ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
ANDRÉ FELIPE TANAKA

# Design do consentimento: o papel do design da experiência do usuário na proteção da privacidade na era digital

São Paulo
2019

ANDRÉ FELIPE TANAKA

# Design do consentimento: o papel do design da experiência do usuário na proteção da privacidade individual na era digital

Monografia apresentada ao
Programa de Educação Continuada
da Escola Politécnica da Universidade
de São Paulo como parte dos requisitos
para conclusão do curso
de MBA em Tecnologias Digitais e
Inovação Sustentável.

Orientador: Prof. Persival Ballesté

São Paulo
2019

## FICHA CATALOGRÁFICA

Tanaka, André Felipe

Design do consentimento: o papel do design da experiência do usuário na proteção da privacidade individual na era digital /

A. F. Tanaka -- São Paulo, 2019.

58 p.

Monografia (MBA em Tecnologias Digitais e Inovação Sustentável) - Escola Politécnica da Universidade de São Paulo. PECE – Programa de Educação Continuada em Engenharia.

1.UX Design 2.Design 3.Privacidade 4.Design do consentimento 5.LGPD I.Universidade de São Paulo. Escola Politécnica. PECE – Programa de Educação Continuada em Engenharia II.t.

*Dedico este trabalho ao Diego, meu companheiro de vida e de longas e inspiradoras conversas sobre absolutamente qualquer coisa.*

## AGRADECIMENTOS

Gostaria de agradecer imensamente à professora Tereza Carvalho pela visão e dedicação postas neste curso tão diverso e inspirador, onde houve desde o princípio grande abertura para diálogo, mudanças e melhorias, incentivando a construção de ótimas - e necessárias - pontes entre a academia e o mercado e permeando temas tão complexos e atuais. Meus sinceros agradecimentos ao meu orientador, professor Persival Ballesté, primeiramente por sua paciência e principalmente pelas inspiradoras aulas e conversas, tão conectadas e empáticas com os problemas da vida real. Um agradecimento especial à colega Laura Varisco, que conheci breve e recentemente por um acaso profissional mas que me auxiliou imensamente por meio de sua brilhante pesquisa de doutorado, estando sempre disposta a ajudar com uma solicitude ímpar. Agradeço também às minhas colegas de classe Caroline Pilon e Isabela Padovan pela amizade, parceria e bom humor ao longo deste curso. Por fim, porém não menos importante, agradeço à minha mãe, Marli, pelo apoio de uma vida toda e por ter me ensinado, sendo professora, sobre o valor da cultura e da educação e ao meu pai, Edson, pelo constante incentivo para que eu mantivesse uma mente curiosa e por ter me apresentado à ficção científica, em especial à obra de Isaac Asimov, que anteviu há décadas muitas das questões que são centrais a este trabalho.

## RESUMO

Na última década assistimos ao crescimento e estabelecimento de modelos de negócios baseados em dados, nos quais por meio de tecnologias como IoT *(Internet of Things)*, computação cognitiva, *machine learning* e inteligência artificial, empresas passaram a coletar uma quantidade imensa de dados sobre seus usuários. Neste cenário onde a coleta e o processamento de dados são ubíquos, a defesa da privacidade e dos dados pessoais do indivíduo recai principalmente sobre o sistema legal, mas a redação de leis como a Lei Geral de Proteção de Dados Pessoais (LGPD) não é suficiente para garantir aos usuários uma experiência de real transparência, uma vez que as tecnologias que processam esses dados tornam-se cada dia mais complexas e abstratas para os usuários em geral. Este trabalho tem como objetivo explorar por que e como o campo do design de experiência de usuário (*UX Design*) deve ser parte integrante do projeto de soluções que façam coleta e processamento de dados pessoais, focando-se especificamente na etapa de consentimento do usuário. Por meio de revisão bibliográfica foi feita uma análise contextual que explora a complexidade dos cruzamentos entre temas como modelos de negócios digitais, sistema econômico, legislação, privacidade e *UX Design*. Com base nesta análise, foram mapeadas oportunidades e possíveis direções de *UX Design* onde a defesa da privacidade gere valor tanto para o usuário quanto para o negócio. O pressuposto legal de que o usuário deve ter direito a uma autogestão de sua privacidade ao consentir ou não a coleta e o processamento de dados pessoais deve ser complementado com um design de experiência que lhe forneça informações de qualidade para esta tomada de decisão, colaborando assim com a criação de modelos de negócio digitais que adotem práticas sustentáveis no que se refere à gestão da privacidade individual.



**Palavras-chave:** UX Design; Design de experiência do Usuário; Privacidade; Dados Pessoais; LGPD; Capitalismo de vigilância; Dataveillance; Consentimento; Dilema do Consentimento; Design centrado no usuário; Privacy by design.

## ABSTRACT

Over the last decade we have witnessed the growth and establishment of data-driven business models in which, using technologies such as IoT, cognitive computing, machine learning and artificial intelligence, companies started collecting an immense amount of data from their users. In this scenario where data collection and processing are ubiquitous, the defense of individual's privacy and personal data relies mostly on the legal system, but the development of laws such as the LGPD (Brazilian equivalent to the EU's GDPR) is not enough to ensure users will have an experience of real transparency, especially considering the fact that the technologies that process these data are becoming increasingly complex and abstract for the average users. This monograph aims to explore why and how the field of user experience design (UX Design) should be an integral part when designing solutions that collect and process personal, focusing specifically on the stage of the user consent. Through a literature review, a contextual analysis was made exploring the complexity of intersections between themes such as digital business models, economic system, legislation, privacy and UX Design. Based on this analysis, opportunities and possible directions of UX Design were mapped in a way that safeguarding the user privacy generates value for both the user and the business itself. The legal assumption that the users should be entitled to self-management of their privacy when they consent or not with the collection and processing of personal data should be complemented by an experience design that provides quality information for their decision making, thus collaborating with the creation of digital business models that adopt sustainable practices regarding the management of individual privacy.



**Keywords:** UX Design; User experience design; Privacy; Personal Data; LGPD; Surveillance Capitalism; Dataveillance; Consent; Consent Dilemma; User centered design; Privacy by design.

## LISTA DE ILUSTRAÇÕES

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| 4G | Rede de internet móvel de quarta geração |
| GDPR | General Data Protection Regulation |
| LGPD | Lei Geral de Proteção de Dados Pessoais |
| IoT | Internet of Things |
| UX | User Experience (experiência do usuário) |

**SUMÁRIO**

# 1. Introdução

O tema da privacidade na era digital é bastante vasto e complexo pois ele é, na realidade, uma intersecção de outros temas que envolvem diversas áreas do conhecimento: discussões sobre privacidade e transformação digital são permeadas por aspectos sociais, técnicos, legais, históricos, entre outros. Este trabalho se trata de uma análise feita sob o ponto de vista do design, buscando entender como esses contextos que permeiam o tema da privacidade influenciam e são influenciados pelo design da experiência do usuário (*UX Design*).

O *UX Design* é uma área do conhecimento que analisa, planeja e projeta a jornada dos usuários ao utilizarem determinado produto ou serviço. Isto requer dos profissionais desta área uma visão holística daquilo que projetam, buscando entendimento dos diversos contextos e agentes que participam dessa jornada. Por tal motivo, ao tratar da privacidade na era digital sob um olhar do *UX Design,* este trabalho torna-se essencialmente multidisciplinar: ele é sobre *UX Design* porém para sê-lo, passa a explorar contextos externos ao *UX Design*.

## 1.1. Motivação, justificativa e objetivo

A documentalização de nossa própria existência é uma característica humana que ao longo do tempo passou por diversas técnicas: sejam comunidades nômades produzindo desenhos rupestres do período Neolítico, sejam adolescentes compartilhando *selfies* em redes sociais, historicamente o ser humano gera e armazena - de forma ativa ou passiva - dados sobre sua própria existência. Este ato, segundo Ferraris (2013), sempre esteve presente no comportamento humano e refere-se tanto a uma questão de registro de memória quanto da própria definição de identidade do indivíduo e da sociedade.

Tal comportamento humano, contudo, alterou-se e adequou-se às técnicas disponíveis em cada tempo histórico. A perenidade e a quantidade de registros históricos gerados tanto da micro quanto da macro-história se transformaram ao longo das décadas, passando por escribas e monges copistas, evoluindo para a imprensa com tipos móveis de Gutenberg, fotografia analógica, vídeo analógico, dados em cartões perfurados, discos rígidos, fotografia e vídeo digitais, dados armazenados em nuvem, etc.

Hoje, com a popularização da internet, dos aparelhos celulares inteligentes (*smartphones*) e dos serviços digitais atrelados a eles, geramos mais dados sobre nós mesmos do que nunca. De acordo com pesquisa publicada pela empresa DOMO, em 2017 eram gerados todos os dias 2,5 quintilhões de bytes. A mesma pesquisa indica que 90% de todos os dados digitais gerados pela humanidade até 2017 foram produzidos num período de apenas dois anos, entre 2015 e 2017.

Vivemos hoje em um contexto social e tecnológico antevisto por estudos feitos desde os anos 80, que apontavam para um futuro onde fariam parte de nosso cotidiano as tecnologias de computação ubíqua e pervasiva (NIEUWDORP, 2007). Os computadores tornaram-se de certa forma invisíveis para os usuários e a coleta e o processamento de dados passaram a acontecer o tempo todo durante o cotidiano dos indivíduos (WEISER et al., 1999).

Mas neste contexto de constante coleta de dados sobre os indivíduos, aumentam de forma significativa as preocupações referentes ao direito à privacidade. Apesar de a sociedade ter aderido massivamente a serviços digitais e redes sociais de forma a ceder dados pessoais constantemente a estas plataformas, ainda não foram desenvolvidas soluções ou diretrizes que esclareçam para os usuários de forma clara, adequada e tangível o que de fato pode ser feito com estas informações pelos controladores de tais serviços e produtos digitais (YOUNG, 2012).

De forma reativa a casos emblemáticos de violações de privacidade ou vazamentos de dados pessoais cometidos por grandes empresas de tecnologia, como por exemplo o caso da Cambridge Analytica junto do Facebook (ISAAK et al., 2018), surgiram nos últimos anos diferentes decretos, acordos e leis que visam regular o uso de dados pessoais, como por exemplo na União Europeia a GDPR (*General Data Protection Regulation*) e no Brasil a LGPD (Lei Geral de Proteção de Dados Pessoais). Ambas regulamentações definem, entre outras questões, que para toda coleta e processamento de dados pessoais é necessário que a empresa ou serviço em questão solicite o consentimento do usuário, ou seja, é necessário que de alguma forma o usuário seja informado do motivo e da forma que seus dados serão coletados e processados e então autorize tal atividade.

Porém a forma como se dá esse processo de requisição de consentimento do usuário não é definida em detalhes pelas leis e, nesta indefinição, surge a questão

que é objeto principal deste estudo: qual a contribuição que pode e deve ser feita pela disciplina do Design da Experiência do Usuário (*UX Design*) para projetar o processo de consentimento do usuário à coleta e processamento de seus dados pessoais?

Existe hoje uma grande assimetria entre o entendimento do usuário sobre o que acontece com seus dados pessoais uma vez coletados pelas empresas e os potenciais usos mercadológicos destes dados. Por meio de avançadas tecnologias, que nem sempre são transparentes ou compreensíveis para os usuários, empresas coletam, processam e cruzam dados de forma a adquirirem um profundo conhecimento sobre o comportamento de cada indivíduo, fato que não é sequer imaginado pelo usuário no momento em que ele consente ter seus dados coletados para poder utilizar determinado produto ou serviço (ZUBOFF, 2019).

Esta assimetria torna-se especialmente notável na forma com a qual muitos sistemas solicitam o consentimento do usuário: normalmente é algo que ocorre no momento em que o usuário está fazendo seu primeiro uso do sistema/serviço, ou seja, um momento em que o usuário está em um estado mental de ansiedade para desfrutar dos benefícios oferecidos. Ali é então apresentada uma interface com um longo texto, escrito em termos bastante técnicos e, abaixo dele, há um botão que diz “Eu concordo” ou algo com o mesmo sentido. Em algumas variações deste formato de consentimento os serviços digitais nem mesmo apresentam de pronto os termos com os quais o usuário supostamente irá concordar: deixam apenas um *hyperlink* sutil que, caso o usuário decida ativamente clicar, ele será levado para uma outra página onde está o texto com os termos de privacidade e uso.

**Figura 1 - Detalhe da interface de requisição de consentimento do Facebook**


*fonte: Facebook*

Este tipo de interface de requisição de consentimento vai contra os conceitos do design centrado no usuário. Conforme defende Donald Norman (2006) em seu livro “O design do dia-a-dia”, “o sistema deve oferecer ações que correspondam às intenções [...]. O estado do sistema deve ser visível e prontamente interpretável, evidenciando os resultados de uma ação”. Os resultados da ação do usuário consentir aos termos referentes à captura e ao processamento de seus dados pessoais frequentemente não são evidenciados por estas plataformas digitais.

