PROGRAMAR É PODER: CONTRADIÇÕES ENTRE AS DIMENSÕES COMUNICACIONAL E TECNOLÓGICA DA CRIPTOGRAFIA DE PONTA-A-PONTA DO WHATSAPP[1]

Affordance is power: contradictions between communicational and technical dimensions of whatsapp's end-to-end encryption

Programar es poder: contradicciones entre las dimensiones comunicacional y tecnológica del cifrado de extremo a extremo del whatsapp

Marcelo Santos
Universidade Finis Terrae
msantos@uft.cl

Antoine Faure
Universidade Finis Terrae

Resumo

Este estudo analisa criticamente a implementação da criptografia de ponta-a-ponta no aplicativo de mensageria instantânea WhatsApp, suportado pela teoria das *affordances*, empiricamente desenvolvido em base ao framework "biografia de plataformas". Depois de apontar as contradições com as evidências levantadas, concluímos que a implementação deve ser interpretada como um movimento estratégico inserido em: (i) uma tática de guerrilha de Relações Públicas do WhatsApp Inc. contra estados nacionais em que se revela (ii) a programação como uma demonstração de poder da corporação de mídia digital para evitar conflitos políticos com os mesmos em que subsiste (iii) um balanço tipo custo-benefício em que prima a massividade comercial em detrimento da utopia tecnológica.

Palavras-Chave: Criptografia. WhatsApp. Affordances.

[1] Este artigo é uma versão traduzida, atualizada e adaptada de um artigo previamente publicado na revista Social Media & Society: Santos, M. & Faure, A. (2018) Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption. *Social Media & Society*. 4(3). https://doi.org/10.1177/2056305118795876

Abstract

The present study analyses critically the roll-out of the end-to-end encryption on WhatsApp, supported by Affordances Theory, guided by the "platform biography" framework that points to a historical perspective of the App. After pointing out the contradictions with evidences from the empirical work, we conclude that the implementation of such affordance should be interpreted as a strategic move inscribed in: (i) a guerrilla Public Relations war between WhatsApp Inc. against national states in which is revealed (ii) a power move by the digital media corporation to avoid political conflicts with them and that (iii) a cost-benefit approach leads to the prevalence of commercial massiveness at the expense of technological utopia.

Keywords: Encryption. WhatsApp. Affordances

Resumen

Este estudio analiza críticamente la implementación del cifrado de extremo a extremo de la aplicación WhatsApp, en base a la teoría de las *affordances*, bajo la perspectiva del historial de la aplicación, siguiendo el modelo de pesquisa "biografía de plataformas". Tras apuntar las contradicciones con las evidencias levantadas, concluimos que la implementación debe ser interpretada como un movimiento estratégico insertado en: (i) una táctica de guerrilla de Relaciones Públicas de WhatsApp Inc. en contra de los estados nacionales en que se revela (ii) una demostración de poder de la corporación de medios digitales para evitar conflictos políticos con los mismos y que subsiste (iii) un balance tipo costo-beneficio en que prima la masividad comercial en detrimento de la utopia tecnológica.

Palabras-Chave: Encriptación. WhatsApp. Affordances

CONTEXTO

Às 0:00 horas de 17 de dezembro de 2015, a população brasileira foi impedida de acessar regularmente o WhatsApp. Motivado pelo descumprimento de uma ordem judicial por parte da empresa, que se negou a compartilhar as mensagens de um criminoso que vinha sendo investigado, uma juíza ordenou aos provedores de serviço (ISP) a interrupção do acesso à aplicação no território nacional por 48 horas[2]. O resultado foi um blecaute[3] nacional que durou ao redor de 12 horas durante o qual aproximadamente 100 milhões de usuários da aplicação (10% dos usuários mundiais neste então) não tinham como acessá-la, até que os advogados que representam a companhia conseguiram reverter a decisão judicial e liberar o acesso. O centro da disputa foi a persistência do governo brasileiro em solicitar o conteúdo das conversas entre suspeitos de uma investigação criminal importante. A companhia, desde então, se mantém ancorada no argumento técnico de que não tem acesso às mensagens dos usuários, portanto seria impossível colaborar com a justiça em tais termos. O próprio Jan Koum, um dos fundadores da aplicação, disse pessoalmente durante uma entrevista anterior ao bloqueio: "Não tem nenhuma chave para ser entregue [para a NSA[4]] (...) Nós não guardamos mensagens nos nossos servidores, não armazenamos o histórico de suas conversas. Elas estão todas no seu telefone" (Rowan, 2014, par 15).

De uma forma ou de outra, o debate segue vigente no Brasil (STF, 2017) e diversas outras tentativas foram feitas a posteriori para bloquear novamente o serviço, sendo outras duas bem sucedidas, e o bloqueio mais longo com a duração de 24 horas em 2016[5] (Abreu 2017). Alguns meses após o primeiro bloqueio em 2015 – e a respectiva controvérsia que o acompanhou – o

[2] *Justiça manda bloquear WhatsApp por 48 horas a partir desta quinta-feira* (EBC Website). Disponível em http://agenciabrasil.ebc.com.br/geral/noticia/2015-12/justica-manda-bloquear-whatsapp-por-48-horas-partir-desta-quinta-feira, recuperado em 26 de dezembro de 2017.
[3] Não foi um blecaute total, já que algumas pessoas contornaram o bloqueio através do uso de uma VPN ou similar, enganando os ISPs.
[4] National Security Agency, agência de segurança governamental dos Estados Unidos.
[5] Mais informação no site www.bloqueios.info. Recuperado em 15 de junho de 2018.

WhtatsApp finalizou a implementação de uma nova *affordance*[6] que operacionaliza definitivamente a impossibilidade técnica de compartilhar as conversas dos usuários com as autoridades: criptografia de ponta-a-ponta, para todas as mensagens e formatos multimídia. No entanto, um detalhe do processo de implementação chamou a atenção: o WhatsApp optou por enviar uma mensagem a ambos usuários envolvidos em cada conversa, avisando-os que sua conversa estava doravante criptografada com a nova tecnologia (ver Figura 1), apesar de que evidentemente a grande maioria dos usuários não entende muito bem o que isto significa. Seguindo Dencik e Leistert (2015) almejamos "escrutinizar propriamente" esta história e identificar os processos e motivações detrás não apenas desta decisão (implementar a funcionalidade) mas do processo (mensagem avisando os usuários).

