V!19
issn 2175-974x | ano 2019 year
semestre 02 semester

André Lemos é Engenheiro Mecânico e Doutor em Sociologia. É Professor Titular do Departamento de Comunicação e do Programa de Pós-Graduação em Comunicação e Cultura Contemporâneas da Universidade Federal da Bahia, onde coordena o Lab404 - Laboratório de Pesquisa em Mídia Digital, Redes e Espaço. Atua nas áreas de comunicação e sociologia, com ênfase em cultura digital ou cibercultura. É membro do Comitê Gestor do Instituto Nacional de Ciência e Tecnologia em Democracia Digital.

Daniel Marques é Bacharel em Design e Mestre em Comunicação e Cultura Contemporâneas. É Professor Assistente da Universidade Federal do Recôncavo da Bahia, e pesquisador no Lab404-Laboratório de Pesquisa em Mídia Digital, Redes e Espaço, da Universidade Federal da Bahia, onde estuda Design, inovação e cultura, Visualização de dados e mapping art, Cultura, comunicação e sistemas de linguagem.

Como citar esse texto: LEMOS, A.; MARQUES, D. Interfaces Maliciosas: estratégias de coleta de dados pessoais em aplicativos. **V!RUS**, São Carlos, n. 19, 2019. [online]. Disponível em: <http://www.nomads.usp.br/virus/_virus19/?sec=4&item=2&lang=pt>. Acesso em: 13 Dez. 2019.

ARTIGO SUBMETIDO EM 18 DE AGOSTO DE 2019

Resumo

O artigo analisa as interfaces maliciosas (IM) presentes em 10 aplicativos usados pela municipalidade de Salvador para a coleta de dados pessoais. Tais aplicativos atuam na construção e experiência da cidade contemporânea, mediando diferentes aspectos da vida social urbana. Essa nova dimensão informacional da cidade, por sua vez, impõe desafios à manutenção da privacidade do cidadão ao fomentar a maximização da produção e coleta de dados pessoais sensíveis. A partir de uma escala de gravidade (EG), as interfaces foram avaliadas com o intuito de identificar os tipos de IM presentes e os graus de ameaça à privacidade dos usuários. Constata-se que todos os aplicativos analisados têm IM, sendo majoritário o nível 1 (leve), demonstrando tendência a sua naturalização. Essas IM fazem parte da expansão da plataformização da sociedade, do processo de datificação e do agenciamento performativo dos algoritmos (PDPA).

Palavras-chave: *Dark patterns*, Aplicativos, Privacidade, Salvador

1 Introdução

A produção da vida social na cidade contemporânea se encontra cada vez mais imbricada com as tecnologias digitais de informação e comunicação. *Smartphones*, assistentes virtuais, aplicativos, algoritmos e redes sociais, por exemplo, passam a ocupar um espaço significativo na tessitura do social, mediando relações de sociabilidade, afeto, trabalho, educação e lazer. O espraiamento dessas mediações, por sua vez, leva ao extremo a ideia de uma "sociedade informacional", tendo em vista a centralidade da produção da informação – e do acesso a uma quantidade cada vez maior de dados – na geração de valor para o chamado capitalismo de plataforma/vigilância (ZUBOFF, 2015).

O dado, portanto, torna-se a nova *commodity* do capitalismo contemporâneo, enquanto o cidadão e a cidade se configuram enquanto fontes desse material. Nesse sentido, à medida em que o valor dos dados se torna maior e mais evidente, passamos a verificar um maior esforço por parte de múltiplas instituições – públicas e privadas – em coletar e extrair valor dessas informações, colocando em risco a manutenção da vida privada. Tendo em vista que a produção e a coleta de dados são o objetivo maior do capitalismo de vigilância, faz-se necessário politizar as estratégias e as mediações através das quais busca-se domesticar o cidadão a produzir cada vez mais dados. O capitalismo de dados é uma forma de "construção da informação", colocando em risco a privacidade dos cidadãos no espaço urbano.

O objetivo desse artigo, portanto, é discutir o que se vem chamando de *Dark Patterns* (DP), interfaces que levam os usuários a desempenhar determinadas ações com intenções diversas. Um dos objetivos é coletar dados pessoais, não necessariamente imprescindíveis para o objetivo do serviço. Essa coleta caracteriza a "dataficação" para fins comerciais ou técnicos. Ao induzir ações de captação desnecessária de dados pessoais, os DP ameaçam a privacidade. O interesse nessa temática vem justamente da crítica à essas ameaças presentes em aplicativos e *websites* (ASH, et al., 2018a, 2018b). Analisamos 10 aplicativos em uso pela Prefeitura Municipal de Salvador, BA. O artigo parte de uma perspectiva neomaterialista e pragmática (FOX; ALLDRED, 2017; LEMOS, 2019a), analisando a ação dessas interfaces. Indicamos uma escala de gravidade (EG) de três níveis para análise, descrição e comparação das interfaces. Propomos chamar esses padrões de "interfaces maliciosas" (IM).

2 Interfaces Maliciosas (IM)

O termo *dark pattern* (DP) foi proposto por Harry Brignull, doutor em psicologia cognitiva pela Universidade de Sussex, profissional da área de design de interação (UI) e experiência do usuário (UX), em uma palestra proferida no evento UX Brighton, em 2010[1]. São estratégias de design utilizadas em interfaces digitais (*websites*, aplicativos, *wearables* etc.) e derivam da tradição de padrões de design (*design patterns*)[2]. A expressão ganhou popularidade e tem sido apropriada por profissionais e acadêmicos do design e da computação. Recentemente o tema apareceu no *Financial Times*[3], *Gizmodo*[4], *The New York Times*[5] e *The Verge*[6].

Para Brignull, os DP não são meramente *bad designs*. Eles são *antipatterns*, criados para fazer com que o usuário realize ações de interesse do aplicativo/empresa sem que ele se dê conta ou tenha como evitar. Diferentemente dos *bad designs*, os DP se caracterizam pela intencionalidade obscura, desenvolvidos para obtenção de resultados específicos sem explicações ao usuário. Nas suas palavras, "esse é o lado sombrio do *design* e, como esse tipo de padrão não tem nome, proponho que passemos a chamá-lo de *dark pattern*" (tradução nossa) (BRIGNULL, 2010, s.p.). Essas estratégias se baseiam na exploração de atributos cognitivos e psicológicos dos usuários, fazendo com que estes não percebam que há um agenciamento do seu comportamento. Brignull propôs uma taxonomia inicial dos DP, catalogando 11 espécies diferentes[7], as quais foram posteriormente expandidas pela literatura.

Propomos traduzir o termo "*dark patterns*" por "interfaces maliciosas" (IM). Nesse artigo vamos discutir as interfaces maliciosas (IM) com relação ao problema do uso de dados pessoais e as ameaças à privacidade. O desenvolvimento das IM para a maximização da produção, coleta e processamento de dados pessoais situa-se em um contexto mais amplo: a cultura da PDPA (LEMOS, 2019a, 2019b) – **plataformização** da sociedade (VAN DIJCK; POELL; DE WAAL, 2018), **dataficação** (MAYER-SCHONBERGER; CUKIER, 2013) e **performatividade algorítmica** (BUCHER, 2017; DANAHER, 2016).