Neste trabalho será explorada a lacuna que existe entre o consentimento do usuário e seu real entendimento dos impactos deste consentimento para sua privacidade, propondo-se uma uma exploração sobre como os conceitos do design centrado no usuário podem ser aplicáveis a este contexto de defesa da privacidade. A este processo de aplicação dos conceitos de design centrado no usuário e UX

design às etapas de solicitação de consentimento do usuário para coleta de seus dados pessoais em plataformas digitais será dado nome de “design do consentimento”.

O objetivo deste trabalho é, primeiramente, analisar do ponto de vista do usuário alguns dos possíveis impactos da coleta e processamento de dados pessoais, contextualizando estes impactos com a atual situação da legislação brasileira. Com base nesta análise, o objetivo seguinte deste trabalho é apontar possíveis direções conceituais de aplicação dos conceitos do design centrado no usuário para tornar mais transparente e eficiente a autogestão da privacidade que hoje é imposta aos usuários. Ao cruzar as direções apresentadas por Solove (2012) para reduzir os impactos negativos do chamado "Dilema do Consentimento" com os princípios do design centrado no usuário apresentados por Norman (2006), espera-se com este trabalho gerar insumos para projetos de *UX Design* que não apenas estejam de acordo com as leis e regulamentações de privacidade, mas também gerem valor para os negócios e para o usuário final.

### 1.2. Metodologia

O principal método utilizado neste trabalho é a revisão de literatura, que foi organizada em três grupos de conhecimento, sendo:

- Tecnologia e sociedade: Computação ubíqua, modelos de negócio digitais e Capitalismo de Vigilância;
- Legal: Privacidade, dados pessoais e a legislação brasileira;
- Design: design centrado no usuário e design de experiência.

Enquanto a revisão bibliográfica dos dois primeiros grupos tem como objetivo o estabelecimento do contexto atual da privacidade e da requisição do consentimento sob o ponto de vista tecnológico, legal e social, a exploração do terceiro tema tem objetivo de buscar diretrizes para futuras propostas, ou seja, analisar as oportunidades e desafios no contexto apresentado sob a perspectiva da disciplina do design centrado no usuário.

### 1.3. Organização do trabalho

Este trabalho está dividido em duas partes. A primeira, contida na seção “2. Análise contextual: Computação Ubíqua e privacidade” trata-se de um tutorial com intuito de fornecer contextualização para o recorte social e tecnológico que foi analisado. Nela são apresentadas e analisadas definições de termos legais e técnicos que foram insumos para a problematização de como o *UX Design*, se mal conduzido, pode ser um elemento que distancia os usuários de um entendimento real dos riscos e consequências de fornecer dados pessoais a plataformas digitais.

Na segunda parte, “3. Design do Consentimento”, são apresentados os motivos pelos quais a disciplina de *UX Design* demonstra-se tão importante quanto as leis (como a LGPD) no que se refere à defesa da privacidade e de dados pessoais. Nessa seção buscou-se analisar como conceitos do design centrado no usuário podem ser aplicados a questões específicas referentes ao processo de requisição de coleta de consentimento de usuários para coleta e processamento de dados.

### 1.4. Contribuições esperadas

Espera-se por meio deste trabalho contribuir com a elaboração futura de diretrizes e boas práticas na defesa da privacidade dos indivíduos frente à coleta e ao processamento de dados pessoais no Brasil. No momento da publicação desta monografia, a lei federal brasileira nº 13.709/2018, publicada no Diário Oficial da União em agosto de 2018, ainda estará em período de *vacatio legis* de 24 meses. Desta forma, caso não seja alterada, a partir de agosto de 2020 a Lei Geral de Proteção de Dados Pessoais (LGPD) estará vigente no Brasil e terá significativos impactos em todos serviços e plataformas digitais que trabalham com dados pessoais no território brasileiro.

Com este trabalho, espera-se contribuir positivamente nas discussões que serão fomentadas a partir da vigência desta lei para que as preocupações de empresas e plataformas digitais brasileiras não fiquem restritas ao cumprimento da lei por si só, mas também explorem as possibilidades de geração de valor para o usuário por meio de transparência e ética nestas operações, desenvolvendo um processo de requisição de consentimento do usuário que atenda às boas práticas das disciplinas do design centrado no usuário e do *UX design*.

## 2. Análise contextual: Computação Ubíqua e privacidade

A discussão sobre o design do consentimento e a gestão da privacidade individual proposta neste trabalho foi feita com base em um contexto tecnológico e socioeconômico específico de sociedades vivendo na era da informação digital. Esta seção tem como objetivo aprofundar este contexto, a fim de explorar alguns dos motivos pelos quais a gestão da privacidade se tornou uma questão socialmente relevante de forma interdisciplinar.

Nas quatro seções a seguir serão explorados: o contexto de modelos de negócios digitais e como eles fomentaram um aumento de captura de dados com auxílio da computação ubíqua; o contexto socioeconômico de como a expansão dos modelos de negócios digitais impactaram o modelo econômico de forma a colocar em risco a privacidade e o próprio comportamento humano; o contexto legal de como a lei brasileira se resguarda repetidamente no conceito de consentimento para a gestão da privacidade e, por fim, o contexto do design da experiência do usuário (*UX design*) e como ele pode ser (e é) utilizado de forma antiética para manipular negativamente usuários de serviços digitais no entendimento das políticas de privacidade.

### 2.1. Modelos de negócios digitais e a coleta de dados pessoais

Houve uma época, em um passado não muito distante, em que imaginava-se um futuro utópico no qual sensores, computadores e o processamento de dados aconteceriam no cotidiano dos indivíduos sem que eles sequer percebessem ou precisassem fazer esforço, pois as tecnologias e sensores estariam completamente integrados ao dia-a-dia da sociedade. A este tipo de integração tecnológica na sociedade foi então dado o nome de computação ubíqua. “A computação ubíqua criou um novo ramo da ciência da computação, um ramo em que se especulava sobre um mundo físico rico e invisivelmente entrelaçado com sensores, atuadores, telas e elementos computacionais integrados perfeitamente em objetos do cotidiano de nossas vidas e conectados por meio de redes constantes” (WEISER, 1999, tradução nossa).

Em muitos aspectos pode-se considerar que esta visão de futuro de Weiser se concretizou por meio da popularização da internet, da internet das coisas (IoT), dos

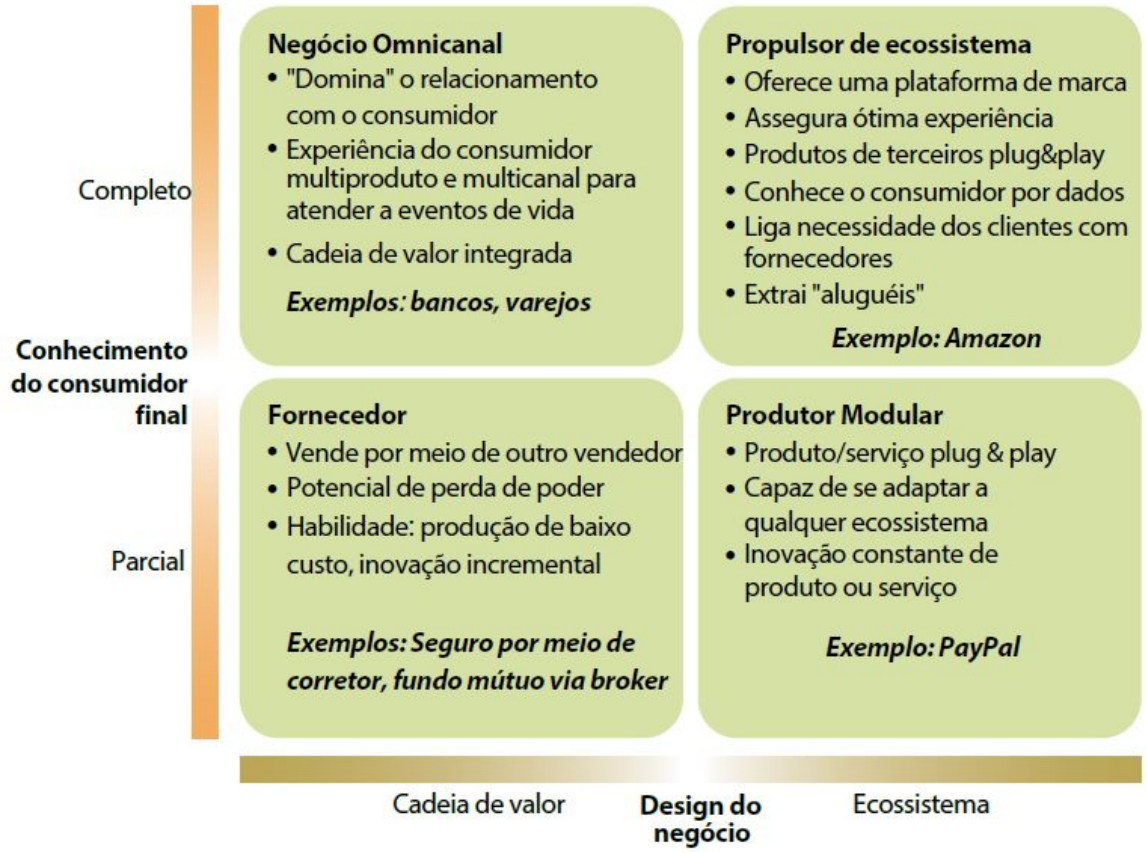
aparelhos *smartphones* e de algoritmos de inteligência artificial baseados em *big data*. A digitalização de empresas e serviços e a utilização de análise de *big data* transformaram modelos de negócio tanto no que se refere a processos internos quanto em seu relacionamento com os consumidores. Quanto a processos internos, a digitalização proporcionou melhorias de eficiência. “Melhorias incrementais de modelos de negócios estabelecidos baseadas em análise de *big data* têm como objetivo otimizar processos existentes e aumentar como um todo a eficiência e a qualidade de produtos e serviços. Aumentar a digitalização reduz dramaticamente os custos transacionais para coletar informações, se comunicar e controlar dispositivos” (LOEBBECKE et al., 2015, tradução nossa).

Já no que se refere ao relacionamento com os consumidores, a digitalização transformou a percepção dos usuários sobre o valor da conveniência de ter produtos e serviços customizados e adaptados aos seus hábitos e rotinas. O cotidiano dos indivíduos passou a ser permeado pelo uso frequente, por exemplo, de plataformas de múltiplos serviços como o Google, redes sociais como o Twitter, Facebook e Instagram, plataformas de comércio eletrônico como a Amazon, serviços digitalizados como Uber, iFood, Netflix, Spotify, etc.

Serviços como estes citados acima têm modelos de negócio extremamente baseados em dados, ou seja, além de oferecerem algum valor central ao consumidor (um sistema de buscas, uma plataforma de vendas online, uma plataforma de transporte compartilhado, uma plataforma de vídeos, etc.), eles oferecem também conveniência ao personalizar o que é oferecido a cada um de seus usuários com base em seus hábitos, individualizando assim o relacionamento das marcas com os consumidores.

Ao executar este processo de coleta e processamento de dados de seus consumidores (*big data analytics*) para conhecê-los melhor, estes serviços têm como objetivo adotar modelos de negócios digitais que, de acordo com o diagrama (Figura 2) apresentado por Peter Weill (2015), se encontram nos dois quadrantes superiores, ou seja, modelos de negócio que buscam se diferenciar do restante por terem domínio do relacionamento com seus clientes. Tal domínio provém do conhecimento profundo e individualizados de seus usuários, graças aos dados fornecido por eles.

**Figura 2 - Modelos de negócios na era digital**




*fonte: Adaptado de WEILL et al., 2015, tradução nossa*

Este movimento de busca por geração de valor a partir de dados fornecidos pelos clientes foi seguido por diversas empresas dos mais diversos segmentos de mercado. Em suas análises Weill indicava, inclusive, que empresas que desejassem sobreviver à era digital deveriam justamente “utilizar suas capacidades digitais para obter informações sobre os objetivos do consumidor e seus momentos de vida” (WEILL, 2015, tradução nossa).

De acordo com Weill, quando uma empresa consegue extrair conhecimento sobre o cliente a partir de determinados dados comportamentais capturados e, com base nesse conhecimento, oferece algo único e personalizado para aquele cliente específico, tem-se aí um “momento da verdade”, ou seja: uma experiência da qual o usuário sempre se lembrará e falará sobre no futuro.