[6] A tradução utilizada para o termo "affordances" é a expressão "funcionalidade". Ao longo deste texto, ambas expressões serão usadas com o sentido mais amplo que carrega a primeira, na falta de uma tradução literal satisfatória em português para o termo *affordances*.

Figura 1. Mensagem comunicando a implementação da criptografia de ponta-a-ponta no WhatsApp (Fonte: Adaptada de www.techtudo.com.br)

Este estudo se inserta, portanto, no campo dos estudos críticos de internet, o qual "sempre situa tais análises [empíricas] ao teorizar e analisar contextos mais amplos, como as estruturas de poder, o estado, o capitalismo, relações de gênero, conflitos sociais e ideologias, que dão forma e são informados pelo ecossistema de mídias em processos dialéticos" (Trottier e Fuchs, 2015, p. 3, tradução livre). Para levar a cabo esta análise crítica, primeiro contextualizaremos como tais questões emergem, para então explorar o conceito de *affordances* – aqui traduzido por *funcionalidades* – e como ambos se relacionam com disputas de poder. Em seguida, explicaremos o método usado e como recolhemos evidencias para suportar uma explicação plausível para as questões levantadas. Finalmente, analisaremos as evidências em torno aos temas de privacidade e segurança em duas dimensões: *comunicacional* (auto-representação da companhia, resenhas técnicas de mídia especializada e entrevistas que aludem aos temas) e *tecnológica* (evidências em base a resenhas específicas da criptografia por parte de expertos do campo e de navegação na aplicação por parte dos autores). Na última seção sintetizamos as conclusões.

Privacidade e Segurança em TICs

Privacidade e segurança nas redes digitais são temas centrais no âmbito da vida digital contemporânea, particularmente após o escândalo de vazamento de dados do Facebook conhecido como Cambridge Analytica (Cadwalladr e Graham-Harrison, 2018). Ambas questões dizem respeito, de forma praticamente inseparável, à forma como as possibilidades de vigilância tem sido irradiadas através da vida digital tanto em fragmentos complementários de discos rígidos distribuídos como na individualização vinculada à proliferação de aplicativos de telefonia móvel. Parece que a vida digital se enquadra com a sociedade de controle tal como proposta pelo filósofo Gilles Deleuze, "provendo a posição de qualquer elemento em um ambiente aberto e em qualquer instante (...) e rastreando a posição de cada pessoa – lícita ou ilicitamente – e efetivando uma modulação universal" (Deleuze, 1992, p. 7, tradução livre). Em outras palavras, a vida digital operacionaliza o controle como uma modulação, "como um gesso auto-deformante que muda constantemente de um momento ao outro" (Deleuze, 1992, p. 4, tradução livre). E ao ativar

tal controle, funciona através de códigos e senhas que criptografam e descriptografam a informação.

A discussão sobre privacidade e segurança ganhou profundidade nos últimos tempos, em especial após as revelações de Edward Snowden durante 2013, vazando as (condenáveis) práticas de espionagem de agências de governos como o estadunidense e o britânico, em colaboração com empresas como Microsoft, Apple, Google, Verizon entre outras (Greenwald, 2013; Greenwald e MacAskill, 2013; Scriberia et al., 2013). No esteio de tais revelações, o próprio Snowden fez uma explícita recomendação apresentando a aplicação Signal como o paradigma de App de mensageria instantânea em termos de segurança e privacidade (Cimpanu, 2015).

Desde então, prima a desconfiança ao analisar estratégias discursivas de marketing que vendem a ideia de entidades privadas, com fins de lucro, como guardiães auto-designados da privacidade cidadã no âmbito digital. De forma análoga à presente análise, Hintz (2015) critica a crescente autonomia com que as mídias sociais, entidades privadas com fins de lucro, têm regulado seu *conteúdo* – tal como censura à nudez no Facebook, ao conteúdo com direitos de autor no YouTube e ao conteúdo "adulto" no Tumblr, como a recente polêmica que levou Apple a retirar este de sua AppStore (Liao, 2018) – e seus *usuários* – como o cesse de serviços arbitrário da Amazon contra o Wikileaks – que não são de forma alguma decisões apolíticas: "o estado terceiriza para as plataformas as intervenções na comunicação dos cidadãos" (Hintz, 2015, p. 110, tradução livre). As decisões que tomam as empresas neste contexto informam a cultura digital e potencialmente restringem a ação política da sociedade civil, levando a disputas sócio-políticas como a que vamos analisar neste estudo.

FUNCIONALIDADES E PODER

Funcionalidades (*Affordances*)

Seguindo Langlois (2014), "tanto as práticas que levam a fazer sentido como a substância do próprio sentido são materiais e tecnológicas em primeiro lugar, e os contextos tecnológico e material determinam o que constitui o sentido e o sem-sentido" (p. 9, tradução livre). *Affordances*, portanto, produzem *sentido* e *sem-sentido* de duas formas. Primeiro ao "instalar as condições segundo as quais o sentido e o sem-sentido aparecem" (Langlois, 2014, p. 11, tradução

livre). A segunda é uma forma ainda mais sutil que a funcionalidade em si como determinante de limites e potencial para comunicação e construção de sentido dentro do software: é o processo de implementação de tal funcionalidade, superando o espectro tecnológico e podendo chegar a ter, como veremos, implicações sociais e políticas.

De acordo com J. J. Gibson (1977, conforme citado por Norman, 1999), a quem o termo é atribuído, *affordances* são relações que resultam de "propriedades acionáveis entre o mundo e um ator (pessoa ou animal)" (p. 39, tradução livre). Em outras palavras, as propriedades de um ambiente abrem possibilidades que são condizentes com cada organismo:

> A funcionalidade de algo não muda na medida em que a necessidade do observador muda. O observador pode ou não perceber e acudir à funcionalidade, de acordo às suas necessidades, mas a funcionalidade em si, ao ser invariante, está presente para ser percebida. (Gibson, 1986, p. 139, tradução livre)

Norman (1999) aplicou o conceito para interfaces mecânicas e eletrônicas, dividindo-o em três diferentes estágios: (1) funcionalidades percebidas, (2) retroalimentação do sistema e (3) as funcionalidades em si. A primeira diz respeito aos *signos visuais* (melhor seriam signos *sensoriais*, para ser mais preciso e atualizar a discussão) que indicam que existe uma funcionalidade detrás da interface, como um botão, uma imagem, um gesto, um comando de voz e assim por diante. Tais signos são parte fundamental do design de TICs, já que o usuário os necessita para identificar uma funcionalidade no sistema, indicando que deve clicar, apertar, mexer os dedos, falar etc. A ausência de tais signos pode ter como consequência a impossibilidade de identificação da funcionalidade por parte dos usuários do software, por mais que a funcionalidade, como afirma Gibson (1986), seja "invariante" e esteja sempre "presente para ser percebida". O segundo elemento, *retroalimentação*, diz respeito aos signos que denunciam a operação da funcionalidade, seu funcionamento, tal como ícones em movimento que indicam que uma aplicação está sendo carregada ou que o software está buscando resultados. Finalmente, as *funcionalidades em si* são o programa que permite ou restringe a gama de ações do usuário, e podem ou não estar acompanhada por um ou por ambos outros elementos. De fato, "as funcionalidades, a retroalimentação, e as funcionalidades percebidas podem ser manipuladas de forma independente umas das outras" (Norman, 1999, p. 40, tradução livre).