Trata-se de fenômenos que caracterizam o atual estado da cultura digital, apontando para a expansão das plataformas digitais na mediação do cotidiano. A plataformização da sociedade, nesse sentido, diz respeito à crescente presença de plataformas digitais – geralmente produtos e serviços associados ao GAFAM[8] – na mediação e realização da vida social. Essas mediações ocorrem, majoritariamente, através da ação de sistemas algorítmicos performativos que atuam na organização da vida social a partir do projeto das plataformas. Como a PDPA desenvolve-se em meio à expansão do capitalismo de dados (ou de vigilância) (SRNICEK, 2017; ZUBOFF, 2015), considera-se o dado pessoal como a principal *commodity* (SADOWSKI,

2019), dada a necessidade de projetar sistemas computacionais capazes de maximizar sua produção, coleta e processamento, ou seja, "**dataficar**" a vida social. O termo PDPA, portanto, refere-se à integração desses fenômenos: as plataformas digitais agem e se materializam a partir da implementação de algoritmos performativos, e de processos diversos de coleta de dados pessoais (dataficação).

Desde 2010, a literatura sobre IM se diversificou em áreas e temas tais como o *design* de *games* (ZAGAL; BJÖRK; LEWIS, 2013), as interações por tecnologias de proximidade (GREENBERG, et al., 2014), a violação da privacidade e maximização de processos de dataficação (BÖSCH, et al., 2016; DOTY; GUPTA, 2013; FRITSCH, 2017), as implicações éticas (GRAY et al., 2018), o ativismo em plataformas digitais (TRICE; POTTS, 2018), as interfaces físicas e de voz (LACEY; CAUDWELL, 2019), entre outros. Autores destacam, inclusive, a instrumentalização de desenvolvedores para a utilização de IM enquanto estratégia competitiva (LEWIS, 2014; NODDER, 2013).

Das questões recorrentes na literatura, destacamos quatro pontos centrais: a) o problema da intencionalidade; b) o foco na observação das microinterações; c) os aspectos éticos e; d) os fatores psicológicos. O problema da intencionalidade é a questão mais comum e boa parte da literatura tende a reconhecê-la como o objetivo maior das empresas. Na nossa postura pragmática, parece ser muito subjetivo afirmar intencionalidade e mais produtivo analisar os efeitos concretos das IM. Na maioria dos casos, elas se enquadram nos limites da legislação vigente (DOTY; GUPTA, 2013).

Muitos experimentam o "paradoxo da privacidade" (WILLIAMS; NURSE; CREESE, 2016). Ao avaliarem o custo-benefício da concessão de dados pessoais em troca de bens e serviços, usuários preocupados com a privacidade acabam cedendo. Esse paradoxo torna-se mais complexo pois dificilmente o usuário é capaz de aferir o valor e as consequências do fornecimento dos seus dados. A assimetria entre o poder das plataformas e a capacidade reduzida de negociação dos usuários gera um processo de naturalização das IM como paradigma hegemônico do design de interação. A existência de literatura dedicada a encorajar e oferecer suporte à implementação de IM aponta para esse cenário (LEWIS, 2014; NODDER, 2013).

Tomemos dois exemplos de IM antes de nos debruçarmos sobre o nosso *corpus* empírico: os aplicativos *Mi Fit* e *Bike* Itaú.

O *Mi Fit* acompanha as *smart bands* da marca chinesa Xiaomi. Há dificuldades para visualizar documentos importantes tais como o "Acordo do Usuário" e as "Políticas de Privacidade", conforme podemos visualizar na Figura 1. Na tela "Configurações" não há nenhum indicativo de que eles estão na seção "Sobre" e, mesmo que o usuário consiga chegar aos documentos, não há uma preocupação em adequar o texto jurídico, longo e complexo, à situação de leitura em telas de *smartphones*. No entanto, a presença desses documentos é obrigatória e vista como uma boa prática na manutenção da privacidade (COLESKY; HOEPMAN; HILLEN, 2016; HOEPMAN, 2014; PATRICK; KENNY, 2003). Para usar o aplicativo, o usuário deve dar o seu consentimento, mesmo com dificuldade em acessar esses documentos. A materialidade da alienação no aplicativo indica a IM. Como todas, elas se produzem em um espaço assimétrico de negociação (ASH, 2018b). O efeito imediato é o aumento da leniência dos usuários em relação a coleta de dados realizada pela Xiaomi.

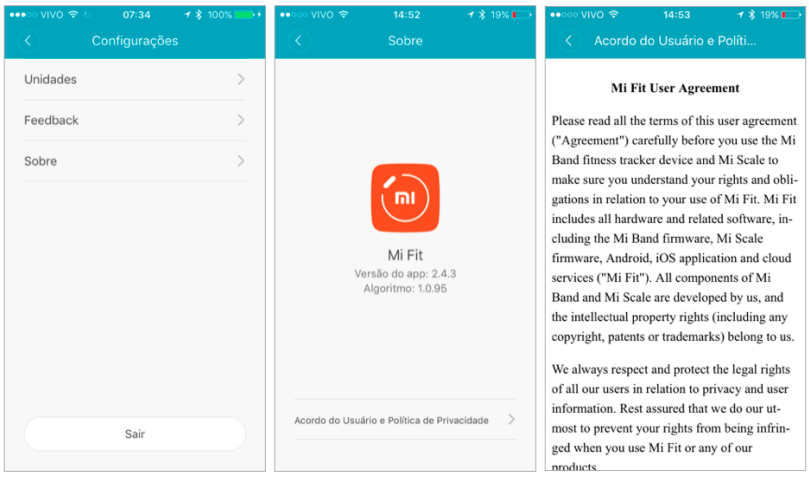

Fig. 1: Exemplo de IM no aplicativo Mi Fit. Fonte: Autores, 2019.

Outra IM comumente encontrada em aplicativos é o *Confirmshaming*, estratégia discursiva visando constranger o usuário a ceder o dado. No exemplo do *Bike* Itaú, apresentado na Figura 2, a primeira tela solicita o acesso à localização em tempo real do usuário, enquanto a segunda estimula o usuário a concluir o cadastro, afirmando que o dado será coletado "*só para mostrar os locais de retirada e devolução mais próximos de você*". Ironicamente, na Política de Privacidade[9] consta explicitamente que os dados coletados

podem ser compartilhados com parceiros. Na segunda tela, a entonação do texto é punitiva, informando que o abandono do cadastro acarretará mais trabalho no futuro, já que as informações não serão salvas.