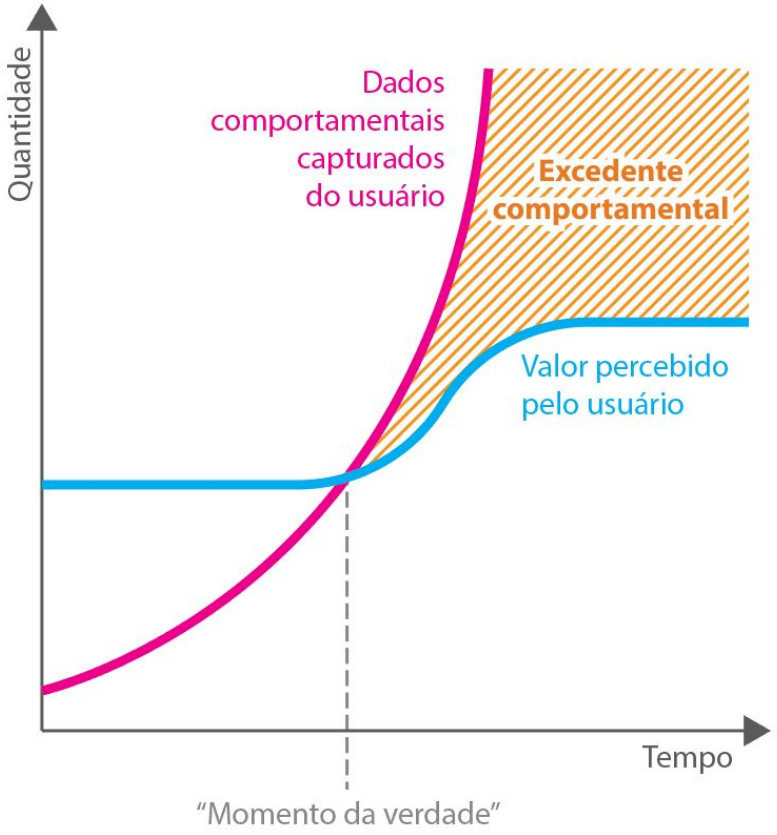
Porém houve uma rápida mudança na forma e na quantidade que tais dados comportamentais dos usuários passaram a ser capturados. O acelerado desenvolvimento das tecnologias de análise de dados combinado ao massivo

aumento da prevalência de *smartphones* fez com que rapidamente os usuários, seduzidos pelos benefícios da conveniência e da personalização dos serviços, se distanciassem do entendimento de quando eles estavam cedendo dados pessoais às empresas e de como estes dados poderiam ser utilizados por elas. “A presença pervasiva de tais tecnologias encoraja o uso ubíquo e incorporado de produtos digitais, reduzindo o esforço cognitivo de algumas tarefas e processos e aumentando a troca intencional e não intencional de dados pessoais por meio da internet” (VARISCO, 2019, tradução nossa).

Ou seja, ao mesmo tempo em que houve uma movimentação dos negócios em direção à coleta de informações sobre o comportamento de seus clientes - caminho este apontado por Weill como necessário para a sobrevivência de negócios digitais - houve, em paralelo, uma aceleração no desenvolvimento das tecnologias de captura e processamento de dados de forma ubíqua e pervasiva. Esta aceleração fez com que ocorresse uma rápida mudança de contexto: passou-se de um cenário onde dados eram utilizados principalmente para melhoria de eficiência e customização de produtos e serviços para um novo cenário onde a quantidade de dados capturados passou a ser muito maior do que a necessária para aplicação estrita em melhorias de produtos ou serviços. Os negócios digitais passaram a ter acesso a um excedente de dados capturados e processados que permitiu que alguns algumas empresas adquirissem mais conhecimento sobre o comportamento de seus clientes do que esses indivíduos tinham ciência.

O conhecimento que determinadas empresas adquirem sobre o comportamento dos usuários obtido a partir destes dados capturados para além da compreensão e percepção do indivíduo foi definido como “Excedente Comportamental” (tradução livre de “*behavioral surplus*”) pela pesquisadora Shoshana Zuboff. Segundo ela, o capitalismo como um todo se transformou e hoje temos um sistema econômico permeado por modelos de negócios que reivindicam a experiência humana como matéria prima para geração de dados comportamentais (ZUBOFF, 2019).

**Figura 3 - Gráfico esquemático para ilustração da percepção de valor pelo usuário a partir de dados comportamentais capturados e processados por uma empresa/serviço**




*fonte: o autor*

Levando-se em conta os conceitos de "Momento da verdade" de Peter Weill e de "Excedente Comportamental" de Shoshana Zuboff, é possível observar na Figura 3 que o "Momento da verdade" é um importante ponto de inflexão para o entendimento do que é o "Excedente comportamental". Enquanto uma empresa captura dados do usuário porém não consegue aplicá-los de forma efetiva para melhorar seu serviço ou produto central, os dados capturados não afetam o valor percebido pelo usuário. Quando acontece o "Momento da verdade", ou seja, quando a empresa é capaz de usar os dados obtidos para gerar conhecimento sobre o comportamento do usuário e oferecer uma experiência melhor e mais customizada, a percepção de valor do usuário é afetada positivamente. Porém quando a empresa, após ter chegado ao ponto em que foi capaz de criar "Momentos da verdade", continua a expandir as formas, a quantidade e a variedade de dados capturados do

usuário sem aplicá-los a novos geradores de valor, ou seja, quando ela expande seu conhecimento sobre o usuário mas não gera novos benefícios tangíveis para ele, tem-se então um conhecimento excedente que Zuboff define como “excedente comportamental”.

Segundo Zuboff, o “excedente comportamental” se tornou uma matéria prima que é negociada entre diferentes agentes no atual modelo de capitalismo. A experiência humana capturada em forma de dados comportamentais permite que as empresas façam leituras e predições de como indivíduos se comportarão em determinadas circunstâncias. Tal informação se tornou algo extremamente valioso e facilmente transacionável nos modelos de negócios digitais vigentes.

Para ter acesso e dar uso comercial a estes dados comportamentais, as empresas requisitam o consentimento do usuário para fazer a captura e processamento de dados pessoais, contudo a capacidade do usuário de compreender a extensão e as implicações deste consentimento acaba sendo ofuscada pela expectativa dos benefícios percebidos nos “Momentos da verdade”.

A este sistema econômico que comercializa dados comportamentais muitas vezes contando com a assimetria de conhecimento existente entre o agente que captura os dados do usuário e o usuário em si, Zuboff deu o nome de “Capitalismo de Vigilância”.

## 2.2. Capitalismo de Vigilância

Laura Varisco (2019) em sua tese "*Personal Interaction Design*" ("O design da interação pessoal", em tradução livre), expõe que com a concretização da computação pervasiva como se vê hoje, por meio da internet, *smartphones* e serviços digitais diversos, a tecnologia em si passou a ser percebida como um elemento não neutro nas interações sociais, pois uma vez que uma tecnologia é incorporada à sociedade de forma tão inseparável, é criado um novo sistema sócio-técnico que molda e redefine as dinâmicas sociais (VARISCO, 2019).

No livro "*The age of surveillance capitalism*" ("A era do Capitalismo de Vigilância", em tradução livre), Shoshana Zuboff explora tal redefinição das dinâmicas sociais sob um ponto de vista econômico, observando que a captura de dados comportamentais dos indivíduos se tornou um processo mercadológico.

> "O Capitalismo de Vigilância reivindica unilateralmente a experiência humana como matéria prima para transformá-la em dados comportamentais. Apesar de uma parte desses dados ser aplicada à melhoria de serviços, todo o restante é apropriado como excedente comportamental que é usado como insumo para avançados processos conhecidos como '*machine intelligence*', que fabricam produtos de predição que, por sua vez, podem prever o que você fará agora, em breve ou no futuro. Finalmente, estes produtos de predição são negociados em um novo tipo de mercado que eu chamo de mercado dos comportamentos futuros". (ZUBOFF, 2019, tradução nossa)

Conforme explorado na seção anterior, a prevalência de *smartphones* e serviços digitais incorporados ao cotidiano permitiu que modelos de negócios digitais passassem a coletar dados dos usuários para extrair conhecimento sobre a vida e o comportamento deles. Esta prática de coleta e uso dos dados dos indivíduos é conhecida como "*self-tracking*" (LUPTON, 2016; VARISCO 2019).

O *self-tracking* ("rastreio de indivíduos", em tradução livre) é algo que pode acontecer de diversas maneiras. Lupton (2016) mapeou cinco modalidades[1] de *self-tracking*, que vão desde processos conscientes de rastreamento, onde o sujeito ativamente decide ceder e monitorar determinados parâmetros sobre si mesmo, até processos de *self-tracking* que podem ser impositivos ou mesmo imperceptíveis para

[1] Para mais detalhes sobre as modalidades de self-tracking, se referir ao estudo de Lupton "*The diverse domains of quantified selves*".

o sujeito. A combinação desses modos de *self-tracking* aliada às possibilidades comerciais de como tais informações podem ser ressignificadas é algo que, para Lupton, levanta importantes questões sobre a defesa da privacidade e do próprio conceito de cidadania (LUPTON, 2016).

Esta percepção é endossada por Nora Young em seu livro "*The Virtual Self*", onde a autora explora como, em troca de determinados prazeres e benefícios, os indivíduos passaram a indiscriminadamente e de forma desatenta ceder seus dados pessoais no contexto da vida digital:

> "Este fenômeno de reportarmos nossos próprios dados digitalmente vem associado a questões bastante reais e preocupantes sobre privacidade. Apesar de nos investirmos nesta volumosa documentação de nossas vidas, nós ainda não discutimos adequadamente o que pode ser feito com estas informações, com quem ou como ela pode ser compartilhada, ou como poderíamos anonimizá-las para proteger informações pessoais". (YOUNG, 2012, tradução nossa)

Esta aparente ingenuidade (ou mesmo ignorância) dos usuários com relação ao que pode ser feito com seus dados pessoais não deve, contudo, ser atribuída exclusivamente ao usuário. Uma vez que há interesse econômico de novos modelos de negócios em comercializar dados comportamentais, Zuboff aponta que também há interesse em preservar uma assimetria de conhecimento entre o que o negócio faz e sabe sobre o usuário em comparação ao que o usuário entende que o negócio pode fazer a partir de seus dados pessoais.

> "O Capitalismo de Vigilância domina uma divisão anormal do aprendizado, na qual é sabido por ele coisas que não é possível que saibamos [...]. É impossível entender algo que foi desenvolvido em segredo e projetado para ser fundamentalmente ilegível [para o usuário]". (ZUBOFF, 2019, tradução nossa)

Quando o usuário concorda em ceder seus dados pessoais a algum serviço ou produto específico, ele tem clareza de qual seu objetivo final naquele processo, ele está em um momento de antecipação e ansiedade por receber algum benefício específico gerado por aquele serviço. Portanto com relação ao benefício

normalmente não há falta de clareza, a assimetria de conhecimento se dá especificamente com relação aos “custos” que podem ser gerados ao usuário após ele concordar com as políticas e termos para poder usufruir de tal benefício.

Zuboff faz um paralelo com a era industrial, iniciada em meados do século XVIII, quando o desenvolvimento da civilização veio com um grande custo ambiental ao consumir de forma irresponsável alguns recursos naturais. Os benefícios da industrialização eram bastante fáceis de compreender para a classe trabalhadora, que passou a ter poder de consumo para adquirir bens industrializados. Porém os custos ambientais não apenas não eram claros ou compreendidos na época, como levou-se décadas para que fossem mensurados ou reconhecidos. Hoje, “uma civilização da informação moldada pelo Capitalismo de Vigilância e seu novo poder ferramental e tecnológico irá prosperar a custo da natureza humana, ameaçando custar nossa própria humanidade” (ZUBOFF, 2019, tradução nossa).

Outro paralelo que pode ser traçado entre esses dois momentos históricos é referente a como grandes desastres ou eventos de grandes proporções que chegam a conhecimento público influenciam e impulsionam discussões sobre as questões relacionadas a eles. Em 1952, por exemplo, houve o episódio em Londres do Grande Nevoeiro, durante o qual por cinco dias a cidade foi coberta por uma névoa de poluição gerada principalmente pela queima de carvão nas fábricas da região, causando milhares de mortes (LASKIN, 2006).

O grande impacto na opinião pública causado por este desastre mudou a forma como a poluição do ar era percebida, de forma que o governo britânico teve que agir e em 1956 foi publicada a primeira legislação do mundo a tratar especificamente de poluição do ar, o *Clean Air Act*.

Se considerarmos o contexto da era da informação e do Capitalismo de Vigilância, eventos relacionados a grandes vazamento de dados pessoais de usuários tiveram impacto e consequências semelhantes, como por exemplo o caso da Cambridge Analytica com o vazamento de dados pessoais de milhões de usuários do Facebook (ISAAK et al., 2018) ou o caso das revelações de Edward Snowden sobre sistemas de vigilância criados pela agência americana NSA (LANDAU, 2013).

Ao vir a conhecimento público, estes e outros casos de vazamentos de dados pessoais e, principalmente, os supostos usos feitos da extração de dados comportamentais para posteriores predições ou mesmo influenciamento de comportamentos[2] começaram a trazer atenção pública à assimetria de conhecimento existente entre os agentes do Capitalismo de Vigilância e os usuários.

Há hoje uma maior preocupação na sociedade com relação à vigilância sobre seus dados ("*dataveillance*"). A privacidade começa a ganhar maior protagonismo no sentido de esperar-se que as soluções tecnológicas sejam projetadas de forma a "criar conhecimento sobre diferentes impactos nas pessoas, na sociedade, na política e na justiça comercial, evitando problemas e percepções incorretas" (VARISCO, 2019, tradução nossa).

