de privacidade e segurança de dados do site**. Disponível em: https://ww2.trt2.jus.br/transparencia/politica-de-privacidade/portal/. Acesso em: 05 jul. 2020.

BRASIL. Tribunal de Justiça do Rio Grande do Sul. **Apelação Cível nº. (CNJ) 016447-98.2013.8.21.7000.** Disponível em: https://www.tjrs.jus.br/novo/busca/?return=proc&client=wp_index. Acesso em 14 mar. 2021

BUCHER, Taina. Imaginários e políticas dos algoritmos: entrevista com Taina Bucher. **DigiLabour**, Laboratório de Pesquisas. jun., 2020. Disponível em: https://digilabour.com.br/2020/07/12/imaginarios-e-politicas-dos-algoritmos-entrevista-com-taina-bucher/. Acesso em 15 jan. 2021.

CASTELLS, Manuel. **A Sociedade em rede**. Trad.: Roneide Majer. Rio de Janeiro: Paz e Terra, 2020.

COULDRY, Nick; HEPP, Andreas. **A construção mediada da realidade**. São Leopoldo: Ed. Unisinos, 2020.

CHRISTIAN, Brian; GRIFFITHS, Tom. **Algoritmos para viver. A ciência exata das decisões humanas**. São Paulo: Companhia das Letras, 2017.

GRAGNANI, Carla; VOLPINI, Sílvia. Escambo volta com a crise. São Paulo, **Estadão**. 2013. Disponível em: https://infograficos.estadao.com.br/focas-economicos-13/escambo.shtml#:~:text=Escambo%20volta%20com%20a%20crise&text=A%20internet%20revitalizou%20uma%20antiga,adeptos%20ao%20redor%20do%20mundo.&text=amparar%20outras%20empresas%20que%20sofriam%20com%20a%20crise. Acesso em 14 mar. 2021

GRASSEGGER, Hannes; KROGERUS, Mikael. The data that turned the world upside down. *In*: MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018.

GUGIK, Gabriel. O que são *cookies*? **Tecmundo**, 2008. Disponível em: https://www.tecmundo.com.br/web/1069-o-que-sao-cookies-.htm. Acesso: 04 jul. 2020.

HAN, Byung-Chul. **Sociedade da Transparência**. Tradução: Enio Paulo Giachini. Petrópolis: Editora Vozes, 2017.

HAN, Byung-Chul. **No enxame**. Perspectivas do digital. Tradução: Lucas Machado. Petrópolis: Editora Vozes, 2018.

HARARI, Yuval Noah. **21 lições para o século 21**. Trad.: Paulo Geiger. São Paulo: Companhia das letras, 2018.

KOPENAWA, Davi; ALBERT, Bruce. **A queda do céu**. Palavras de um xamã yanomami. São Paulo: Companhia das Letras, 2015.

LANEY, Douglas. **3D Data Management**: Controlling Data Volume, Velocity and Variety. Meta Group, 2001.

LEMOS, Ronaldo. Começa uma nova era para o tratamento de dados no Brasil. **Folha de São Paulo**, São Paulo, 12, jul., 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/07/comeca-uma-nova-era-para-o-tratamento-de-dados-no-brasil.shtml. Acesso em 14 mar. 2021

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LIPOVETSKY, Gilles; SERROY, Jean. **A estetização do mundo. Viver na era do capitalismo artista**. São Paulo: Companhia das Letras, 2015.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018.

MARCHANT, Alexander. **Do escambo à escravidão**. As relações econômicas de portugueses e índios na colonização do Brasil, 1500-1580. Tradução: Carlos Lacerda. Rio de Janeiro: Companhia Editora Nacional, 1943.

MARTINS, TG; SCHOR, P. **Desembalando a caixa preta**. São Paulo: Einstein, 2021.

Disponível em: https://www.scielo.br/pdf/eins/v19/pt_2317-6385-eins-19-eED6037.pdf. Acesso em 14 mar. 2021

MORAES, Alexandre de. **Direito constitucional**. 32. ed. São Paulo: Atlas, 2016.

MOROZOV, Evgeny. ***Big Tech***. A ascensão dos dados e a morte da política. Tradução: Claudio Marcondes. São Paulo: Ubu, 2018.

MOZILLA. MDN web docs. ***Cookies HTTP***. Disponível em: https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Cookies. Acesso em: 05 jul. 2020.

O'NEIL, Cathy. **Algoritmos de destruição em massa**. Como o Big Data aumenta a desigualdade e ameaça a democracia. Trad.: Rafael Abraham. Santo André: Editora Rua do Sabão, 2020.

SALESFORCE. **Desvendando os cookies**: uma receita para transformar a experiência on-line. Disponível em: https://www.salesforce.com/br/quarta-revolucao-industrial/o-que-sao-cookies/. Acesso em 05 jul. 2020.

SANTOS, Mario Filipe Cavalcanti de Souza. Por que não há mais escapatória: a vigência dos princípios norteadores da proteção de dados pessoais no Brasil e sua aplicação nas relações de consumo, bem como no tratamento desses dados. **Revista Jurídica da Seção Judiciária de Pernambuco**, Recife, v. 1, n. 13, p. 217-255, 2021.

SCHREIBER, Anderson. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. *In*: **Tratado de proteção de dados pessoais**. MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo W.; RODRIGUES JR., O. L. (org.) Rio de Janeiro: Forense, 2021.

SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity, 2017.

SUMPTER, David. **Dominados pelos números. Do Facebook e Google às fake News, os algoritmos que controlam nossa vida**. 1. ed. Rio de Janeiro: Bertrand Brasil, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara S. de. Consentimento e proteção de dados pessoais na LGPD. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (org.) **Lei geral de proteção de dados pessoais e suas repercussões no Direito brasileiro**. 2. ed. São Paulo: Revista dos Tribunais, 2020.

TIROLE, Jean. **Economia do bem comum**. São Paulo: Zahar, 2020.

VERRUMO, Marcel. O que são *cookies*? **Super Interessante**. Disponível em: https://super.abril.com.br/tecnologia/o-que-sao-cookies/#:~:text=Provavelmente%20nada.,pessoa%20de%20um%20determinado%20tipo%E2%80%9D.&text=E%20%C3%A9%20exatamente%20essa%20a,um%20pequeno%20arquivo%20de%20texto. Acesso em: 2 jul. 2020.

ZUBOFF, Shoshana. Big Other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology. *In*: BRUNO, Fernanda et al. (org.). **Tecnopolíticas da Vigilância. Perspectivas da margem**. São Paulo: Boitempo Editorial, 2018.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. A luta por um futuro humano na nova

fronteira do poder. Rio de Janeiro: Intrínseca, 2020.