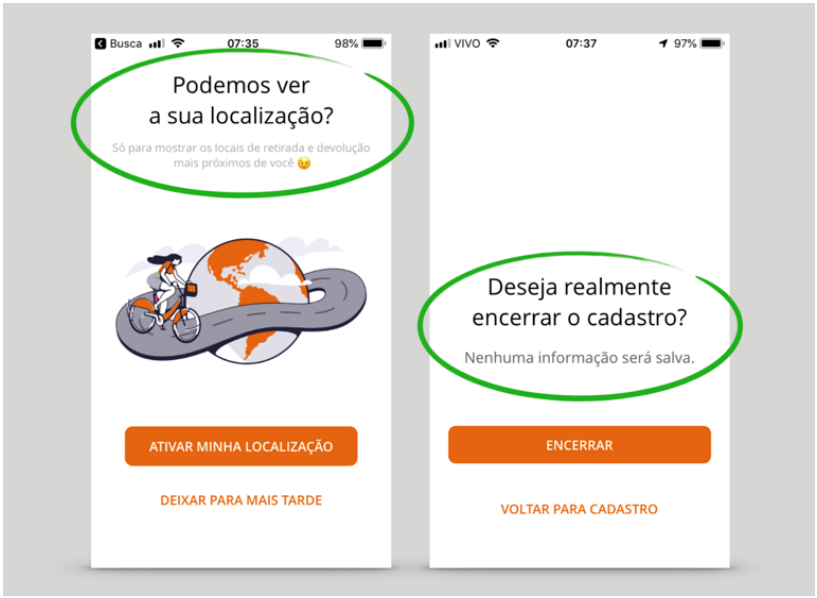

Fig. 2: *Confirmshaming* no Bike Itaú. Fonte: Autores, 2019.

3 Metodologia

Tendo em vista o cenário delineado acima, buscamos verificar a presença de IM e a ameaça à privacidade em 10 aplicativos, conforme Quadro 1, escolhidos por oferecerem serviços de interesse público na capital baiana, desenvolvidos por empresas privadas ou pelo Estado. Foram excluídos aqueles destinados a usos específicos (por nicho, como funcionários públicos, por exemplo). A análise das telas principais de cada aplicativo (aquelas que negociam algum tipo de dado pessoal, tanto a partir de requisição formal – formulários, cadastros, pedido de consentimento etc. – quanto a partir da interação com as funcionalidades) foi realizada utilizando o *software* ATLAS.ti[10]. A média de telas analisadas foi 8,1/app. O aplicativo com maior número de telas analisadas foi o *Bike* Itaú (15); no outro extremo, encontra-se o SAC BA (4).

	APLICATIVOS	OBJETIVO
01	**Bike Itaú**	Aluguel temporário de bicicletas
02	**CittaMobi**	Monitoramento de linhas e pontos de ônibus
03	**Coleta Seletiva**	Divulgação de pontos de coleta seletiva
04	**Detran.BA**	Solicitação e acompanhamento de serviços do Detran-BA
05	**Fácil Estacionar**	Estacionamento em Zona Azul
06	**FAZ Salvador**	Estacionamento em Zona Azul
07	**NOA Cidadão**	Canal de denúncias e acompanhamento de problemas em vias públicas de Salvador
08	**Rotativo Digital**	Estacionamento em Zona Azul
09	**Rotativo Salvador**	Estacionamento em Zona Azul
10	**SAC BA**	Solicitação e acompanhamento de serviços do SAC-BA

Quadro 1: Aplicativos analisados. Fonte: Autores, 2019.

Após a primeira codificação das IM, criamos diferenças de graus em uma "escala de gravidade" (EG) em termos de ameaças à privacidade. Essa diferenciação foi necessária para desenvolver análises comparativas. Propomos a seguinte EG: 1 - nível leve; 2 - nível moderado e 3 - nível grave. No nível leve (1) estão

enquadrados as IM que prescrevem a coleta de dados pessoais desnecessários para a realização da tarefa, mas que possuem alguma relação com a funcionalidade do aplicativo. No nível moderado (2) estão as IM que facilitam o compartilhamento dos dados pessoais com instituições externas, sendo que os dados solicitados estão de alguma forma envolvidos diretamente com o objetivo do serviço. O nível grave (3) é o das IM que coletam dados irrelevantes à tarefa e os compartilha com terceiros e/ou alienando o usuário do processo de coleta. Um aplicativo pode ter grau 3, sem ter graus 1 ou 2, e assim sucessivamente. É possível verificar o esquema de classificação na Figura 3.

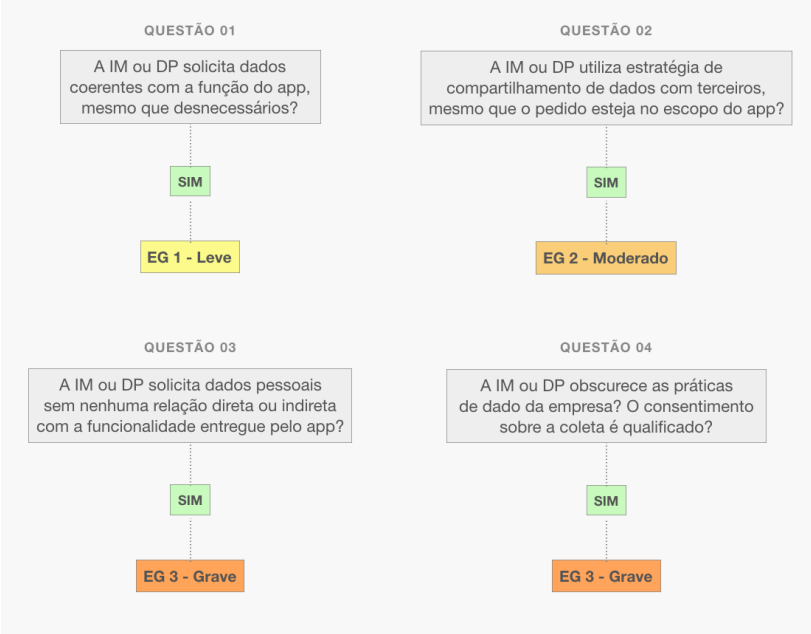

Fig. 3: Estrutura de classificação da Escala de Gravidade (EG). Fonte: LEMOS; MARQUES, 2019.

4 Distribuição das IM por aplicativo

O exemplo a seguir mostra como a análise foi feita para todos os aplicativos. Como é possível visualizar na Figura 4, no *Bike* Itaú[11] o usuário é forçado a se registrar para ter acesso ao serviço (IM - *Forced Registration*, EG1). É importante destacar que o *call to action* para realizar o cadastro/*login* não aparece de imediato. No primeiro acesso, o usuário se depara somente com o mapa contendo as estações disponíveis e as bicicletas. Essa é uma estratégia para estimular a interação livre, sem o desconforto inicial de preencher um formulário. Somente no momento de solicitar a liberação da bicicleta é que o usuário deve realizar um cadastro.