Hutchby (2001) desenvolveu um marco de trabalho com funcionalidades com o objetivo de analisar tecnologias entre duas tradições: determinismo e construtivismo. De acordo com o autor, as funcionalidades abordam as possibilidades e restrições que a materialidade de todo objeto oferece graças a suas características próprias. Portanto, tal como teoria de meios (Meyrowitz, 1994) e a abordagem das materialidades (Lévrier e Wrona, 2013) ressaltam, as funcionalidades condicionam o uso de forças sociais. Em consequência, a dimensão política das funcionalidades tributa a um tipo de enquadre, isto é, uma ação que restringe e habilita, ademais de seu próprio uso, interpretações sobre si. Este é um dos cruzamentos entre teoria das *affordances* com o campo da comunicação, em que o enquadre pode ser interpretado como um mecanismo de persuasão indireta que corresponde à forma em que uma mensagem (ou, no caso, uma funcionalidade) é exibida e/ou introduzida ao usuário.

Poder

Como relacionar funcionalidades, política e poder? Sugerimos que esta problemática reside para além do discurso, incorporando precisamente o componente tecnológico de sua transformação, tal como proposto pela teoria das *affordances*. Gillespie (2010) analisa o papel de tecnologias digitais na vida contemporânea, subjacente ao discurso de neutralidade das plataformas e aplicações, afirmando que aí residem "as tensões inerentes de seu serviço" (p. 348, tradução livre). Em outra palavras, neste campo, parte das disputas de poder se evidencia nas funcionalidades, mas também nas estratégias de representação das próprias tecnologias, que apela às projeções que buscam, às suas imagens desejadas ante o público. Não obstante, a tecnologia não se restringe apenas a ser o suporte do discurso; é também o discurso do suporte (Lévrier e Wrona, 2013, p. 7).

No âmbito das plataformas, usuários e poder, no entanto, a questão do agenciamento é complexa. Na medida que usuários ordinários são os criadores do conteúdo que habita e viaja na maior parte destas plataformas, os mesmos se convertem, provavelmente, nos agentes mais visíveis daquilo que na superfície, são mídias neutras chamadas de "plataformas" (Gillespie, 2010). No entanto, os usuários não são os únicos e definitivamente não são os mais poderosos agentes neste campo: "Os donos das plataformas e os desenvolvedores de Apps são agentes produtores e forças sociais; eles podem exercer seu poder econômico e político para alterar ou

sustentar hierarquias existentes e, para tal fim, desenvolvem suas tecnologias" (van Dijck, 2013, p. 18, tradução livre). Concordamos com van Dijck (2009) que, em face de tamanha complexidade, "uma aproximação multidisciplinar para o agenciamento dos usuários deveria gerar um modelo que de conta dos múltiplos papéis que os usuários têm, ao mesmo tempo que *dá conta dos operadores das tecnologias e sites – proprietários como atores que manipulam a agência dos usuários*" (p. 55, nossa ênfase, tradução livre). Portanto propomos estudar plataformas e Apps não apenas desse uma perspectiva de cima para baixo, mas também considerando sua essência profunda, tal como revelada por uma análise precisa da evolução de suas funcionalidades. Nesta linha, cada funcionalidade de uma plataforma ou aplicação deve ser situada no momento preciso de sua análise política, de forma a abrir a conclusão para os aspectos estéticos, materiais, práticos e discursivos que enquadram a percepção de seus usuários, seu imaginário e a apropriação que fazem de tais tecnologias de informação.

A Teoria Ator-Rede (TAR) ajuda a situar agentes não humanos neste contexto, como mostra a definição de software de Langlois (2014), que destaca seu papel comunicacional:

> um novo tipo de ator comunicacional, como uma entidade que produz sentidos e expressividade, uma entidade que interage conosco. Incrustados nestas interações (...) está, com frequência, o interesse especifico das plataformas de mídia social, em particular aquelas com fim de lucro. (Langlois, 2014, p. 52)

Sob este ponto de vista, o poder não é visto como algo abstrato que paira sobre a vida digital, mas sim como uma hegemonia socioeconômica que afeta a distribuição de poder nos âmbitos político, econômico e cultural nas sociedades, gerando disputas que transpassam das fronteiras off-line às online e vice-versa. Neste estudo, no entanto, não adentramos as questões de caráter econômico mais profundas, pese a sua relevância, e sim focamos nas disputas de poder político que escondem as funcionalidades de plataformas, usando a criptografia do WhatsApp como um estudo de caso.

MÉTODO

O método aplicado para este estudo é derivado do framework *Platform Biography* de Burgess e Baym (2016), um modelo ao mesmo tempo sistemático e serendipitoso para analisar plataformas digitais que aplica uma variedade de fontes secundarias para circunscrever a

evolução do objeto de estudo como uma forma de "dar sentido à sua complexidade e à forma como se altera ao longo do tempo" (Burgess e Baym, 2017). Tal método defende que "os traços culturais distintivos das plataformas de mídia social devem muito à particularidade de seus principais objetos sócio-técnicos. Embora a presente pesquisa não busca esgotar a análise do WhatsApp enquanto plataforma, ela oferece uma explicação plausível para a visibilização da criptografia ponta-a-ponta implementada em abril de 2016. Se bem não é uma funcionalidade central para a operação cotidiana de usuários comuns da aplicação, consideramos que esta é altamente significativa considerando o momento histórico no tocante à privacidade e segurança, na medida em que se vem convertendo em questões centrais nos debates contemporâneos sobre a dimensão política da tecnologia. Isto fica evidente nos conflitos recentes entre serviços de mensageria instantânea que usam criptografia e governos que demandam acesso à informação que circula na App: Brasil (2015, 2016) e Irã (2014) com WhatsApp; Irã e Rússia a partir de 2018.