Mas se por um lado estes casos de vazamentos de dados e a subsequente discussão pública sobre eles começaram a reduzir a lacuna de conhecimento entre o que pode ser feito com dados pessoais capturados por modelos de negócios digitais e o que de fato os usuários entendem sobre isso, por outro lado a acelerada velocidade com a qual se desenvolvem as tecnologias envolvidas no contexto de computação ubíqua e pervasiva que temos hoje dificultam que tal assimetria de conhecimento se reduza de forma eficaz.

Da mesma forma que alguns anos após o Grande Nevoeiro em Londres houve a publicação do *Clean Air Act*, casos de vazamento ou mau uso de dados pessoais também geraram reações em forma de regulamentações, como em 2016 na União Europeia o GDPR (*General Data Privacy Regulation*) e em 2018 no Brasil a LGPD (Lei Geral de Proteção de Dados Pessoais). Tais leis, assim como o *Clean Air Act* estava diretamente relacionado ao momento econômico na então era industrial inglesa, estão intrinsecamente ligadas ao momento socioeconômico atual e ao Capitalismo de Vigilância. Elas têm como um de seus objetivos definir normas para tentar impedir práticas mercadológicas abusivas com relação à captura e uso de dados pessoais.

---

[2] A ideia de que por meio de análise de dados comportamentais e psicográficos seja possível influenciar o comportamento de indivíduos ou grupos é questionada, contudo uma publicação recente de Sandra Matz e Michal Kokinski - que fez parte do time de pesquisa da Universidade de Cambridge em 2013 - indica que é possível ter impacto significativo em comportamentos ao utilizar-se o direcionamento de mensagens com base em perfis psicográficos (MATZ et al., 2017).

## 2.3. Legislação brasileira, privacidade e consentimento

Quando se trata da defesa da privacidade de indivíduos e da sociedade frente a novos contextos tecnológicos ou paradigmas socioeconômicos, leis como a GDPR e a LGPD não são casos isolados e há diversos precedentes no passado.

Historicamente as transformações tecnológicas mudam a forma como os indivíduos e a sociedade lidam com o conceito de privacidade: a cada nova tecnologia desenvolvida, novos desafios referentes à proteção da privacidade e dos direitos de imagem se impõem. E quanto maior a velocidade de reprodutibilidade das mídias, mais complexos se tornam os desafios. De forma reativa a mudanças de paradigmas tecnológicos e de interações sociais, ao longo do tempo a sociedade identificou diferentes necessidades do desenvolvimento de regulamentações para proteger sua privacidade de alguma forma. Isto pode ser traçado de volta a tecnologias como, por exemplo a fotografia.

> “Com o advento da fotografia e, portanto, da reprodutibilidade da imagem de forma mais ampla, foi conferida ao Homem a faculdade de registrar de forma fidedigna a fisionomia, a cultura, os costumes e os momentos históricos [...]. A consequência desse importante avanço técnico é a exploração indevida da imagem alheia. Nesse sentido, conforme a propagação da imagem pessoal se alastrava, as sociedades sentiram a necessidade de tutelar a proteção à imagem, já que o coletivo passou a interferir na esfera privada dos indivíduos”. (CASAL, 2016)

Quando se trata de sua própria imagem, como no exemplo citado acima, é tangível para o indivíduo identificar quando há alguma interferência do coletivo em sua esfera privada, pois a averiguação do uso indevido deste dado é de fácil apreensão. Porém o complexo contexto tecnológico em que vivemos hoje torna a percepção do uso indevido de dados pessoais muito mais subjetiva. A forma como geramos e compartilhamos quaisquer tipos de dados sobre nós mesmos se transformou em grande escala com o advento de tecnologias digitais.

Nesta seção serão analisadas algumas leis brasileiras que foram redigidas desde a redemocratização em 1988 e que têm impacto na forma como empresas, serviços, produtos e plataformas digitais podem capturar e fazer uso de dados pessoais dos indivíduos, interferindo portanto em sua privacidade.

Antes da redação e publicação da lei 13.709/2018 (vulgo a LGPD), que trata especificamente sobre a proteção de dados pessoais e que foi redigida dentro do paradigma de uma sociedade conectada pela internet, já existiam na legislação brasileira questões referentes à defesa do direito à privacidade do indivíduo.

Na Constituição da República Federativa do Brasil de 1988 e ainda vigente, no artigo 5º referente aos direitos e deveres individuais e coletivos consta:

> "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"

Com o advento e a popularização da internet e as transformações nas relações sociais, fez-se necessária a regulamentação da internet de forma mais específica, de forma que em 2014 foi promulgada a lei nº 12.965/2014, também conhecida como Marco Civil da Internet no Brasil. Nesta lei, entre outras questões, há um aprofundamento sobre o entendimento legal da proteção à intimidade e vida privada dos indivíduos em um contexto digital.

O artigo 7º do Marco Civil trata dos direitos e garantias do usuário da internet no Brasil:

> "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;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> [...]
> 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:
> a) justifiquem sua coleta;

> b) não sejam vedadas pela legislação; e
> c) 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;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;"

Por esta lei, portanto, fica estabelecido que é um direito inviolável dos usuários de internet que suas vidas privadas não sejam violadas, que operações de coleta, uso, processamento e compartilhamento de dados pessoais necessitam justificativa e que, principalmente, tais operações necessitam de consentimento do usuário. Além disso, também é garantido ao usuário o direito de solicitar a exclusão definitiva de dados pessoais que ele tenha fornecido a determinado serviço.

Observando o texto desta lei sob a ótica de um usuário de algum serviço digital na internet com relação a seus dados pessoais, uma vez que o usuário tenha fornecido seu "livre consentimento" e sejam fornecidas a ele "informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais", este serviço digital poderá fazer, desde que "justificado", o uso destes dados. Portanto, pelo texto desta lei, após fornecer seu consentimento, a única ação possível por esse usuário no que se refere aos seus dados pessoais é solicitar a "exclusão definitiva" deles, porém a lei não especifica de que forma pela qual o usuário deve fazer esta solicitação e nem com que prazo ela deve ser atendida.

Especificamente tratando-se do entendimento de "consentimento", além de mencionar que ele deve ser "livre, expresso e informado" e que devem ser fornecidas "informações claras e completas" sobre as operações envolvendo dados pessoais, não há no Marco Civil da Internet nenhuma explicitação mais profunda sobre o entendimento legal de "consentimento" no contexto digital.

O Marco Civil da Internet, apesar de pioneiro (note-se que ele foi publicado 4 anos antes da GDPR, na União Europeia) deixou diversas lacunas sobre o significado de "tratamento de dados" e "consentimento", sobre forma que tais dados

seriam processados e qual deveria ser o nível de transparência disto para com o titular dos dados. Com o objetivo de se aprofundar nas questões específicas referentes à proteção de dados pessoais foi promulgada em 2018 a lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais.

Se antes, contando apenas com o Marco Civil da Internet, o titular de dados pessoais tinha apenas direito a solicitar a exclusão dos seus dados pessoais (caso tivesse consentido previamente a coleta), com a Lei Geral de Proteção de Dados, em seu artigo 18 diversos novos direitos foram garantidos a este usuário:

> "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei."

Além de definir os direitos do titular de dados de forma mais ampla, a LGPD também especificou o conceito de "consentimento", definindo em seu Artigo 5º, inciso XII que consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Assim como no Marco Civil da Internet no Art.7º inciso IX garante o direito aos usuários de internet ao "consentimento expresso sobre  consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais", a LGPD em

seu Art. 7º, inciso I define que “O tratamento de dados pessoais poder ser realizado [...] mediante fornecimento do consentimento do titular”, porém o entendimento do que é este consentimento é bastante detalhado em seus artigos 8º e 9º:

> “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.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
> § 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.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração. [...]
> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador; [...]
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; [...]
> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as

> mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

Apesar de ser mais específica sobre o que pode ser legalmente considerado um “consentimento” válido fornecido pelo titular dos dados pessoais, a LGPD possui alguns termos abertos a interpretações diversas no contexto digital, como por exemplo a nulidade do consentimento em caso de “vício de consentimento” (Art.8º § 3º), “conteúdo enganoso ou abusivo” e em que “não tenham sido apresentadas [informações] previamente com transparência, de forma clara e inequívoca” (Art.9º § 1º e 2º).

Termos como “de forma clara” têm sua interpretação especialmente dificultada em um contexto tecnológico que, conforme foi explorado na seção anterior deste trabalho, muitas vezes possui sistemas que foram projetados com intuito manter uma assimetria de conhecimento entre o usuário e o negócio digital. Uma vez que a mesma lei deve ser aplicada ao titular dos dados pessoais e aos agentes manipuladores destes dados pessoais, é bastante delicado depender de conceitos como “de forma clara” quando sabe-se que a capacidade de entendimento das duas partes envolvidas é, de partida, desigual[3].

Além disso, a clareza e a transparência da informação que deve ser fornecida ao titular dos dados pessoais não dependem exclusivamente dos textos com os termos legais que normalmente são apresentados aos usuários. Além da grafia do texto em si, o momento em que o consentimento é requisitado dentro da jornada de uso do produto pode influenciar seu entendimento ou sua capacidade de julgamento sobre estes termos. A própria forma como os termos são exibidos e as condições de concordar ou não concordar com eles pode ser projetada de forma a sutilmente influenciar o usuário a não dar atenção aos termos.

Portanto apesar de a LGPD ter grandes avanços no aumento da cobertura da defesa dos dados pessoais dos usuários no Brasil, apenas leis e regulações podem não ser suficientes para assegurar que modelos de negócios digitais adotem boas práticas, ética ou transparência neste campo.

---

[3]Com relação à dificuldade de tratar sobre o conceito de consentimento quando há desigualdade de conhecimento entre as partes, este tema será tratado mais a fundo na seção “3.1. O dilema do consentimento e possibilidades para o *UX Design*”

## 2.4. *UX design* e a assimetria de conhecimento

Leis e regulamentações como a LGPD, conforme analisado na seção anterior (“2.3. Legislação brasileira, privacidade e consentimento”), buscam resguardar a segurança dos dados pessoais dos usuários por meio, dentre outros mecanismos, da obrigatoriedade de requisição de consentimento do usuário para a coleta, processamento e compartilhamento destes dados. Porém, conforme explorado na seção “2.2. Capitalismo de vigilância”, dentro do atual modelo econômico da era digital existem diversos modelos de negócios digitais que se beneficiam e por vezes buscam que haja uma assimetria de conhecimento entre o negócio e o usuário, ou seja, há interesse econômico de alguns agentes em manter o usuário alheio a determinados entendimentos.

Uma vez que, no contexto de uso de dados pessoais, uma lei obrigue negócios digitais a requisitarem o consentimento do usuário “de forma clara e inequívoca” (como por exemplo a LGPD em seu artigo 9º §2º) e esta obrigação tenha implicações nos interesses econômicos destes negócios digitais, torna-se relevante discutir a forma com a qual este consentimento é solicitado ao usuário.

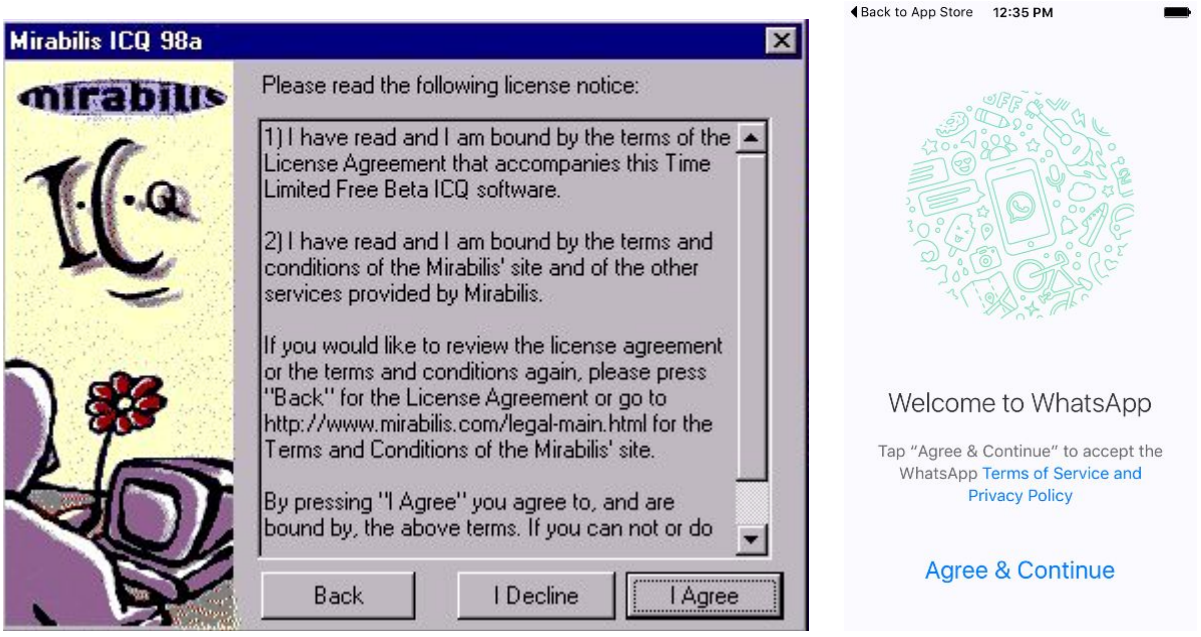
**Figura 4 - Exemplo de jornada do usuário em primeiro acesso a serviço digital**


*fonte: o autor*

Normalmente, conforme ilustrado na Figura 4, na jornada de uso de um determinado serviço digital, o momento em que é requisitado que o usuário consinta

com os termos de privacidade é no primeiro acesso ao serviço, durante o processo de criação de sua conta. A forma como, em plataformas digitais, estes termos costumam ser apresentados ao usuário requisitando seu consentimento não sofreu muitas alterações nas últimas décadas. Abaixo, na Figuras 5, constam exemplos das telas de requisição de consentimento de dois *softwares* de mensagens instantâneas: à esquerda o ICQ, em sua versão lançada em 1998 para sistema operacional Windows; à direita o Whatsapp, em uma versão lançada em 2018 para iOS (sistema operacional de *smartphones* da Apple).