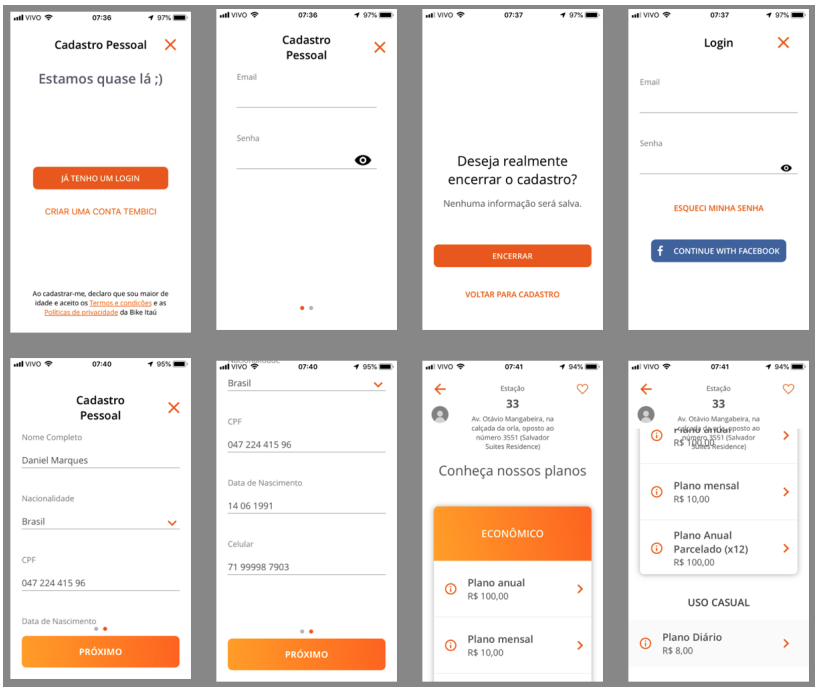

Fig. 4: *Forced Registration* no *Bike* Itaú. Fonte: Autores, 2019.

Na quarta tela, o usuário é estimulado a realizar o *login* a partir da API de cadastro do *Facebook* (IM - *Forced Registration* e API *Fest*). Como há indícios de compartilhamento de dados com terceiros (*Facebook*), o EG é moderado (2). Na primeira tela temos um exemplo da EG3 (IM - *Hidden Legalese Stipulations*), pois o consentimento do usuário é solicitado antes da realização do cadastro, alienando o usuário das práticas de dado do *Bike* Itaú. Esse aplicativo tem os três níveis de ameaça à privacidade do usuário.

Após análise de todos os aplicativos, dos 21 tipos de IM já catalogados em *websites* e na literatura especializada[12], verificamos a ocorrência de nove e acrescentamos mais um, ausente nessa catalogação, o "API *Fest*", totalizando 10 IM. O Gráfico 1 apresenta a ocorrência das IM. Entre todas as IM, as mais comuns são "*Forced Registration*" (9 ocorrências) e "*Information Milking*" (8 ocorrências). *Forced Registration* é a obrigação de cadastramento. *Information Milking* é a solicitação de informações que não são estritamente necessárias a realização da tarefa. Ambas estão diretamente relacionadas a um processo de maximização da coleta de dados pela constante inserção de dados no sistema e podem, a depender do aplicativo, caracterizar os três níveis de ameaça (como veremos à frente, no Gráfico 1).

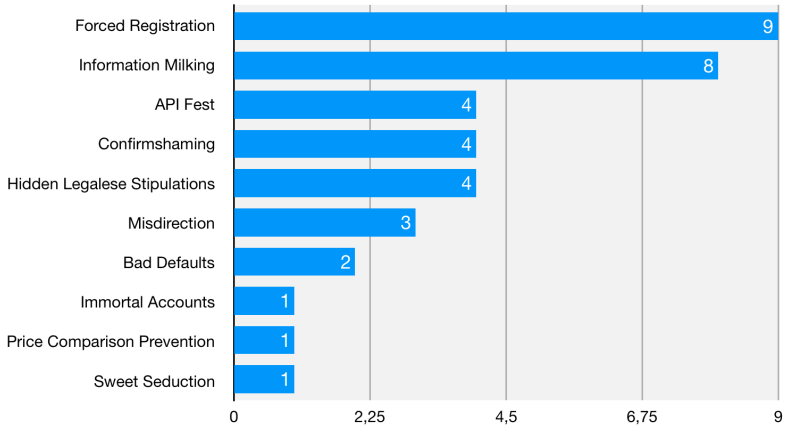

Gráfico 1: Ocorrência de IM por aplicativo (n = 10 aplicativos analisados). Fonte: Autores, 2019.

Destaca-se também a presença das IM API *Fest*, *Confirmshaming* e *Hidden Legalese Stipulations*, todas com quatro ocorrências cada uma. Essas IM estão relacionadas de forma direta ou indireta com a ampliação da coleta de dados pessoais e modulação de comportamentos. No primeiro caso (API *Fest*), é possível verificar que a interface utiliza sistemas de outras plataformas parceiras (*Google* e *Facebook*, por exemplo) para realizar a tarefa. A adoção dessas API, entretanto, inclui também a implementação de *trackers* que enriquecem as bases de dados das plataformas com novas fontes de dados. *Confirmshaming* é a estratégia discursiva de constrangimento do usuário para ceder o dado ou realizar a tarefa. Trata-se de uma manipulação cujo intuito é fazer com que o usuário se sinta culpado por não cumprir o programa de ação do aplicativo. Essa IM subverte a lógica do consentimento informado, tendo em vista que utiliza de linguagem persuasiva para convencer usuários a optar pela coleta e processamento de informações pessoais (ver gravidade no Gráfico 5). Alguns exemplos de *Confirmshaming* podem ser visualizados na Figura 5.

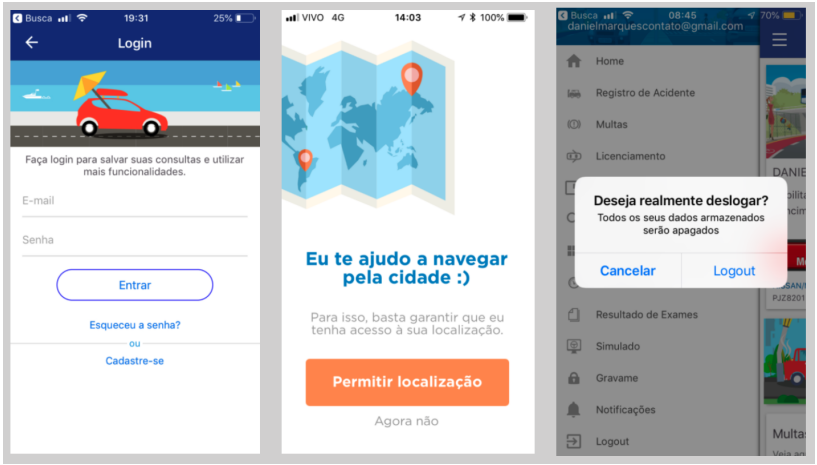

Fig. 5: *Confirmshaming* no Detran.BA (1, 3) e *Cittamobi* (2). Fonte: Autores, 2019.

A IM *Hidden Legalese Stipulations* indica formas de ocultação de acesso a informações legais importantes sobre a tarefa realizada. Nesse caso, trata-se de documentos como "Política de Privacidade" e "Termos de Uso". Como visto no exemplo da *Mi Fit*, essa IM pode, potencialmente, alienar os usuários acerca das práticas de dado das plataformas, tornando-o domesticado em relação ao programa de ação prescrito.

Observando a ocorrência das IM por *app*, verificamos a maior presença de IM no *Bike* Itaú (07), *CittaMobi* (06), Rotativo Digital (06) e Rotativo Salvador (05). Todos esses aplicativos foram desenvolvidos e são operados por empresas privadas. Embora cumpram funções diferentes, estão relacionados a aspectos da mobilidade urbana e lidam majoritariamente com dados de geolocalização. Os resultados podem ser visualizados no Gráfico 2.