Para compreender a implementação de tal funcionalidade, os processos adjuntos e a análise crítica dos mesmos, analisamos comparativamente representações da App com as funcionalidades. Em outras palavras, confrontamos e contrastamos o *discurso comunicacional* em torno à tecnologia e a *análise técnica*, ambos detalhados a seguir.

Perspectiva Comunicacional

Os objetivos da análise sob a perspectiva *comunicacional* são: (i) comparar os valores prevalentes da companhia, tal como documentados pela mesma e/ou por outras fontes *antes* e *depois* da implementação da criptografia e (ii) estabelecer um ponto de comparação com a aplicação Signal, paradigma de segurança e privacidade em Apps de mensageria instantânea, de forma a evidenciar as diferenças entre ambas. Usamos tanto fontes de auto-representação (como a aplicação se define, se qualifica, se descreve etc.), como representações da mídia que tangenciassem os temas de privacidade e segurança. As fontes consultadas foram as seguintes[7]:

[7] Se bem tentamos contatar a empresa para indagar algumas das questões levantadas, não houve resposta por parte da mesma até o momento da escritura deste artigo.

- *Internet Archive*: mapeamos sistematicamente as mudanças nos sites do WhatsApp e do Signal, com especial atenção à página inicial e às páginas com algum tipo de auto-representação, como por exemplo ‘sobre nós’;
- Blog do WhatsApp;
- Entrevistas de mídia com os fundadores e/ou outros representantes da aplicação;
- Comentários de executivos do aplicativo na mídia social;
- Reportagens de mídia especializada sobre o WhatsApp e/ou seus fundadores.

Perspectiva das Funcionalidades (*Affordances*)

Os objetivos desta perspectiva são: (i) explorar comparativamente as funcionalidades relacionadas com privacidade e segurança do WhatsApp com funcionalidades equivalentes de aplicativos similares como Signal, Telegram e Facebook Messenger; (ii) avaliar a validez da implementação da criptografia a partir da análise de expertos em privacidade e segurança. Desta forma buscamos validar se o discurso corporativo e a percepção da mídia em geral em relação à criptografia se materializa como funcionalidade – ou não. As fontes consultadas foram as seguintes:

- Navegação no aplicativo pelos autores (WhatsApp), centrada nas funcionalidades específicas relacionadas com aspectos de privacidade e segurança (criptografia, mensagens secretas, capturas de tela etc.);
- Navegação no aplicativo pelos autores, similar ao anterior, só que nos aplicativos similares: Signal, Telegram e Facebook Messenger;
- Análise segundo opiniões de expertos em meios especializados, blogs ou sites organizacionais, com destaque para a *Electronic Frontier Foundation* (EFF), reconhecidos especialistas mundiais em privacidade e segurança digital.

Os resultados serão apresentados como perspectivas *Comunicacional* e *Tecnológica* na próxima seção. No entanto, antes se faz necessário um breve levantamento biográfico do WhatsApp para aprofundar o contexto da análise.

ANÁLISE

Breve biografia do WhatsApp

WhatsApp é um serviço de mensageria móvel fundado em 2009 por dois ex-funcionários do Yahoo: Jan Koum e Brian Acton. A ideia original, no entanto, foi do ucraniano Koum, quem deixou seu país ainda no fim da adolescência. Aquilo que era inicialmente um aplicativo de 'status update' evoluiu rapidamente para a forma atual de mensageria instantânea multimídia incluindo chamadas de áudio e vídeo *over the top*, ou seja, usando a infraestrutura existente do tráfego de dados via ISPs. Não obstante, o discurso se manteve em um tom bastante técnico ao longo dos anos, distante de qualquer preocupação evidente com a privacidade dos usuários. Em Abril de 2010, por exemplo, o site do aplicativo incluía a seguinte definição:

> WhatsApp Messenger é um aplicativo de mensageria que te permite o intercambio de mensagens com seus amigos e contatos sem ter que pagar tarifas de SMS. WhatsApp Messenger é inter-plataforma (...) Para enviar e receber mensagens, WhatsApp utiliza o plano de internet que você já dispõe para seu telefone inteligente. (Site antigo do WhatsApp acessado via Web Archive)

Como veremos, ao longo do tempo não se altera esta tônica e segurança e privacidade não aparecem como preocupações centrais de WhatsApp Inc.

Perspectiva Comunicacional

Auto-Representações

A continuação compararemos as estratégias comunicacionais do WhatsApp e do Signal – a aplicação paradigmática em termos de segurança e privacidade, recomendada por Edward Snowden. O objetivo é explicitar as contradições entre o discurso recente do WhatsApp advogando pela importância e a relevância da privacidade e da segurança para a empresa e o discurso histórico de ambos aplicativos.

Signal é o resultado da fusão de dois aplicativos de comunicação previamente existentes, chamados *RedPhone* e *TextSecure*, todos produtos da Open Whisper Systems. Não só os próprios nomes já dizem muito, mas o logo do aplicativo está claramente centrado em torno à ideia de segredo, ou melhor, de uma conversa protegida (veja Figura 2).