**Figura 5 - Comparação das interfaces de requisição de consentimento entre os aplicativos ICQ (1998) e Whatsapp (2018)**



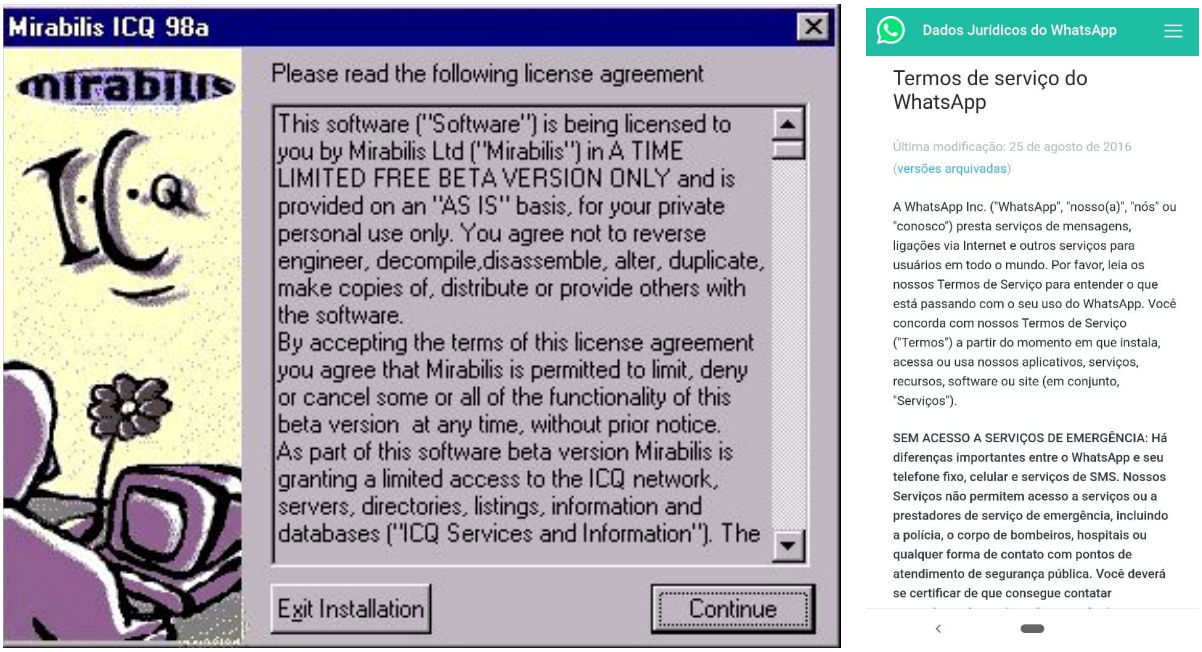

*fontes: http://www.planetsys.com.br/htm/help/ICQinst.htm (acesso em 1/9/2019) e https://ssd.eff.org/en/module/how-use-whatsapp-ios (acesso em 1/9/2019)*

Apesar das claras diferenças visuais entre cada uma destas interfaces (cores, proporção, tipografia, diagramação, etc.), em uma análise específica sobre a forma como as informações estão organizadas e como é proposto o fluxo de navegação do usuário, ambas são muito semelhantes entre si. Um intervalo de 20 anos separa o momento de publicação das versões do *software* de cada uma dessas telas e, apesar disso, ambas fazem uso da mesma estrutura lógica: um texto simplificado explicando ao usuário que a partir dali ele aceitaria algum termo (não explícito nesta

tela) e um botão em posição de destaque onde o usuário, ao clicar, continuará sua navegação e ao mesmo tempo concordará com os tais termos.

Os termos em si só seriam exibidos para o usuário caso ele decidisse clicar no *hyperlink* para lê-los, ação que em nenhum dos dois exemplos era mandatória. A forma como tais termos eram exibidos para o usuário também pouco mudou nesses 20 anos de intervalo. Como pode-se notar na Figura 6, a exibição dos termos tanto do ICQ em 1998 quanto do Whatsapp em 2018 consiste, basicamente, em uma tela com uma longa barra de rolagem vertical contendo um texto corrido fazendo a descrição técnica e legal daquilo que o usuário estaria consentindo.

**Figura 6 - Comparação das interfaces de exibição de termos de serviço e privacidade entre os aplicativos ICQ (1998) e Whatsapp (2018)**

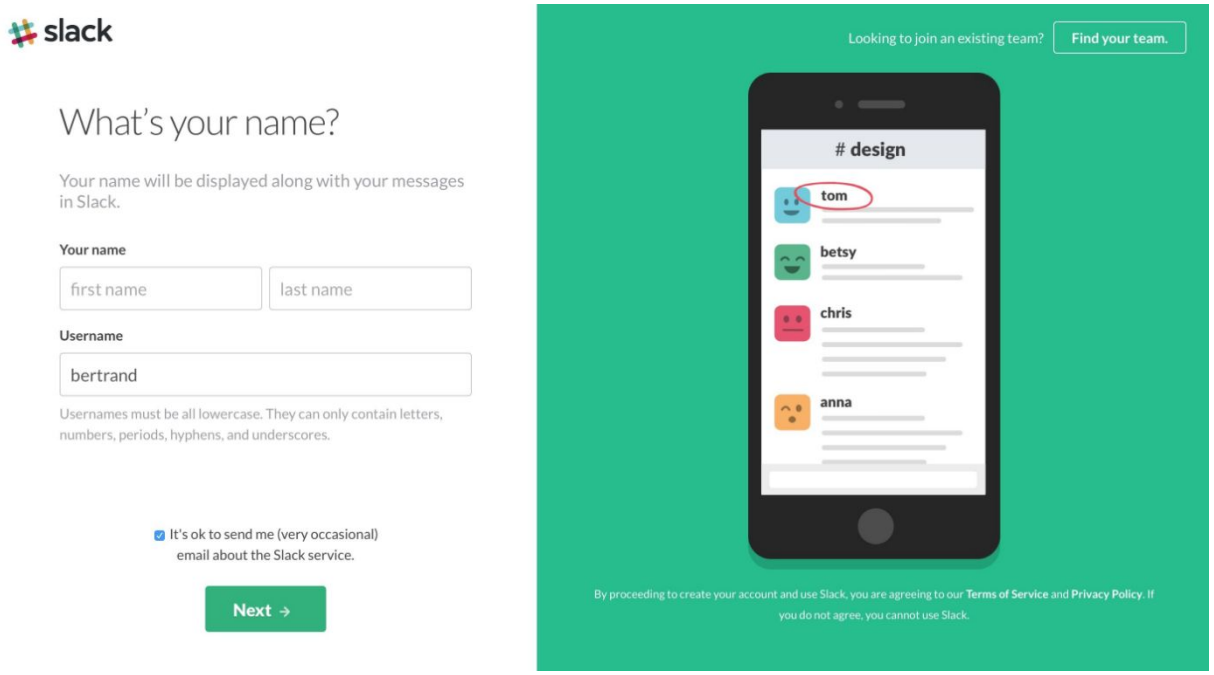



*fontes: http://www.planetsys.com.br/htm/help/ICQinst.htm (acesso em 1/9/2019) e https://www.whatsapp.com/legal/?lg=pt&lc=BR&eea=0 (acesso em 1/9/2019)*

Se ao analisar estes exemplos das Figuras 5 e 6 é possível afirmar que houve poucas mudanças na estrutura e no fluxo de navegação como se requisitava o consentimento do usuário, por outro lado há exemplos recentes tanto de melhorias como de pioras nas interfaces de requisição de consentimento ao usuário.

Na Figura 7 consta uma imagem da interface de criação de uma conta no serviço digital Slack que foi capturada no ano de 2017. Note-se que esta interface não está mais presente no Slack e foi reprojetada diversas vezes desde então.

**Figura 7 - Interface de criação de conta do Slack em 2017**




*fonte: https://nicelydone.club/products/slack/sign-up-2/create-a-team-slack-6/*
*(acesso em 9/1/2019)*

No que se refere à jornada do usuário, diferente dos exemplos anteriores do ICQ e do Whatsapp, onde o consentimento aos termos de serviço e privacidade ocorria em um momento separado da inserção de dados cadastrais, neste exemplo de 2017 a interface do Slack concatenava ambas etapas em uma única interface, sendo que ao clicar no botão "*Next*" o usuário ao mesmo tempo confirmaria seus dados de cadastro e consentiria aos termos de serviço e privacidade, conforme era informado na legenda abaixo da ilustração na direita da interface (Figura 7.1).

**Figura 7.1 - Detalhe da figura 7**

Há grande destaque visual nesta interface para o botão “*Next*” (“Próximo”), que com seu formato retangular e cor verde ganha grande contraste com o fundo branco da página, evidenciando para o usuário por meio do texto e do ícone da seta para a direita que, para continuar a navegação sua navegação adiante, aquele botão deveria se pressionado. Note-se que cognitivamente falando, o botão com um texto que diz “Próximo” associado a uma seta para a direita, no contexto ocidental gera no usuário a expectativa de um único resultado, que é ir para a próxima tela dentro da navegação do sistema.

Contudo o texto que consta na Figura 7.1, posicionado distante do botão “*Next*” e portanto se assemelhando a uma legenda da ilustração do aparelho celular, implica que ao clicar no botão “*Next*” o usuário já estaria concordando com os termos de serviço e de privacidade da plataforma. Ou seja, a forma como essa interface foi projetada induz o usuário a executar duas ações quando ele cognitivamente acredita estar fazendo apenas uma.

Não faz parte do escopo deste estudo entrar no mérito de juízo da intencionalidade existente no projeto das interfaces mencionadas em todos exemplos nesta seção. O intuito da utilização dos exemplos é apenas ilustrar que a forma com a qual se solicita o consentimento de um usuário pode influenciar em seu entendimento.

Isto posto, consideremos então os casos onde há intencionalidade daqueles que projetaram o sistema e as interfaces em confundir o usuário. Sabendo-se que é possível, por meio de determinados padrões visuais e manipulações cognitivas, induzir um usuário a executar uma ação que ele não desejava tomar conscientemente, modelos de negócio digitais podem fazer isso intencionalmente para conseguir que o usuário, por exemplo, consinta em ter seus dados coletados, processados e compartilhados sem que ele de fato entenda claramente que está fazendo-o.

O *UX designer* e PhD em ciência cognitiva Harry Brignull cunhou em 2010 o termo “*dark patterns*” (“padrões obscuros” em tradução livre) do *UX design*. Segundo Brignull, padrões obscuros são "Interfaces que foram cuidadosamente projetadas para induzir os usuários a fazer determinadas ações. [Estas ações acontecerem] não é um erro do usuário, elas foram pensadas e desenhadas com base em um sólido

entendimento da psicologia humana e não têm em mente os interesses do usuário" (BRIGNULL, 2010, tradução nossa).

Brignull definiu doze categorias de padrões obscuros que poderiam ser aplicados a interfaces com intuito de confundí-los e, posteriormente, estas categorias foram utilizadas como base para outro estudo que identificou cinco tipos de estratégias de uso de padrões obscuros (GRAY et al., 2018).

**Figura 8 - Sumário de estratégias de "padrões obscuros"**


*fonte: GRAY et al., 2018, tradução nossa*

Se considerarmos, por exemplo, as interfaces nas quais o usuário deve ativamente clicar em botões com texto "Eu concordo" para dar seu consentimento a algum termo específico sem contudo saber o conteúdo deles, os casos mais comuns de estratégias de padrões obscuros que é possível identificar em serviços digitais seriam a "Interferência na interface", onde o design dos elementos gráficos visa confundir o usuário, "Esconder", onde os termos são ocultados do usuário de forma proposital e a "Ação forçada", que forçaria o usuário a executar a ação de consentir com os termos para pode usar ou continuar usando alguma funcionalidade.