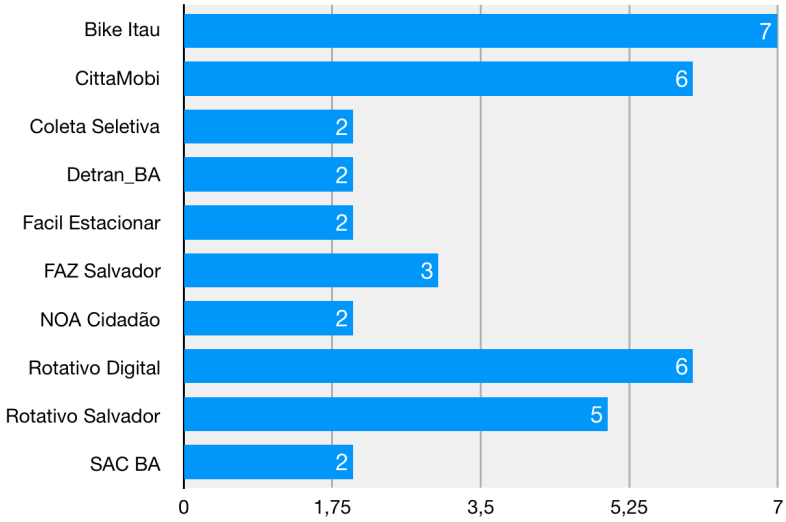

Gráfico 2: Ocorrência de IM por *app* (n = 10 IM verificados). Fonte: Autores, 2019.

Parece esperado que haja um maior empenho por partes de empresas privadas em explorar a retirada de dados pessoais. Os aplicativos mais próximos da administração pública (Coletiva Seletiva, Detran BA, NOA Cidadão e SAC BA) apresentam um número menor de IM. Embora esse dado seja uma pista interessante, faz-se necessário aprofundar essa discussão a partir de um melhor entendimento sobre o contexto de sua produção, bem como sobre os processos atuais de gerenciamento pela máquina pública e/ou iniciativa privada.

Aplicativos de uma mesma categoria podem apresentar IM diferentes, como o caso do Fácil Estacionar, FAZ Salvador, Rotativo Digital e Rotativo Salvador. Todos são credenciados pela Transalvador com o intuito de oferecer venda de créditos para Zona Azul Digital. Não é possível, portanto, atrelar a adoção de determinada estratégia de interação à entrega de uma funcionalidade específica.

5 Escala de gravidade

Todos os aplicativos analisados contém IM, conforme apresentado no Gráfico 3. Isso corrobora a hipótese de que a IM é uma característica da PDPA. 70% dos aplicativos foram classificados como nível 1 (leve). Os níveis 2 e 3 aparecem em 17% e 13%, respetivamente. Esses dados apontam para uma crescente naturalização e pervasividade da IM[13]. Essa naturalização pode gerar impactos na forma como entendemos a negociação de dados pessoais com as plataformas, pois à medida que práticas abusivas de interface se tornam lugar comum, os consumidores tendem a abrir mão da sua privacidade mais facilmente.

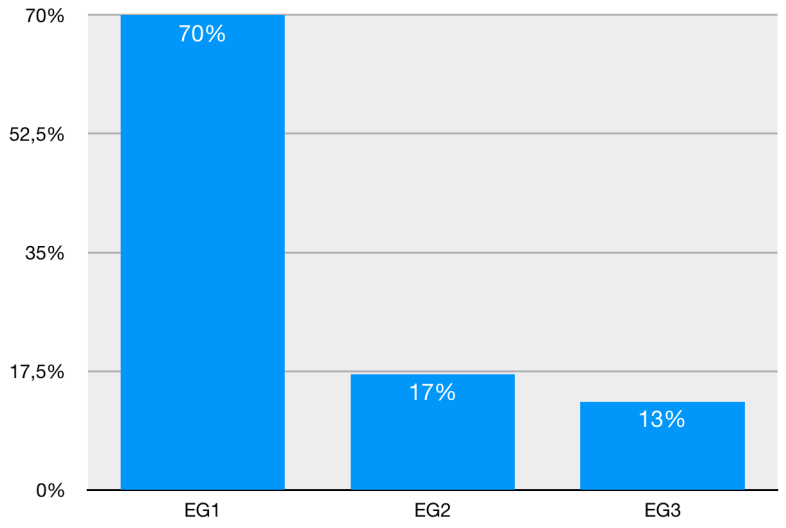

Gráfico 3: Distribuição das IM encontrados por EG. Fonte: Autores, 2019.

Sobre a distribuição da EG, percebe-se a presença mais significativa de IM classificados como EG2 e EG3 em aplicativos produzidos e administrados pela iniciativa privada. Os casos mais graves são do *CittaMobi* e do *Bike* Itaú, nos quais encontramos todos os níveis de EG. Nos dois casos ocorre uma parceria público-privada, na qual as empresas facilitam e gerenciam a oferta de determinado serviço de interesse público. Os outros mais graves são Rotativo Salvador, Rotativo Digital e Faz Salvador, que apresentam os níveis EG1 e EG3. Os resultados detalhados aparecem no Gráfico 4.

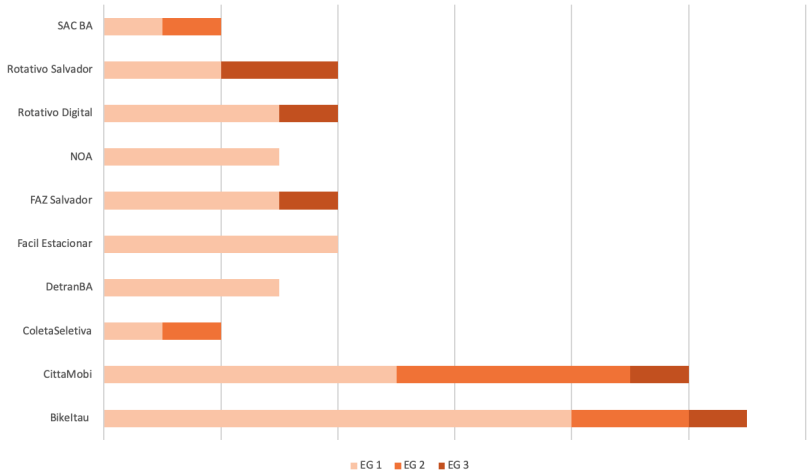

Gráfico 4: Detalhamento da EG por *apps*. Fonte: Autores, 2019.

É possível verificar, também, a relação entre as IM e a EG, conforme o Gráfico 5. Das dez categorias de IM encontradas no *corpus*, quatro se enquadram somente no nível leve (EG1) (*Sweet Seduction*, *Price Comparison Prevention*[14], *Immortal Accounts*[15] e *Confirmshaming*), três no nível moderado (EG2) (*Information Milking*, *Forced Registration* e API *Fest*) e seis no nível grave (EG3) (*Misdirection*[16], *Information Milking*, *Hidden Legalese Stipulations*, *Forced Registration*, *Bad Defaults* e API *Fest*). Embora apareça em uma variedade maior de IM, verificamos uma ocorrência maior de casos classificados como EG2 (Gráfico 3).