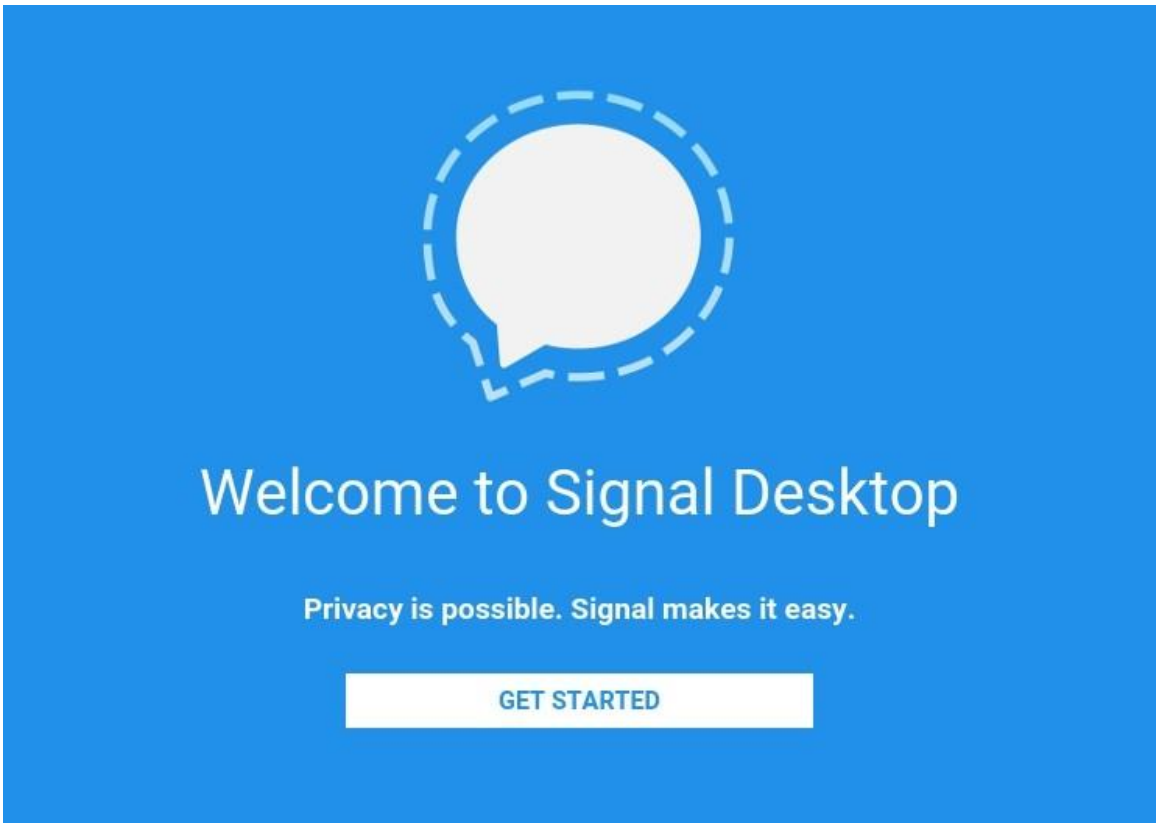

Figura 2: O logo da App Signal enfatiza a privacidade e a segurança (Fonte: Softpedia.com).

A página de bem-vindo da App não tem rodeios: "Privacidade é possível. Signal a torna fácil" (ver Figura 2, tradução livre). A través da aproximação biográfica, ao observar criticamente a estratégia discursiva detrás deste aplicativo, se evidencia sem dificuldade a preocupação institucional com privacidade e segurança na própria gênese do software – algo que não foi observado na análise do WhatsApp. Site, slogan, logotipo, nomes, todos estes elementos comunicativos em torno ao aplicativo remetem à ideia de que Signal prioriza a privacidade das mensagens intercambiadas no serviço por sobre qualquer outro valor. Em 2015, o título do site da organização Open Whisper Systems apontava para âmago da empresa: "Segurança, Simplificada. Segurança de código aberto para dispositivos móveis" (tradução livre a partir de Archive.org). Em 2016, a página corporativa tinha sido atualizada com a mensagem "Privacidade que cabe no seu bolso", unindo tecnologia móvel com privacidade – além, claro, do jogo de palavras em relação ao preço.

Por outro lado, analisando as diferentes versões do site do WhatsApp ao longo dos anos, desde sua criação, não observamos uma tradição de valorização ou preocupação com segurança e privacidade. A evidência biográfica do site aponta para outros valores como o cerne da organização – ao menos desde a perspectiva a auto-representação – como pode ser visto a seguir:

Tabela 1. Auto-representação do WhatsApp ao longo do tempo de acordo com seu website (Fonte: Adaptado de Archive.org).

Data	Auto-representação	Interpretação
2009	"WhatsApp é uma Agenda de Endereços mais inteligente para seu telefone inteligente"	Ideia de "status update"
2010	"WhatsApp é um aplicativo de mensageria/conversa de smartphone a smartphone"	Interoperabilidade e serviço de chat
Early 2011	"Rápido. Pessoal. Incrível."	Eficiência técnica, valores culturais contemporâneos
Late 2011	"Incrível. Interplataforma. Agora com conversas grupais"	Melhoria técnica das funcionalidades
2012	Simples. Pessoal. Mensagens em tempo real."	Acessibilidade, individualidade e velocidade

Finalmente, entre 2013 e 2015, houve poucas alterações, com foco nos aspectos visuais do site em vez do conteúdo, o que nos mostra que a companhia manteve privacidade e segurança como valores secundários em sua apresentação. Permutam palavras-chave como: simples, pessoal, tempo real, confiável, interplataforma, grátis, rápido, incrível. As motivações detrás do empreendimento, como demonstra a Figura 3 a continuação, apontam para uma visão muito mais dirigida ao tecno-otimismo que para uma cruzada em defesa da privacidade e da segurança, como dá a entender o discurso recente.