E se considerarmos as interfaces onde os termos de serviço e privacidade são de fato exibidos para os usuários, como por exemplo na Figura 6, poderia-se ainda considerar a estratégia de padrão obscuro "Obstrução", onde por meio de linguagem técnica e extensa o usuário pode ser dissuadido de tentar compreender os termos com os quais ele estaria concordando.

Neste sentido, as estratégias de padrão obscuro no *UX design* são ferramentas comuns e necessárias dentro do conceito de Capitalismo de Vigilância de Zuboff, onde para o usuário “é impossível entender algo que foi desenvolvido em segredo e projetado para ser fundamentalmente ilegível” (ZUBOFF, 2019, tradução nossa).

Assim sendo, pode-se dizer que este tipo de projeto de *UX design* que intencionalmente prejudica o usuário é, além de antiético, danoso para o próprio desenvolvimento da sociedade como um todo, pois ele fomenta uma assimetria de conhecimento entre os indivíduos e os serviços e produtos que eles utilizam. As estratégias de uso de padrões obscuros em *UX design* fomentam e induzem os usuários a se manterem alheios a questões que podem lhes ser extremamente prejudiciais.

A disciplina de *UX design* tem como base os conceitos do design centrado no usuário e não deveria, portanto, comportar tais práticas. Conforme exemplifica Jonathan Shariat em seu livro “*Tragic Design: The Impact of Bad Product Design and How to Fix It*” (“Design trágico: O impacto do design de produto ruim e como consertá-lo”, em tradução livre), “designers são como os guardiões dos portões da tecnologia. Eles têm um papel crítico na forma como tecnologias irão impactar as vidas das pessoas” (SHARIAT et al., 2017, tradução nossa).

Propositalmente alimentar a assimetria de conhecimento é algo extremamente irresponsável, especialmente em períodos de grande transformação como o que vivemos agora, onde novos paradigmas de organizações tecnológicas e socioeconômicas se impõem de forma a colocar em risco a experiência humana de privacidade. O papel de um *UX designer* frente a estes desafios vai para além de sua responsabilidade enquanto técnico, há um papel ético e social de grande impacto para toda a sociedade a ser exercido. Conforme afirma Donald Norman, “os princípios que guiam a qualidade, bem como um design centrado na pessoa não são apenas relevantes para uma vida mais prazerosa – ele pode salvar vidas” (NORMAN, 2006). Ao contrário de induzir a assimetria de conhecimento, “o design deve sempre trabalhar para prevenir os erros [do usuário], reduzindo a carga cognitiva deles em vez de encarregar-lhes do fardo de evitar o erro” (SHARIAT et al., 2017, tradução nossa).

# 3. Design do consentimento

Em sistemas digitais que trabalham com a coleta de dados pessoais o consentimento dos usuários é recolhido, normalmente, por meio de interfaces que apresentam os termos de uso e privacidade junto de um botão no qual, ao clicar, o usuário registra estar de acordo com tais termos. Ao projeto desta experiência de usuário que ocorre quando são informadas a ele questões envolvendo o uso de seus dados pessoais e é solicitado que ele concorde ou não com estas questões será dada a definição, neste trabalho, de "design do consentimento".

Nesta seção será abordado como o *UX design* pode ser uma ferramenta complementar de grande importância para suprir lacunas deixadas por regulamentações e leis de proteção da privacidade, explorando como aspectos do design centrado no usuário e do design de proposta de valor no sentido de responsabilidade corporativa podem ser aplicados à privacidade.

## 3.1. O dilema do consentimento e possibilidades para o *UX Design*

Conforme foi abordado na seção “2.3. Legislação brasileira, privacidade e consentimento”, a lei federal nº13.709/2018 - a Lei Geral de Proteção de Dados Pessoais (LGPD) - faz uso constante do conceito de requisição de consentimento por parte do usuário, o detentor dos dados pessoais.

O uso legal da requisição de consentimento relativo a operações com dados pessoais tem o intuito de impedir que sejam executadas quaisquer ações que o usuário considere prejudiciais a si mesmo sem que ele saiba ou consinta com isso. É uma forma de redigir legislações de defesa da privacidade que já existia nos Estados Unidos da América desde os anos 70 (SOLOVE, 2012) e se mantém como um padrão até hoje, onde:

> “A lei fornecia às pessoas um conjuntos de direitos para possibilitá-las tomar decisões sobre como gerenciar seus dados. Estes direitos consistiam primeiramente no direito de conhecimento, acesso e consentimento no que se refere à captura, uso e compartilhamento de dados pessoais. O objetivo deste conjunto de direitos era dar às pessoas o controle sobre seus dados pessoais e por meio deste controle as pessoas poderiam decidir por si próprias como balancear os custos e os benefícios da captura, uso o compartilhamento de informações sobre elas” (SOLOVE, 2012, tradução nossa).

A esta concepção de sistema onde o usuário é o gestor de sua própria privacidade foi dado o nome por Solove de “*privacy self-management*” (“autogestão da privacidade”, em tradução livre).

Em seu artigo “*Introduction: Privacy self-management and the Consent Dilemma*” (2012), Solove aponta três motivos pelos quais ele acredita que a autogestão de privacidade, apesar de bem intencionada, possui problemas causados pelo contexto no qual ela está inserida:

- Estudos sociais empíricos apontam que existem problemas cognitivos na autogestão de privacidade que impedem que um indivíduo, em determinadas situações, consinta com algo de forma bem informada e racional, não sendo portanto capaz de avaliar custos e benefícios relacionados a sua privacidade;

- Devido a problemas estruturais, mesmo um indivíduo que consinta de forma bem informada não tem capacidade por si só de gerenciar sua privacidade. Há demasiados agentes envolvidos na captura, coleta, processamento e compartilhamento de seus dados pessoais, tornando impraticável que o usuário lide com cada um dos agentes individualmente;

- A autogestão da privacidade foca-se em indivíduos, sendo que a privacidade tem impactos na sociedade. Aquilo com que um indivíduo isolado consentir pode não refletir o resultado final desejado pela sociedade como um todo.

Mas quando são redigidas leis que buscam formatos alternativos à autogestão da privacidade, frequentemente as soluções apresentadas são, de acordo com Solove, paternalistas: elas definem o que pode ou não ser feito sobre a privacidade individual, tirando o direito de escolha do indivíduo. Ou seja, se por um lado leis que reforçam a autogestão da privacidade não garantem que o consentimento do usuário tenha real significado devido a problemas contextuais, por outro lado leis que tomam decisões pelo usuário de forma paternalista cerceiam o próprio consentimento dele, criando o que Solove nomeou como o dilema do consentimento (SOLOVE, 2012).

Ainda segundo Solove, para que seja possível avançar numa nova direção, os problemas da autogestão da privacidade e do dilema do consentimento precisam ser reconhecidos por aqueles que redigem as leis e regulamentações de privacidade.

Como sugestões para a redação de futuras leis que não enfrentem estes mesmos problemas, Solove sugere três possíveis diretrizes:

- **Repensar o consentimento e aplicar "*nudges*"[4]:** Nesta diretriz, Solove sugere que a forma como o Direito trata o consentimento ainda não está alinhada com as complexidades cognitivas já cientificamente conhecidas nestes processos humanos de tomada de decisão, pois tratam tais decisões como questões binárias, sendo que o contexto possui, na realidade, diversas nuances. Neste sentido, Solove sugere uma mistura de consentimento com a aplicação de "*nudges*", que seriam uma forma mais branda de paternalismo, sendo portanto menos restritivos do que regulamentações tradicionalmente paternalistas. Os *nudges* serviriam como sugestões não impositivas para o usuário de quais as decisões mais indicadas para ele tomar.

- **Desenvolvimento de uma autogestão parcial da privacidade:** Solove exemplifica que quando trata-se de outros objetos que não a privacidade, como por exemplo carros, o modo mental dos consumidores é ter poder de decisão de escolha sobre alguns quesitos no momento da compra, porém assumindo que serão garantidos a eles parâmetros mínimos de segurança sobre os quais eles não precisarão se preocupar. Portanto não se espera que, para comprar um carro, os usuários sejam *experts* em carros. Neste sentido, Solove indica que é necessário que a legislação da privacidade busque esse meio termo daquilo que deve ser garantido e do que deve ser opcional. Além disso, Solove sugere que um caminho possível seria padronizar a gestão da privacidade de forma que o usuário possa fazê-la de forma global e unificada, não por dividindo-a por entidade envolvida no processo.

[4] O termo "*nudge*", usado por Thaler e Sunstein em seu livro "*Nudge*: Como tomar melhores decisões sobre saúde, dinheiro e felicidade" (2009), trata-se da ação de, por meio de pequenas mudanças na arquitetura do processo de tomada de decisão, alterar de forma previsível o comportamento esperado de indivíduos sem, contudo, privar-lhes do direito de escolha.

- **Ajuste do foco e do *timing* da gestão da privacidade:** Solove expõe que hoje as leis de privacidade possuem um foco muito grande no momento inicial da jornada do usuário (por exemplo, no momento da criação de sua conta no serviço digital), sendo que a forma como os dados pessoais podem ser usados pelo serviço varia ao longo do tempo. Solove sugere que tranforme-se o processo de informar o usuário e solicitar seu consentimento em algo mais distribuído ao longo da jornada de uso do serviço, pois isto poderia facilitar o entendimento do usuário. Fragmentaria-se o consentimento em pedaços menores e mais simples que seriam apresentados ao usuário em momentos que fizessem sentido de acordo com o uso e os dados cedidos pelo usuário.

Ao observar essas três sugestões de diretrizes propostas por Solove, que têm como objetos o Direito e o desenvolvimento de leis e regulamentações de privacidade, é importante notar que estas recomendações têm também grande aderência com o campo de *UX Design*, como por exemplo na aplicação de *nudges* ou mesmo no consentimento distribuído de forma dispersa ao longo da jornada.

Além disso, ao contrário do Direito - onde há esta discussão sobre prós e contras do paternalismo - é importante ressaltar que o Design, por outro lado, é essencialmente não-neutro na mediação do que o usuário pode escolher fazer ou não. Conforme foi explorado na seção “2.4. *UX design* e a assimetria de conhecimento”, onde foi apresentado que o design pode ser uma ferramenta usada com intuito de confundir o usuário por meio de estratégias de padrões obscuros, quando algo é projetado com base nos princípios do design centrado no usuário, o designer é conscientemente paternalista ao tomar decisões pelo usuário sobre como ele fará e não fará uso daquele objeto.

As próprias conclusões de Solove sobre o Dilema do Consentimento, nas quais ele sugere o uso de *nudges* como uma forma de paternalismo direcionado indicam que, para atingirmos um novo patamar na forma como tratamos a defesa da privacidade, é necessário ir para além das leis e regulamentações. É necessário discutir e trabalhar na forma que tratamos o consentimento no sentido literal de formato, jornada e experiência do usuário.

### 3.2. Design centrado no usuário aplicado à privacidade e ao consentimento

Donald Norman, em seu livro “O Design do dia-a-dia” (2006) definiu sete princípios que deveriam ser aplicados ao design de objetos do dia-a-dia para se obter produtos facilmente compreensíveis e utilizáveis pelos usuários, sendo:

- **Usar ao mesmo tempo o conhecimento no mundo e o conhecimento na cabeça**: refere-se a fazer um design que seja possível do usuário compreender, onde ao utilizar um determinado objeto para cumprir uma tarefa o usuário seja capaz de, com seu próprio conhecimento aliado ao conhecimento disponível ao seu redor, aprender como executar tal tarefa;

- **Simplificar a estrutura de tarefas**: refere-se ao design que busca facilitar que os usuários cheguem ao objetivo desejado da forma mais simples possível, uma vez que tarefas demasiadamente complexas ou que exijam muitos passos podem, além de escapar da memória de curto prazo do usuário, gerar uma sobrecarga cognitiva nele;

- **Tornar as coisas visíveis - encurtar ou superar as lacunas de execução e avaliação**: refere-se ao design de sistemas que indiquem de forma clara o que é possível o usuário fazer com eles, quais seus estados atuais e quais os resultados que serão atingidos caso o usuário execute determinadas ações, estando portanto claramente alinhado às expectativas e intenções do usuário.

- **Fazer corretamente os mapeamentos:** refere-se a fazer um design intuitivo, fazendo a correlação correta entre o que o usuário espera que aconteça e o que de fato acontece;

- **Explorar o poder das coerções naturais e das artificiais:** refere-se a fazer um design que evite que o usuário cometa erros ao evidenciar de forma muito clara (e por vezes inescapável) como deve-se fazer o uso correto;

- **Projetar para erros:** refere-se ao design que assume que o usuário pode vir a cometer erros ao utilizar o sistema e, portanto, fornece maneiras para que ele perceba que cometeu um erro e possa reverter sua ação sem custos, incentivando assim que o usuário se permita explorar o sistema.

- **Quando tudo mais falhar, padronizar:** refere-se ao design que, quando é necessário ser feito de forma mais arbitrária, não intuitiva ou sem ter os mapeamentos corretos, pelo menos assume uma forma de padronização de larga escala. Assim, caso o usuário seja forçado a aprender a lógica desse sistema em específico de forma não intuitiva, ele terá que fazê-lo apenas uma vez, pois o padrão se repetirá em outros casos.