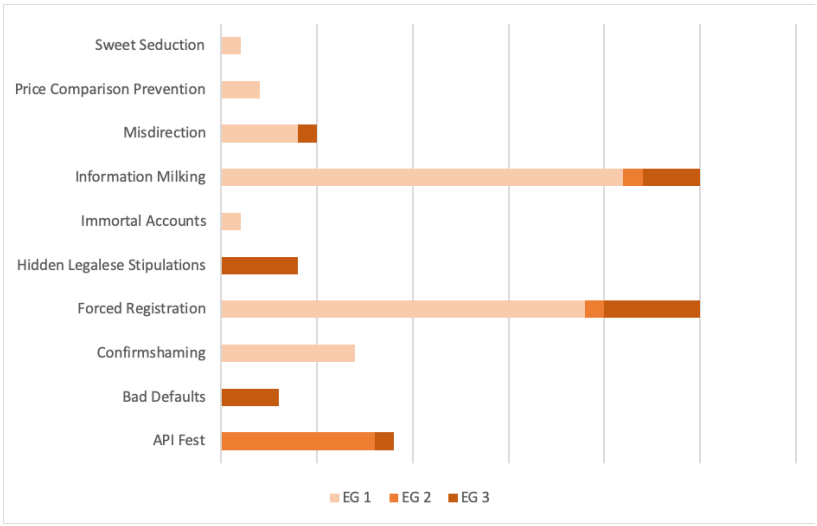

Gráfico 5: Detalhamento da EG por IM. Fonte: Autores, 2019.

Muitas das IM categorizadas na EG1 reforçam o argumento de sua naturalização, como a base do capitalismo de dados, dando início à cadeia de desenvolvimento de produtos e serviços dataficados. É cada vez mais comum encontrar websites e aplicativos que exigem cadastro de forma obrigatória (*Forced Registration*) e desenvolvam estratégias diversas para incentivar o usuário a fornecer seus dados (*Information Milking* e *Confirmshaming*). No nível EG2, há indícios de compartilhamento de dados com terceiros e os riscos à privacidade tendem a aumentar, gerando processos de perfilização (PONCIANO et al., 2017; SILVEIRA, 2018). Destaca-se, no EG2, a presença da IM API *Fest* com a utilização de APIs de terceiros, sem que se saiba com muita clareza as práticas de dado da empresa. Sua implementação mais "conservadora" está nos formulários de requisição de dados pessoais no momento do cadastro, conforme vimos anteriormente na Figura 4. É possível verificar outras instâncias de sua ocorrência na Figura 6.

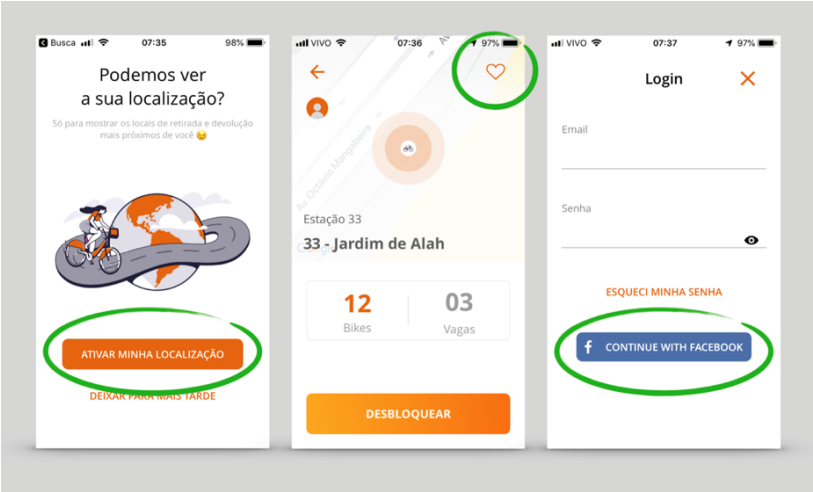

Fig. 6: *Information Milking* no *Bike* Itaú. Fonte: Autores, 2019.

A primeira tela solicita o acesso à geolocalização do usuário, com a promessa de otimizar o serviço e permitir a visualização das estações mais próximas. Na segunda, de forma mais sutil, temos a opção de *favoritar* uma determinada estação (ver detalhe em verde). Essa ação e a integração com a API do *Facebook* produzem maior granularidade na coleta de dados, enriquecendo o perfil do usuário e potencializando o valor do dado. Em todos os casos, há requisição de coleta de dados pessoais que não são estritamente essenciais para a realização do serviço e indícios de compartilhamento com terceiros.

6 Conclusão

Esse artigo analisou dez aplicativos em uso de interesse público na cidade de Salvador. Destacamos a discussão sobre a privacidade em meio à expansão da PDPA e o uso das *dark patterns* (DP), que propomos chamar de interfaces maliciosas (IM). Como mostramos na análise do *corpus*, todos os aplicativos têm IM, mesmo que em diferentes níveis de gravidade, demonstrando uma tendência a sua naturalização, como um processo de expansão da plataformização da sociedade, do processo de datificação e do agenciamento performativo dos algoritmos. O crescimento e avanço desses processos – como verificado através da análise das interfaces – aponta para a necessidade de politizar as novas formas de mediação da vida social urbana. Boa parte dos aplicativos analisados buscam atuar no relacionamento entre cidadão e cidade de alguma maneira, mediando e afetando a experiência na urbe. Essa nova sociabilidade urbana, portanto, torna-se alvo das estratégias de coleta e de produção de dados pessoais, tendo em vista seu valor no que tange a cultura digital marcada pela PDPA. Busca-se não só construir a informação como uma nova experiência urbana, mas também domesticar os usuários na prática cotidiana de produção dessas informações, alimentando o capitalismo de vigilância.

A pesquisa partiu de uma perspectiva pragmática e neomaterialista, analisando as ações geradas pela materialidade das interfaces e correlacionando-as à captação de dados sem a devida atenção dos usuários. A fim de criar um mecanismo de comparação e de ajuste dos graus de ameaça à privacidade, propomos a criação de uma Escala de Gravidade (EG) em três níveis (1 - leve, 2 - moderado, 3- grave). Resultante das análises da codificação das IM no *ATLAS.ti*, chegamos à conclusão de que 70% dos aplicativos estão no grau EG1. Os mais graves são os aplicativos *Cittamobi* e *Bike* Itaú, com os três níveis e os Rotativo Salvador, Rotativo Digital e Faz Salvador com os níveis E1 e E3.

A pesquisa aponta para a necessidade de novas etapas que permitirão traçar um quadro mais completo do uso das IM. Análises suplementares de documentos (de licitação do serviço, manual técnico dos aplicativos), conversa com desenvolvedores, *survey* com usuários, ampliação do *corpus* empírico, entre outras ações, devem ser realizadas em pesquisas futuras para uma melhor cartografia do problema.