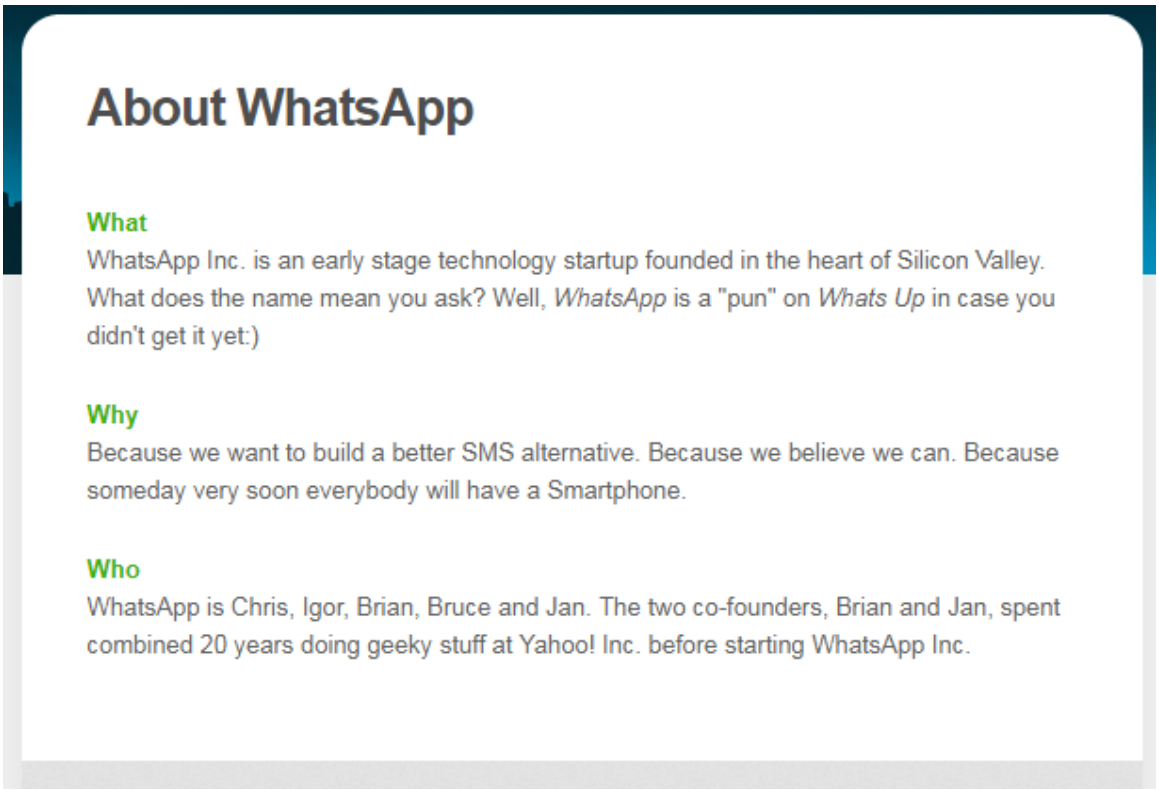

Figura 3: Captura de tela do site do WhatsApp em 2009 mostra a primeira página de 'Sobre Nós' (Fonte: Archive.org).

Representação na mídia

A mídia especializada parece convencida de que a privacidade é efetivamente uma preocupação central para o WhatsApp. Ou ao menos era, até sua aquisição por parte do Facebook em 2014. Seus fundadores foram chamados de "defensores devotos da privacidade" (Statt, 2018, par 5, tradução livre) e "grandes adeptos da privacidade" (Dwoskin, 2018, tradução livre). Neste contexto, o compartilhamento de dados com o Facebook representa, para o autor Henry Burrell (2017) do portal TechAdvisor, "um pequeno, mas significativo sinal de que o WhatsApp, agora propriedade do Facebook, está sendo obrigado a ceder em alguns dos seus valores relacionados à privacidade" (par 42, tradução livre). O mesmo autor defende que a empresa instalou a criptografia ponta-a-ponta "porque como companhia eles acreditam no seu direito a ter conversas privadas quando usa seu serviço" (Burrell, 2017, par 33, tradução livre).

Tal histórico de preocupação com privacidade e segurança é reforçado pela fábula do 'sonho americano' em que a terra da liberdade e das oportunidades recebe o jovem oprimido

ucraniano, que se converte em outro exemplo meritório de sucesso no paraíso democrático. Ironias à parte, na mesma semana que o Facebook anunciou a aquisição do WhatsApp, a revista Wired publicou uma entrevista com Jan Koum, na qual podemos ver melhor suas expectativas e seus valores pessoais: "As pessoas nos têm que diferenciar [o WhatsApp] de companhias como Yahoo! e Facebook que coletam e armazenam seus dados em seus servidores" (citado por Rowan, 2014, par 15, tradução livre). Outra declaração de Koum, na mesma entrevista, deixa entrever a inspiração que leva a criptografar o aplicativo: "[Koum] tinha apenas três regras que o acompanhavam em seus empreendimentos iniciais: seu serviço desafiadoramente não teria publicidade (...); *não armazenaria mensagens para não por em risco a privacidade dos cidadãos*; e manteria um foco incansável em entregar uma experiência de usuário fluida, confiável, sem dificuldades" (Rowan, 2014, par 3, ênfase nossa, tradução livre). Se o Facebook deve ser considerado o único culpado pelos desvios nas políticas e funcionalidades relacionadas à privacidade, é uma pergunta a ser desvelada no futuro, mas a saída de ambos fundadores da empresa é sintomática: Koum saiu em 2018 (Statt, 2018), justamente motivado por conflitos relacionados ao tema da privacidade (Dwoskin, 2018) e o comentário de Acton no Twitter logo após o escândalo Cambridge Analytica não tem como passar despercebido:

Figura 4: Mensagem de Brian Acton no esteio do escândalo Cambridge Analytica (Fonte: Twitter).

No lançamento da criptografia, os fundadores assinaram um texto no blog do WhatsApp dizendo: "WhatsApp sempre priorizou que seus dados e sua comunicação fossem o mais segura possível" (Koum e Acton, 2016, par 1, tradução livre), referindo-se respectivamente ao tipo de principio ou declaração de valores como as previamente mencionadas por Koum na entrevista

citada anteriormente. No entanto, apenas alguns meses antes da implementação da criptografia, WhatsApp anunciou, metamorfoseado em uma inocente atualização de Termos de Serviço e Política de Privacidade (WhatsApp Inc., 2016) que compartilharia a informação de WhatsApp com o Facebook (Budington e Gebhart, 2016). Aquela "pequena, mas significativa" concessão foi operacionalizada denunciando que a companhia favoreceu uma "experiência de usuário fluida, confiável, sem dificuldades" às custas do "risco a privacidade dos cidadãos" e não vice-versa.

Perspectiva Tecnológica

Guerrilha de Relações Públicas

No dia 5 de abril de 2016 os fundadores do WhatsApp anunciaram no blog oficial da companhia: "Hoje mais de um bilhão de pessoas usa o WhatsApp para estar em contato com seus amigos e família por todo o mundo. E a partir de agora, cada um deles pode falar livremente e de forma segura no WhatsApp" (Koum e Acton, 2016, par. 8, tradução livre). Era o fim de um longo processo de implementação da encriptação provavelmente sem equivalente no mundo: mais de um bilhão de pessoas[8] foi beneficiado com a nova funcionalidade. No entanto, conforme discutido previamente, paira a questão sobre a mensagem que o WhatsApp circulou em cada conta de cada conversa, alertando para a nova funcionalidade, que seria invisível aos olhos do usuário normal na ausência de tal mensagem.

As funcionalidades são a evidência dura que reflete o que jaz sob o discurso corporativo das empresas de tecnologia. Convenhamos que é pouco provável que a implementação de uma funcionalidade tão complexa, sofisticada e custosa seria apenas visando aos frutos do marketing. WhatsApp foi adquirido pelo Facebook pouco depois das revelações de Snowden e o projeto de criptografia começou pouco depois da aquisição (Brandom, 2014), aparentemente impulsado pelos fundadores do aplicativo (Dwoski, 2018). Além disso, o Facebook já teve sua boa cota de acusações de violação de privacidade, acumulando vários processos e a insatisfação dos usuários de meios digitais com este tipo de violação não é nenhuma novidade; portanto a criptografia

[8]Em Janeiro de 2018 o aplicativo havia superado 1.5 bilhão de usuários de acordo com um post de Zuckerberg no Facebook datado de 14 de junho de 2018. Recuperado de https://www.facebook.com/zuck/posts/10104501954164561.

poderia ser um movimento criativo e estratégico para evitar tal tipo de conflito de forma simultaneamente legal e tecnológica.