A primeira edição deste livro de Norman é de 1982, contexto histórico onde as discussões sobre tecnologia e privacidade estavam bastante distantes do ponto onde se encontram hoje, em que as comunidades de pesquisadores e *designers* discutem cada vez mais a necessidade de criar sistemas considerando "*privacy by design*" ("privacidade desde a concepção" em tradução livre) (VARISCO, 2019).

Mas apesar deste distanciamento histórico entre os princípios do design centrado no usuário de Norman da discussão sobre como lidar com o dilema do consentimento de Solove (tratada na seção anterior), é possível identificar aplicações diretas dos princípios de Norman nas diretrizes indicadas por Solove para o futuro da gestão da privacidade e do consentimento.

Estas possíveis aplicações serão listadas e comentadas abaixo em três tabelas separadas, uma para cada diretriz indicadas por Solove, de forma a relacionar em cada uma das linhas um dos princípios do design centrado no usuário de Norman, qual o grau de aplicabilidade do princípio à diretriz de gestão de privacidade em questão e um breve comentário sobre a aplicabilidade definida.

## Diretriz: Repensar o consentimento e aplicar *nudges*

| Princípios de Norman | Aplica-bilidade | Observações |
|---|---|---|
| Usar ao mesmo tempo o conhecimento no mundo e o conhecimento na cabeça | Alta | Ao propor que o consentimento seja repensado, Solove aponta como um dos principais problemas a dificuldade cognitiva de o usuário assimilar a complexidade daquilo com o que ele está consentindo. Neste sentido, “repensar o consentimento” pode ser criar um processo de consen-timento no qual o usuário seja capaz de entender de pronto do que se tratam os termos com os quais ele concorda, buscando-se uma forma mais intuitiva do que textos redigidos com uma linguagem técnica do ramo do Direito. |
| Simplificar a estrutura de tarefas | Baixa | O processo de consentimento utilizado normalmente hoje não é uma tarefa que exige grande esforço cognitivo do usuário, contudo justamente o fato de ele ser demasiado simples e simplista (um único consentimento para uma porção de resultados e impactos diferentes que ocorrerão no pequeno, médio e longo prazo) torna o consentimento problemático, pois faz o usuário tratá-lo com pouca atenção. |
| Tornar as coisas visíveis | Alta | Norman defende que o estado de um sistema deve ser facilmente percebido, de forma a indicar para o usuário quais os efeitos de suas ações. Neste sentido, o processo de consentimento poderia ser repensado em um formato mais fragmentado ao longo da experiência do usuário como um todo, sinalizando esparsamente em quais momentos e interações específicas haverá alguma operação envolvendo dados pessoais |
| Fazer corretamente os mapeamentos | Alta | Por vezes o processo de consentimento é executado ao mesmo tempo que o usuário cria uma conta em um novo serviço, de forma que em um único botão ambas ações são concretizadas, gerando um mapeamento incorreto entre a intenção do usuário e os resultados atingidos. |
| Explorar o poder das coerções | Alta | Coerções no sentido que Norman as explora (vulgo impedindo o usuário de errar) seriam consideradas políticas paternalistas por Solove, de forma que a sugestão de Solove pela aplicação dos *nudges* seria uma adaptação das coerções, ou seja, indicações mais favoráveis de quais as decisões mais seguras para o usuário ao ter que decidir se consente ou não com determinados termos de privacidade. |
| Projetar para erros | Alta | A requisição do consentimento de forma simplificada no início da experiência do usuário no serviço não condiz com a dificuldade posterior que frequentemente é encontrada para se retirar esse consentimento ou parte dele. |
| Quanto tudo mais falhar, padronizar | Média | No caso do consentimento, a padronização só faz sentido se for aplicada em nível global, o que é difícil de ser imaginado na prática visto que cada serviço e cada país tem requisitos específicos no que se refere ao uso de dados pessoais. |

**Direção: Desenvolvimento de uma autogestão parcial da privacidade**

| Princípios de Norman | Aplica-bilidade | Observações |
|---|---|---|
| Usar ao mesmo tempo o conhecimento no mundo e o conhecimento na cabeça | Média | A autogestão parcial proposta por Solove assume que o usuário seria responsável apenas por uma parte das decisões referentes a sua privacidade, já as outras fariam parte de um “pacote mínimo” padronizado, sobre o qual ele não precisa se preocupar. O usuário não precisaria ser um *expert* em privacidade, bastaria ele saber que alguém, de forma paternalista, decidiu fixar quais suas garantias mínimas. |
| Simplificar a estrutura de tarefas | Alta | A autogestão parcial da privacidade, em contraposição à autogestão total, simplifica as tarefas do usuário no sentido de aliviar sua carga cognitiva, pois tomam-se por ele algumas decisões que seriam mais elementares. |
| Tornar as coisas visíveis | Média | A autogestão parcial da privacidade, ao tomar algumas decisões pelo usuário, nem sempre será capaz de evidenciar seus estados, ações e resultados, pois o usuário pode não compreender questões sobre as quais ele não tomou decisões ativas. |
| Fazer corretamente os mapeamentos | Alta | Para que uma autogestão parcial da privacidade seja efetiva, as decisões que forem ser tomadas de antemão devem ter mapeamentos alinhados com as expectativas básicas do usuário com relação à sua privacidade. |
| Explorar o poder das coerções | Alta | Na autogestão parcial da privacidade existem, por essência, coerções em uso, uma vez que decisões já teriam sido tomadas previamente pelas leis, coibindo possíveis erros do usuário. |
| Projetar para erros | Baixa | Na autogestão parcial da privacidade há questões que não poderão ser alteradas pelo usuário, pois há predefinições nas leis, de forma que alguns comportamentos não poderão ser corrigidos ou desfeitos. |
| Quanto tudo mais falhar, padronizar | Alta | A autogestão parcial da privacidade requer que seja estabelecido um conjunto de requisitos mínimos relacionados à privacidade que devem ser garantidos para o usuário sem gerar uma grande carga cognitiva de decisão para ele. A definição desses requisitos mínimos demanda uma padronização global que permita que os usuários aprendam isto apenas uma vez e tal conhecimento seja válido para qualquer sistema que ele venha a utilizar. |

## Direção: Ajuste do foco e do *timing* da gestão da privacidade

| Princípios de Norman | Aplica-bilidade | Observações |
|---|---|---|
| Usar ao mesmo tempo o conhecimento no mundo e o conhecimento na cabeça | Alta | Norman, ao definir este princípio, levava em conta que a capacidade cognitiva dos indivíduos é limitada. Nesta direção de Solove, ao propor o ajuste do *timing* e do foco da gestão da privacidade, propõe uma gestão mais fragmentada, ou seja, onde o usuário tornaria-se mais capaz de gerir sua própria privacidade se as decisões que fossem solicitadas a ele fossem menores e, portanto, de apreensão mais fácil. |
| Simplificar a estrutura de tarefas | Baixa | Ao se criar uma gestão de privacidade mais distribuída, haverá mais tarefas para o usuário executar ao longo de sua jornada no sistema, visto que o consentimento deixaria de ser dado apenas no início da jornada e se espalharia em diversos pontos dela. |
| Tornar as coisas visíveis | Alta | A autogestão da privacidade com consentimento concentrado no ponto inicial da jornada colabora para que muitas ações e resultados não sejam visíveis para o usuário. Fragmentar o consentimento pode facilitar o processo de tornar os estados visíveis para o usuário. |
| Fazer corretamente os mapeamentos | Alta | Uma vez que a autogestão da privacidade seja aplicada em *timings* diferentes para o usuário, são aumentadas as chances desse consentimento “esparso” ter maior correlação com as reais intenções do usuário ao longo de sua jornada de uso do serviço. |
| Explorar o poder das coerções | Baixa | A ideia de Solove em mudar o foco e o *timing* da gestão da privacidade baseia-se mais em fornecer ao usuário mais momentos de decisão (porém mais simplificados) do que em criar coerções que evitem que ele cometa erros. |
| Projetar para erros | Alta | Uma vez que as decisões a serem tomadas pelo usuário para gestão de sua privacidade sejam menores e mais espaçadas ao longo de sua jornada, é mais fácil projetar para o erro, permitindo que o usuário perceba o resultado de suas ações e possa desfazer ações menores mais facilmente. |
| Quanto tudo mais falhar, padronizar | Baixa | A mudança de foco e de timing é muito dependente do tipo de jornada do usuário projetado para cada sistema, de forma que a padronização desta quebra de timing seria demasiadamente complexa. |

Dos vinte e um cruzamentos entre as diretrizes para o futuro da gestão da privacidade de Solove (2012) e os princípios do design centrado no usuário de Norman (2006), apenas cinco deles foram considerados de baixa aplicabilidade, portanto mais de 75% dos princípios do design centrado no usuário têm relevância para a criação de uma nova forma de gestão da privacidade que não dependa tanto do consentimento e nem seja demasiadamente paternalista.

Desta forma evidencia-se que os problemas e soluções apontados por Solove em seu estudo sobre o dilema do consentimento, apesar de se referirem inicialmente à esfera legal, na verdade estão extremamente ligados à jornada do usuário ao utilizar um sistema e à forma como ocorrem suas interações dentro desse sistema, pontos estes que são centrais na disciplina de *UX design*. A evolução de políticas e regulamentações de gestão da privacidade necessariamente passa por discussões que envolvem *UX design*, ética e a forma que essas disciplinas passarão a gerar valor não apenas para o usuário e a sociedade, mas também para o próprio negócio.

### 3.3. Privacidade como proposta de valor

Apesar de todos riscos e preocupações apresentados neste estudo no que se refere à defesa da privacidade dos usuários na era da informação digital, é importante ressaltar que operações que envolvem dados pessoais de usuários não são essencialmente mal-intencionadas e obviamente nem sempre estão interessadas em gerar excedente comportamental.

Há claros benefícios sendo gerados pelo avanço tecnológico envolvido nas tecnologias de processamento de dados. A coleta de dados de diversas fontes de forma ubíqua gerando enormes bases de dados (*big data*) e tecnologias como *machine learning*, inteligência artificial e computação cognitiva trouxeram diversos avanços para a humanidade e em muitos aspectos ampliaram a capacidade humana de cumprir determinadas tarefas.

Os ganhos em eficiência e eficácia que algoritmos de inteligência artifical trouxeram a campos como a medicina, por exemplo, são imensos. Apenas para citar um exemplo, pesquisadores da Alemanha, França e Estados Unidos da América desenvolveram um algoritmo capaz de detectar câncer de pele de forma mais efetiva do que dermatologistas experientes (a máquina acertou corretamente 95% das vezes enquanto o painel de médicos humanos acertou 86,6%) (EPSTEIN, 2019).

Contudo mesmo quando não há intencionalidade dos sistemas de se aproveitar mercadologicamente do excedente comportamental gerado por suas capturas de dados, a governança de tais bases de dados é de extrema importância para manter informações e dados pessoais seguros. A discussão em torno de leis como GDPR e a LGPD gira em torno especificamente dos dados pessoais, de forma que muitas vezes aponta-se como solução para manutenção da privacidade o processo e anonimização das bases, ou seja, não associar aos registros dados que sejam identificáveis sobre um indivíduo em específico.

Legalmente a definição de dado pessoal busca delimitar claramente o entendimento, como por exemplo no Art. 5º da LGPD, que define dado pessoal como qualquer “informação relacionada a pessoa natural identificada ou identificável”. Porém a ideia de um dado ser “identificável” é bastante subjetiva, uma vez que na era da informação digital há inúmeras bases de dados espalhadas pelo mundo, referentes a produtos diferentes em plataformas diferentes que podem, ao

ter seus dados cruzados, gerar padrões e informações que podem tornar um registro específico identificável, revelando portanto informações potencialmente sensíveis de um indivíduo em específico. Um caso bastante referenciado no qual isto ocorreu foi num desafio proposto pela plataforma de vídeos sob demanda Netflix. A empresa lançou um concurso onde eles divulgaram uma base anonimizada de preferências de 500 mil usuários para geração de *insights* sobre a base. Dois pesquisadores, ao fazer o cruzamento desta base com dados públicos da plataforma IMDB foram capazes de descobrir informações pessoais de diversos usuários da Netflix. “Usando o IMDB como fonte de conhecimento prévio, nós identificamos com sucesso usuários da Netflix, revelando suas preferências políticas e outras informações potencialmente sensíveis” (NARAYANA et al., 2008, tradução nossa).

Ou seja, apesar de as bases de dados usadas pela Netflix nesse caso não conterem dados considerados pessoais, por meio de um processamento conjunto com informações externas estes dados anonimizados se tornaram identificáveis. Tal situação legal é extremamente complexa de ser prevista em leis ou regulamentações sobre privacidade.