É importante perceber como os diversos atores se posicionam em relação à questão da privacidade estabelecendo assim formas concretas de sua construção e discussão na sociedade digital contemporânea. Algumas questões emergem da pesquisa e apontam para uma discussão política e jurídica. Como a prefeitura, no caso em questão, fez a licitação desses aplicativos? Qual a sua visão da privacidade? Como os usuários foram chamados a participar (se foram)? Como essas plataformas vão se adaptar à LGPDP (Lei Geral de Proteção de Dados Pessoais)? Que tipo de pressão será exercida pelos usuários, já que são, compulsoriamente, obrigados a usar as plataformas para ações de cidadania?

Referencias

ALEXANDER, C.; ISHIKAWA, S.; SILVERSTEIN, M. **A Pattern Language:** Towns, Buildings, Construction. Nova Iorque: Oxford University Press, 1977.

ASH, J.; ANDERSON, B.; GORDON, R.; LANGLEY, P. Digital interface design and power: Friction, threshold, transition. **Environment and Planning D: Society and Space**, v. 36, n. 6, p. 1136-1153, 2018b. Disponível em: <http://journals.sagepub.com/doi/10.1177/0263775818767426>;. Acesso em: 28 jan. 2019.

ASH, J.; ANDERSON, B.; GORDON, R.; LANGLEY, P. Unit, vibration, tone: a post-phenomenological method for researching digital interfaces. **Cultural geographies**, v. 25, n. 1, p. 165-181, 2018a. Disponível em: <http://journals.sagepub.com/doi/10.1177/1474474017726556>;. Acesso em: 28 jan. 2019.

BRIGNULL, H. Dark Patterns: dirty tricks designers use to make people do stuff. **90 Percent of Everything.** 2010. [Blog] Disponível em: <https://www.90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/>;. Acesso em: 28 jan. 2019.

BÖSCH, C.; ERB, B.; KARGL; KOPP, H.; PFATTHEICHER, S.Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. **Privacy Enhancing Technologies**, n. 4, p. 237-254, 2016. Disponível em: <https://www.degruyter.com/view/j/popets.2016.2016.issue-4/popets-2016-0038/popets-2016-0038.xml>;. Acesso em: 28 jan. 2019.

BUCHER, T. The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms. **Information Communication and Society**, v. 20, n. 1, p. 30-44, 2017. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1154086>;. Acesso em: 28 jan. 2019.

CHUNG, E. S.; HONG, J. I.; LIN, J.; PRABAKER, M. K.; LANDAY, J. A.; LIU, A. L. Development and evaluation of emerging design patterns for ubiquitous computing. In: CONFERENCE ON DESIGNING INTERACTIVE SYSTEMS PROCESSES, PRACTICES, METHODS, AND TECHNIQUES, 5., 2004, Cambridge. **Proceedings ...** Nova Iorque: ACM, 2004. p. 233-242. Disponível em: <http://portal.acm.org/citation.cfm?doid=1013115.1013148>;. Acesso em: 12 jul. 2018.

COLESKY, M.; HOEPMAN, J. H.; HILLEN, C. A Critical Analysis of Privacy Design Strategies. In*:* IEEE SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS, 2016, San Jose. **Proceedings...** Disponível em: <https://ieeexplore.ieee.org/document/7527750>;. Acesso em: 12 jul. 2018.

DANAHER, J. The Threat of Algocracy: Reality, Resistance and Accommodation. **Philosophy and Technology**, v. 29, n. 3, p. 245-268, 2016.

DIAMANTOPOULOU, V.; KALLONIATIS, C.; GRITZALI, S.; MOURATIDIS, H. Supporting privacy by design using privacy process patterns. In*:* IFIP INTERNATIONAL CONFERENCE ON ICT SYSTEMS SECURITY AND PRIVACY PROTECTION, 2017, Rome. **Proceedings...** Disponível em: <https://link.springer.com/chapter/10.1007/978-3-319-58469-0_33>;. Acesso em: 12 jul. 2018.

DOTY, N.; GUPTA, M. Privacy Design Patterns and Anti-Patterns: Patterns Misapplied and Unintended Consequences. In: SYMPOSIUM ON USABLE PRIVACY AND SECURITY, 9., 2013, Newcastle. **Proceedings...** Disponível em: <https://dl.acm.org/citation.cfm?id=2501604>;. Acesso em: 12 jul. 2018.

FOX, N. J.; ALLDRED, P. **Sociology and the New Materialism:** Theory, Research, Action. Londres: SAGE Publications, 2017.

FRITSCH, L. Privacy dark patterns in identity management. In: FRITSCH, L.; ROßNAGEL, H.; HüHNLEIN, D. (Eds.). **Open Identity Summit 2017**. Bonn: Gesellschaft fÜr Informatik, 2013. p. 93-104. Disponível em: <https://dl.gi.de/handle/20.500.12116/3583>;. Acesso em: 12 jul. 2018.

GRAF, C.; WOLKERSTORFER, P.; GEVEN, A.; TSCHELIGI, M. A Pattern Collection for Privacy Enhancing Technology. In: INTERNATIONAL CONFERENCES OF PERVASIVE PATTERNS AND APPLICATIONS, 2., 2010, Lisboa. **Proceedings...** Disponível em: <http://www.thinkmind.org/index.php?view=instance&instance=PATTERNS+2010>;. Acesso em: 12 jul. 2018.

GRAY, C. M.; KOU, Y.; BATTLES, B.; HOGGATT, J.; TOOMBS, A. L. The Dark (Patterns) Side of UX Design. In: CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS - CHI '18, 2018, Montreal. **Proceedings...** Montreal: ACM Press, 2018. Disponível em: <http://dl.acm.org/citation.cfm?doid=3173574.3174108>;. Acesso em: 30 abr. 2019.

GREENBERG, S.; BORING, S.; VERMEULEN, J.; DOSTAL, J. Dark patterns in proxemic interactions. In: CONFERENCE ON DESIGNING INTERACTIVE SYSTEMS - DIS '14, 2014, Vancouver. **Proceedings...** Disponível em: <http://dl.acm.org/citation.cfm?doid=2598510.2598541>;. Acesso em: 30 abr. 2019.

HOEPMAN, J.H. Privacy Design Strategies. In: CUPPENS-BOULAHIA, N.; CUPPENS, F.; JAJODIA, S.; ABOU EL KALAM, A.; SANS, T. (Eds.). **ICT Systems Security and Privacy Protection:** SEC 2014. Berlim: Springer, 2014. p. 446-459. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-642-55415-5_38>;. Acesso em: 30 abr. 2019.

LACEY, C.; CAUDWELL, C. Cuteness as a 'Dark Pattern' in Home Robots. In: ACM/IEEE INTERNATIONAL CONFERENCE ON HUMAN-ROBOT INTERACTION 2019, Daegu-South Korea. **Proceedings...** Daegu-South Korea: IEEE, 2019. p. 374-381. Disponível em: <https://ieeexplore.ieee.org/document/8673274/>;. Acesso em: 30 abr. 2019.

LEMOS, A. **Epistemologia da Comunicação, Neomaterialismo e Cultura Digital.** [no prelo, 2019a]

LEMOS, A. **Plataformas, dataficação e performatividade algorítmica (PDPA):** Desafios atuais da cibercultura. [no prelo, 2019b.]