Portanto os anúncios da mídia e via blog e o esforço para que a criptografia fosse visível podem ser interpretados como se a companhia tivesse a intenção de projetar uma imagem de privacidade e segurança aos usuários que poderiam estar considerando mudar para aplicativos concorrentes – como o Signal ou o Telegram – devido a melhores funcionalidades neste quesito. Além disso, o anúncio dos fundadores no Blog da empresa deixa entrever um enquadre intencional opondo liberdade versus controle. Não obstante, tal decisão também encapsula um gesto político, posto em evidência pelos conflitos com a corte brasileira: *é uma forma de assegurar aos usuários menos experimentados tecnologicamente que será impossível compartilhar informação com qualquer governo*, ainda que a empresa quisesse ou fosse legalmente compelidos a fazê-lo, como no caso brasileiro. Ao tornar pública a encriptação, o WhatsApp busca converter uma funcionalidade essencialmente técnica em sentido comum como uma *estratégia para cooptar a opinião pública* para tomar seu partido em caso de haver novos conflitos com qualquer corte no mundo.

Ao 'ilustrar' o público, a companhia fomenta uma espécie de *guerrilha* comunicacional, na medida que se constrói de baixo para cima, inversamente a estratégias comunicacionais tradicionais no modelo broadcast de difusão. Esta intencionalidade se evidencia na medida em que o mensageiro próprio do Facebook também implementou tal funcionalidade, embora com muito menos alarde (Greenberg, 2016). Este chamado público e de certa forma dramático para conseguir a simpatia do público, como um efeito colateral de sua conscientização tecnológica, é mais explícita ainda nos comentários de Zuckerberg após o primeiro bloqueio no Brasil: "É um dia triste para o Brasil (...) Se você é brasileiro, *por favor faça ouvir sua voz*. #ConectaBrasil #ConectaOMundo" (Zuckerberg, 2015, ênfase nossa, tradução livre, ver figura 5 para o original). A convocatória de Zuckerberg para uma espécie de resistência contra governos que não entendem que o que eles pedem é tecnicamente impossível, ao mesmo tempo que dá a entender que a implantação da criptografia foi alavancada de forma espontânea, como se não houvesse deliberação dos executivos. *Simultaneamente, politiza e despolitiza a questão*.

Figura 5: Post de Zuckerberg após o bloqueio do WhatsApp no Brasil em 2015 (Fonte: Perfil pessoal do Facebook, 17 de dezembro de 2015).

Este movimento de xadrez político do WhatsApp é sintetizado no comentário de John Naughton no The Guardian sobre a implementação da encriptação:

> (...) de forma que quando chegue a polícia, munida de um mandato, os executivos corporativos são, infelizmente, 'incapazes de ajudar'. *Isto é simultaneamente sagaz estratégia corporativa e astúcia política*. (Naughton, 2016, par 9, ênfase nossa, tradução livre)

Esta encenação de uma guerrilha assimétrica de relações públicas busca assimilar os usuários como militantes, insinuando que eles pertencem ao grupo dos 'fracos' (usuários e corporação) contra os 'fortes' (Estado), embora WhatsApp e Facebook se assemelhem muito mais a um "fenômeno poder-corporativo-estatal" (Trottier e Fuchs, 2015, p. 34, tradução livre).

Encriptação soluciona tudo… ou não?

A implementação da criptografia ponta-a-ponta foi aplaudida por especialistas em segurança e privacidade. De acordo ao relatório "Who has your back", da *Electronic Frontier Foundation* (Cardozo, Crocker, Lynch, Opsahl e Reitman, 2017), o WhatsApp realizou um bom trabalho com a encriptação usando o *Protocolo Signal*. No entanto, outras questões não confirmam o mesmo esmero com segurança e privacidade, levando os especialistas a não recomendar o aplicativo:

> Nós não temos problemas com o desempenho da criptografia (...) Na verdade, nos preocupa a segurança do WhatsApp, *justamente apesar* dos melhores esforços do Protocolo Signal. (Budington e Gebhart, 2016, par 4, ênfase nossa, tradução livre)

Em outras palavras, a recente preocupação com privacidade e segurança não ressoa com algumas das decisões da companhia, transformadas em funcionalidades, atributos ou configurações. Novamente a EFF (Budington e Gebhart, 2016) levanta algumas limitações relevantes do aplicativo nestes temas: respaldo sem encriptação; notificações de mudança de chave que levam ao clássico problema do *man in the middle*; o aplicativo web para acessar WhatsApp, exposto às vulnerabilidades dos navegadores; e o polêmico compartilhamento de dados com o Facebook, rompendo promessas públicas dos fundadores do aplicativo.

Além dos pontos fracos destacados pelos especialistas da EFF, uma forma de vazar informação de uma conversa privada nos aplicativos de mensageria instantânea é a captura de telas, inclusive quando a mensagem tem duração limitada (como um temporizador de 'autodestruição'). O Telegram, por exemplo, tem uma funcionalidade que notifica o outro usuário de uma captura de tela quando se usa a funcionalidade de 'conversas secretas' (ver Figura 6).

Em síntese, parece claro que embora a criptografia ponta-a-ponta é uma funcionalidade valorizada pela comunidade e que aborda diversas problemáticas de segurança e privacidade simultaneamente, as limitações dos nuances de sua implementação também são dignas de nota. Entendemos tais limitações como pistas que sugerem outras dimensões de sua *raison d'être*: política, conforme visto anteriormente, e comercial, a ser discutida a seguir.

Figure 6: Notificação de captura de tela de mensagens em conversa secreta no Telegram (Imagem: Softpedia).