Conforme mencionado anteriormente neste trabalho, o aumento de casos de grandes vazamentos de dados pessoais e quebras de privacidade em meios digitais aumentaram a busca por soluções que sejam projetadas com "*privacy by design*", ou seja, privacidade desde a concepção. Um método desenvolvido neste sentido é o conceito de privacidade diferencial, que trabalha com estatística e matemática para que determinadas análises de bases de dados sejam processadas de forma tal que nunca seja possível garantir que uma informação específica se refira a um indivíduo específico. Em outras palavras, numa análise de dados que usa o método matemático de privacidade diferencial é estatisticamente impossível determinar se um indivíduo específico faz parte de um recorte amostral A ou B. É possível saber a proporção geral de indivíduos em A e em B, mas não a informação sobre um indivíduo específico. "Informalmente, a privacidade diferencial requer uma distribuição de probabilidade nos resultados de uma análise de dados de forma tal que, se um indivíduo específico fizer ou não fizer parte desse conjunto de dados, o resultado da análise será essencialmente o mesmo" (DWORK, 2011, tradução nossa).

Este tipo de aplicação de método de preservação da privacidade é invisível para o usuário final: se uma empresa usa privacidade diferencial em suas atividades de análise de dados internas ou não, no serviço ou produto final que é entregue ao usuário este valor não será visível, é algo que faz parte de uma visão estratégica de responsabilidade da empresa com a privacidade de seus usuários.

Este processo de as próprias empresas compreenderem a importância estratégica e o valor social de adotar boas práticas de governança de dados e defesa da privacidade individual é chave para que, ao tornar isto um diferencial para o consumidor, seja gerado um movimento do mercado como um todo.

Simon Zadek (2004) em seu artigo "*The path to corporate responsibility*" ("O caminho para a responsabilidade corporativa" em tradução livre) explora este tema:

> "Conforme as visões das organizações com relação a um determinado problema mudam e amadurecem, o mesmo ocorre com as da sociedade. Para além de manter ordem na própria casa, as companhias precisam estar alinhadas com as ideias do público sobre quais os papéis e responsabilidades das corporações. A jornada de uma companhia atravessando estas duas dimensões - organizacional e social - invariavelmente as levam para o que chamo de 'aprendizado civil'" (ZADEK, 2004, tradução nossa).

Neste mesmo artigo Zadek mostra que as empresas aderem a determinadas pautas em diferentes estágios de comprometimento, havendo uma escala de evolução nestes níveis que vai desde estágios mais básicos como “Defensivo” e “*Compliance*” até estágios mais avançados, como “Gerencial” e “Estratégico”, conforme pode-se verificar na tabela a seguir:

**Estágios de responsabilidade corporativa**

| Estágio | O que é feito | Porque é feito |
|---|---|---|
| Defensivo | Negação de práticas, impactos ou responsabilidades. (*"Isso não aconteceu. Isso não é conosco"*). | Para defender-se contra ameaças que possam afetar as vendas, a marca ou outros resultados no curto prazo. |
| Obediência *(compliance)* | Adoção de políticas e procedimentos para atender a legislação, como um custo para fazer negócios. (*"Faremos apenas o que tem que ser feito."*). | Para reduzir perdas de valor econômico no médio prazo em função de riscos legais e litígios em geral. |
| Gerencial | Incorporação das questões nos processos de gestão. *("Isso é parte do negócio.")* | Para reduzir perdas de valor econômico no médio prazo e buscar ganhos no longo prazo, a partir da integração de práticas responsáveis no dia-a-dia das operações. |
| Estratégico | Integração das questões nas estratégias do negócio. *("Isso nos dá diferenciais competitivos.")* | Para ampliar valor econômico no longo prazo e obter vantagens competitivas através do alinhamento de estratégias e processos de inovação com as questões. |
| Liderança Social | Mobilização para um amplo envolvimento do mercado nas questões. *("Precisamos garantir que todos façam isso.")* | Para ampliar valor econômico no longo prazo através da redução de eventuais desvantagens do pioneirismo e para obter ganhos através da ação coletiva. |

*Fonte: Adaptado pelo autor a partir da adaptação da Ekobé, a partir de ZADEK (2004).*

Considerando um contexto onde regulamentações voltadas à defesa de dados pessoais, como a LGPD no Brasil, foram publicadas bastante recentemente, muitas empresas ainda se encontram nos dois primeiros estágios desta tabela, defensivo e *compliance*, buscando evitar perdas, sanções e multas. Contudo o caminho para que a sociedade como um todo evolua as discussões sobre a defesa de suas próprias experiências, seus dados comportamentais e sua privacidade passa, necessariamente, por uma transformação no mercado. Se hoje práticas corporativas como, por exemplo, adoção de análise de dados usando privacidade diferencial, ainda são incipientes, o movimento das corporações na direção de tratar a privacidade de seus consumidores como algo estratégico deve se tornar um diferencial, pois existe um grande potencial em se transformar a defesa da privacidade em um gerador de valor para a empresa, para o consumidor e para a sociedade.

## 4. Considerações finais

Este estudo teve como objetivo fazer uma contextualização sobre questões relacionadas à privacidade na era da informação digital e como a disciplina de *UX design* poderia ser aplicada a esse cenário de forma a gerar valor para os usuários, as empresas e a sociedade.

Se por lado o levantamento feito sobre o design do consentimento - que cruzou as direções apontadas por Solove (2012) para o futuro da gestão da privacidade com os princípios do design centrado no usuário de Norman (2006) - pode encontrar aplicações práticas no projeto de interfaces de requisição de consentimento de usuários sobre a coleta e processamento de seus dados pessoais, por outro lado tornou-se evidente, principalmente com base na revisão bibliográfica de Zuboff (2019), que este olhar focado em *UX design* trata-se de um pequeno recorte de questões maiores, que extrapolam o design de sistemas e plataformas digitais em si.

A utilização de estratégias de padrões obscuros no *UX design* (GRAY et al., 2018), por exemplo, trata-se apenas de um reflexo de uma lógica de mercado que está em crescimento na economia global. Assim, apesar de ser relevante discutir a ética na prática de *UX design* neste contexto da privacidade individual, a discussão que mostra-se mais urgente é sobre o atual modelo econômico em si e sobre como, dentro dele, a privacidade ainda existe majoritariamente como um gerador de valor financeiro (por meio dos mercados de comportamento surgidos a partir da geração de excedentes comportamentais) e não um gerador de valor social.

O campo do *UX design*, no contexto da era digital, inegavelmente faz parte de tanto dos problemas quanto das soluções para o futuro da gestão da privacidade humana, mas ele certamente não o faz de forma isolada. Porém é importante notar que, justamente por ser uma área do conhecimento que busca trabalhar com base em uma visão holística dos problemas tratados, o design é uma área chave para liderar este movimento de busca de geração de valor a partir da defesa da privacidade, puxando consigo outras áreas do conhecimento envolvidas.

## 4.1. Trabalhos futuros

Os cruzamentos e comentários apresentados neste trabalho com relação às diretrizes de Solove (2012) e os princípios do design centrado no usuário de Norman (2006) servem de insumos para projetos de *UX design* que visem tratar a privacidade de forma mais estratégica, porém tais cruzamentos não foram aprofundados a ponto de poderem ser considerados nem diretrizes de design, nem manuais de boas práticas e nem propostas reais ou tangíveis de *UX design*. Assim ressalta-se aqui a importância do desenvolvimento de trabalhos futuros que explorem, a partir destes cruzamentos e dos contextos apresentados neste trabalho, como podem se dar aplicações práticas no campo do design para projetar soluções digitais que gerem valor a partir da defesa da privacidade de forma ética e evitando as problemáticas do Dilema do Consentimento.

Para além dos possíveis desdobramentos de trabalhos futuros ligados especificamente ao *UX design*, também é importante ressaltar a necessidade de pesquisas futuras como a feita por Zadek (2004) sobre o processo de transformação da responsabilidade corporativa, porém focadas em questões relacionadas à privacidade, ética e governança de dados. Os formatos de negócios digitais propostos por Weill (2015) que indicam "conhecimento do cliente" como gerador de valor para o negócio podem ter impactos negativos na sociedade, havendo portanto espaço para melhoria deles enquanto geradores de valor social. É necessário aprofundar os estudos sobre como, dentro da era digital, a preservação da privacidade e da experiência humana podem gerar valor econômico por meio de novos modelos de negócios digitais que, ao mesmo tempo que adquiram conhecimento sobre seus clientes, sejam socialmente sustentáveis.

## 5. Referências

BELL, Genevieve; DOURISH, Paul. **Yesterday's tomorrows: notes on ubiquitous computing's dominant vision**. Personal and ubiquitous computing, v. 11, n. 2, p. 133-143, 2007.

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

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, 24 de abril de 2014, Brasília, DF.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, 15 de agosto de 2018, Brasília, DF.

BRIGNULL, Harry. **Dark Patterns**. Disponível em <https://www.darkpatterns.org>. Acesso em 30 agosto 2019.

CASAL, Camila. **A evolução do direito de imagem no Direito Brasileiro**. JusBrasil, 2016. Disponível em: <https://camilacasal.jusbrasil.com.br/artigos/339215138/a-evolucao-do-direito-de-imagem-no-direito-brasileiro>. Acesso em 11 maio 2019.

CASE, Amber. **Calm technology: Principles and patterns for non-intrusive design**. " O'Reilly Media, Inc.", 2015.

DOURISH, Paul; BELL, Genevieve. **Resistance is futile: reading science fiction alongside ubiquitous computing**. Personal and Ubiquitous Computing, v. 18, n. 4, p. 769-778, 2014.

DWORK, Cynthia. **Differential privacy**. Encyclopedia of Cryptography and Security, p. 338-340, 2011.

EPSTEIN, Sophia. Robodocs. **Weapons of Reason**, Londres, vol.6, p.39-43, 2019. Disponível em <https://medium.com/the-ai-issue-weapons-of-reason/robodocs-5d6c7a970fea>. Acesso em 6 setembro 2019.

FERRARIS, Maurizio. **Documentality - Or why nothing social exists beyond the text**. From ontos verlag: Publications of the Austrian Ludwig Wittgenstein Society-New Series (Volumes 1-18), v. 3, 2013.

GRAY, Colin M. et al. **The dark (patterns) side of UX design**. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, 2018. p. 534.

ISAAK, Jim; HANNA, Mina J. **User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection**. Computer, v. 51, n. 8, p. 56-59, 2018.

NIEUWDORP, Eva. **The pervasive discourse: an analysis**. Computers in Entertainment (CIE), v. 5, n. 2, p. 13, 2007.

LANDAU, Susan. **Making sense from Snowden: What's significant in the NSA surveillance revelations**. IEEE Security & Privacy, v. 11, n. 4, p. 54-63, 2013.

LASKIN, David. **The great London smog**. Weatherwise, v. 59, n. 6, p. 42-45, 2006.

LEE, Kai-Fu. **AI superpowers: China, Silicon Valley, and the new world order**. Houghton Mifflin Harcourt, 2018.

LOEBBECKE, Claudia; PICOT, Arnold. **Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda**. The Journal of Strategic Information Systems, v. 24, n. 3, p. 149-157, 2015.

LUPTON, Deborah. **The diverse domains of quantified selves: self-tracking modes and dataveillance**. Economy and Society, v. 45, n. 1, p. 101-122, 2016.

MATZ, Sandra C. et al. **Psychological targeting as an effective approach to digital mass persuasion**. Proceedings of the national academy of sciences, v. 114, n. 48, p. 12714-12719, 2017.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Robust de-anonymization of large datasets (how to break anonymity of the Netflix prize dataset)**. University of Texas at Austin, 2008.

NORMAN, Donald A. **O design do dia-a-dia**. Rio de Janeiro: Rocco, 2006.

SHARIAT, Jonathan; SAUCIER, Cynthia Savard. **Tragic Design: The Impact of Bad Product Design and How to Fix It**. " O'Reilly Media, Inc.", 2017.

SILVER, Nate. **O sinal e o ruído**. Editora Intrínseca, 2013.

SOLOVE, Daniel J. **Introduction: Privacy self-management and the consent dilemma**. Harvard Law Review, v. 126, p. 1880, 2012.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge: Improving decisions about health, wealth, and happiness**. Penguin, 2009.

VARISCO, Laura. **Personal Interaction Design: Introducing in the Design Process the Discussion on the Consequences of the Use of Personal Information**. 2018. 304 p. Tese (Doutorado) - Politecnico Di Milano, Dipartimento di Design, Milão, 2019

WEILL, Peter; WOERNER, Stephanie L. **Thriving in an increasingly digital ecosystem**. MIT Sloan Management Review, v. 56, n. 4, p. 27, 2015.

WEISER, Mark; GOLD, Rich; BROWN, John Seely . **The origins of ubiquitous computing research at PARC in the late 1980s**. IBM systems journal, v. 38, n. 4, p. 693-696, 1999.

YAU, Nathan; SCHNEIDER, Jodi. **Self-Surveillance**. Bulletin of the American Society for information Science and Technology, v. 35, n. 5, p. 24-30, 2009.

YOUNG, Nora. **The virtual self: How our digital lives are altering the world around us.** McClelland & Stewart Limited, 2012.

ZADEK, Simon. **The path to corporate responsibility**. Harvard business review, v. 82, n. 12, 2004.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for the future at the new frontier of power**. Profile Books, 2019.