LEWIS, C. **Irresistible Apps**. Berkeley: Apress, 2014.

MATHUR, A.; ACAR, G.; FRIEDMAN, M. J.; LUCHERINI, E.; MAYER, J.; CHETTY, M.; NARAYANAN, A. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. **Proceedings ACM Human-Computer Interaction**, v. 1, 2019. Disponível em: <https://arxiv.org/abs/1907.07032>;. Acesso em: 18 Ago. 2019.

MAYER-SCHONBERGER, V.; CUKIER, K. **Big Data:** A Revolution That Will Transform How We Live, Work, And Think. Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2013.

NODDER, C. **Evil by Design:** Interaction Design to Lead Us into Temptation. Indianapolis: John Wiley & Sons, 2013.

PATRICK, A. S.; KENNY, S. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. In: DINGLEDINE R. (Ed.). **Privacy Enhancing Technologies - 2003:** Lecture Notes in Computer Science. Heidelberg: Springer, 2003. p. 107-124. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-540-40956-4_8>;. Acesso em: 30 abr. 2019.

PEARSON, S.; SHEN, Y. Context-aware privacy design pattern selection. In: INTERNATIONAL CONFERENCE ON TRUST, PRIVACY AND SECURITY IN DIGITAL BUSINESS, 7., 2010, Bilbao-Spain. **Proceedings...** Berlim/Heidelberg: Springer-Verlag, 2010. p. 69-80. Disponível em: <http://dl.acm.org/citation.cfm?id=1894888.1894898>;. Acesso em: 12 jul. 2018.

PONCIANO, L.; BARBOSA, P.; BRASILEIRO, F.; BRITO, A.; ANDRADE, N. Designing for Pragmatists and Fundamentalists: Privacy Concerns and Attitudes on the Internet of Things. In: BRAZILIAN SYMPOSIUM ON HUMAN FACTORS IN COMPUTING SYSTEMS (IHC'17), 16., 2017, Joinville. **Proceedings...** Disponível em: <http://arxiv.org/abs/1708.05905>;. Acesso em: 12 jul. 2018.

SADOWSKI, J. When data is capital: Datafication, accumulation, and extraction. **Big Data & Society**, v. 6, n. 1, p. 1-12, 2019.

SILVEIRA, S. A. **Tudo sobre Tod@s:** Redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições Sesc SP, 2018.

SRNICEK, N. **Platform capitalism**. Cambridge: Polity Press, 2017.

TRICE, M.; POTTS, L. Building Dark Patterns into Platforms: How GamerGate Perturbed Twitter's User Experience - Present Tense. **Present Tense: A Journal of Rhetoric in Society**, v. 6, n. 3, p. 1, 2018. Disponível em: <https://www.presenttensejournal.org/volume-6/building-dark-patterns-into-platforms-how-gamergate-perturbed-twitters-user-experience/>;. Acesso em: 12 jul. 2018.

VAN DIJCK, J.; POELL, T.; DE WAAL, M. **The Platform Society**. Nova iorque: Oxford University Press, 2018.

WILLIAMS, M.; NURSE, J. R. C.; CREESE, S. The perfect storm: The privacy paradox and the Internet-of-things. In: INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY, 11., 2016, Salzburg-Áustria. **Proceedings...** Disponível em: <https://ieeexplore.ieee.org/document/7784629>;. Acesso em: 12 jul. 2018.

ZAGAL, J. P.; BJÖRK, S.; LEWIS, C. Dark Patterns in the Design of Games. In: FDG 2013 - INTERNATIONAL CONFERENCE ON THE FOUNDATIONS OF DIGITAL GAMES, 8., 2013, Chania-Grácia. **Proceedings...** Disponível em: <http://www.fdg2013.org/program/papers.html>;. Acesso em: 12 jul. 2018.

ZUBOFF, S. Big other: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v. 30, n. 1, p. 75-89, 2015.

---

1 Disponível em: youtube.com/watch?v=zaubGV2OG5U

2 A instrumentalização dos padrões de design foi postulada pelo arquiteto Christopher Alexander (1977) para criar uma linguagem universal para a arquitetura. A popularização do seu trabalho motivou outros campos, como a engenharia de software e o design de interação.

3 Disponível em: ft.com/content/e24dea0a-6b57-11e9-80c7-60ee53e6681d.

4 Disponível em: gizmodo.com/senators-introduce-bill-to-stop-dark-patterns-huge-plat-1833929276.

5 Disponível em: nytimes.com/2016/05/15/technology/personaltech/when-websites-wont-take-no-for-an-answer.html.

6 Disponível em: theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you.

7 Disponível em: https://www.darkpatterns.org/types-of-dark-pattern.

8 Acrônimo para os *Big Five*: *Google*, *Amazon*, *Facebook*, *Apple* e *Microsoft*.

9 Disponível em: https://bikeitau.com.br/bikesalvador/politica-de-privacidade/.

10 As telas foram capturas e importadas para o software. Não há isonomia na quantidade de capturas. A codificação focada identificou as IM. Nem todas as IM descritas pela literatura dizem respeito a problemas de privacidade, consequentemente, nem todas aparecem no *corpus*.

11 Parceria entre a Prefeitura Municipal de Salvador e o banco Itaú. Os usuários podem utilizar 400 bicicletas espalhadas por 50 estações. Ele é um mediador para realizar pagamento do serviço (planos diários, mensais e anuais), localizar a estação mais próxima e efetivar o empréstimo da bicicleta.

12 Podemos encontrar exemplos em diversas fontes, como o site oficial de Brignull (darkpatterns.org/hall-of-shame), perfil do projeto no Twitter (twitter.com/darkpatterns), comunidade desenvolvida por pesquisadores (dark.privacypatterns.eu), comunidades no Reddit dedicadas ao tema (reddit.com/r/darkpatterns/) (reddit.com/r/assholedesign/). Alguns outros artigos contribuíram para a expansão do catálogo de IM, como Bosch, et al. (2016) e Gray, et al. (2018).

13 Estudos recentes corroboram essa afirmação. Arunesh Mathur, et al. (2019) demonstraram a presença de IM em 11,1% de aproximadamente 11.000 *websites* de compra *online analisados*. A análise revelou a ação de serviços online que oferecem a implementação de IM em sites de compra, no formato de *plugins* e *add-ons*. Esses serviços são divulgados abertamente como formas de impulsionar as vendas.

14 Estratégias de interação que dificultem a realização de comparações de preço por parte dos consumidores. Embora seja mais comum em cenários de *e-commerce*, verificamos a presença de *Price Comparison Prevention* em *apps* presentes no *corpus* desta pesquisa que lidam com a venda de pacotes de serviços.

15 O usuário é impedido de encerrar o serviço contratado ou cancelar sua conta em determinado *app* ou *website*. Empresas tendem a impor obstáculos para que os usuários mantenham seus dados atrelados à plataforma.

16 O objetivo desta IM é desviar a atenção do usuário de aspectos da interface que não são do interesse da empresa, ou direcionar o olhar ou ação para a realização da tarefa prescrita no programa de ação.