Trade-off: massividade comercial x utopia tecnológica

Uma das fraquezas de segurança do WhatsApp, detectadas na seção anterior, é a mudança de chave de criptografia (que gera o problema conhecido como *'Man in the middle'*). Este mesmo problema foi objeto de debate tanto na mídia especializada como entre profissionais e especialistas do meio, uma vez que foi indevidamente magnificado como uma 'porta dos fundos' pelo *The Guardian* (Ganguly, 2017). Esta classificação escandalosa foi rapidamente esfriada e definida como uma "falha" (Chadwick, 2017) por um editor sênior do mesmo meio. Desde então a mesma falha foi catalogada como um "*trade-off*" por alguns especialistas em segurança (Chadwick, 2017; Portnoy e Bonneau, 2017) e em cibercultura (Tufekci, 2017). Em outras palavras, podemos dizer que a WhatsApp Inc. fez escolhas que priorizaram a massividade comercial em lugar de outros valores ou objetivos como, por exemplo, mais segurança ou melhor

privacidade para seus usuários. Neste sentido, o caso do WhatsApp parece ser emblemático das tensões descritas por Jose van Dijck (2013), em sua *História Crítica da Mídia Social*: "Plataformas tiveram que navegar entre o capital de risco do Vale do Silício, que pressiona por retornos de curto prazo e um rápido trânsito à bolsa de valores, e o espírito participativo originário, o autêntico responsável pelo crescimento das plataformas em primeiro lugar" (p. 15, tradução livre). EFF sintetiza tal *trade-off* comparando WhatsApp com Signal, o que ajuda a visibilizar as falhas do primeiro, complementando o que fizemos na seção anterior:

> WhatsApp (...) era uma ferramenta popular e massiva antes da inclusão da criptografia ponta-a-ponta. O objetivo era incorporar a criptografia de uma forma que os usuários sequer sabiam que estava lá (...) WhatsApp não está competindo com o Signal no mercado, mas sim compete com muitos outros aplicativos que não têm a criptografia ponta-a-ponta como padrão e não têm que fazer tais escolhas. (Portnoy e Bonneau, 2017, par 12, tradução livre)

A tabela a continuação sintetiza cinco dos *trade-offs* que refletem as tensões de ambos lados em que WhatsApp deve navegar, seguindo a proposta de van Dijck:

Tabela 2. Trade-offs evidenciam o favorecimento da massividade comercial por sobre a privacidade e a segurança do usuário do aplicativo (Elaboração: Autores).

Trade-offs	
Funcionalidade Insegura	*Massividades/Beneficio Comercial*
Respaldo padrão sem criptografia	Melhor experiência de usuário: mais fácil manter e recuperar as conversas respaldadas.
Mudança de chave de criptografia com a mudança de dispositivo	Permite ao usuário uma mudança de aparato sem obstáculos técnicos, facilitando a tendência mercadológica da obsolescência programada
Aplicativo versão web insegura, sustentado pela segurança e privacidade do navegador utilizado	Maior conveniência dos usuários, que não têm que descarregar e atualizar constantemente um software de tipo 'cliente', que seria a opção mais segura
Compartilhamento de dados com o Facebook	Provavelmente um trade-off que permitiu manter a promessa de manter o WhatsApp eternamente livre de propaganda. Alternativamente, simplesmente uma decisão arbitrária do Facebook com vistas a aprimorar seu negocio de comercialização de modelamento de perfis para publicidade.
Captura de tela sem monitoramento	Se mantem uma funcionalidade útil para o dia a dia, apesar das possibilidades de vazamento de informação íntima e/ou privada.

CONCLUSÃO

Detrás do discurso de defensores da segurança e privacidade por parte dos fundadores no ato do lançamento da criptografia ponta-a-ponta, visto tanto da perspectiva idealista como da comercial, e detrás da decisão de tornar a encriptação visível, três histórias emergem: (i) uma guerrilha comunicacional de relações públicas alimentada de baixo para cima (usuários) pela WhatsApp Inc. quem, através de sutis iniciativas de gestão da opinião pública mobiliza seus bilhões de usuários como militantes para ajudá-la a enfrentar (ii) uma disputa de poder entre a corporação e os Estados, em que a variável do desenvolvimento tecnológico de funcionalidades –

como a criptografia – pode ser lido como uma declaração tecnopolítica ou, seguindo a metáfora bélica, uma arma para-legal; e as vulnerabilidades e/ou imperfeições resultado de opções na implementação das mesmas são vistas como (iii) a contrapartida da opção pela massividade comercial versus a utopia tecnológica, tal que em algum ponto no caminho, o conto de fadas do sonho americano de Koum é subjugado pelas pressões capitalistas de Silicon Valley e o discurso utópico de start-ups cede a um "Capitalismo de Plataforma" (Srnicek, 2017) muito mais pragmático e menos inspirador, dentro da lógica da busca de dividendos para os acionistas.

Programar é uma forma de exercer poder, por parte dos desenvolvedores de tecnologia. Implica opções. A implementação da criptografia do WhatsApp não foi, portanto, impulsada somente por valores inculcados no idealismo da cultura digital *start-up*, nem somente por razões mercadológicas.

As funcionalidades são uma manifestação concreta de poder das mídias digitais. Como a outra face do ponto anterior, opções estratégicas de desenvolvimento têm tamanha relevância que geram inclusive reações negativas de governos variados: Reino Unido (Hintz, 2015; Burrell, 2017), Brasil (Abreu, 2017) e EUA (McCarthy, 2015), para citar alguns exemplos.

Massividade prevalece sobre a privacidade, segurança e outros possíveis compromissos que a companhia ou seus fundadores poderiam ter, simpatizar ou defender. Bases de dados massivas são "a galinha dos ovos de ouro" (van Dijck, 2013, p. 16, tradução livre) das plataformas de redes sociais digitais. Adicionalmente, na medida em que o Facebook gradualmente quebrou as promessas originais do WhatsApp, e na medida em que as contradições aumentaram, até mesmo os fundadores do aplicativo abandonaram o barco.

A politica das mídias sociais parece, consequentemente, transitar entre sua capacidade de vigilância e alguns remendos de privacidade. No "complexo vigilante-industrial" (Trottier e Fuchs, 2015, p. 34, tradução livre), parece que o poder-corporativo-estatal revela a disputa direta não só do WhatsApp com diversos Estados singulares, mas com discursos éticos de privacidade, e normas de segurança dirigidas ao governo das pessoas. Trata-se de uma espécie de cooperação que parece operar como uma negociação permanente sobre que tipo de regulação a companhia está disposta a cumprir de forma que também o Estado saia ganhando. Em síntese, a dimensão legal se confunde com a política, enquanto as companhias de tecnologia como o WhatsApp

procuram se proteger de ambas ao colocar-se ativamente em uma posição de impossibilidade de cooperar: *ad impossibilita nemo tenetur*[9].

REFERÊNCIAS

Abreu, J. S. (2017). Public hearing on encryption and WhatsApp blockages: the arguments before the STF. *bloqueios.info*, InternetLab, June 26th, translated by Ana Luiza Araujo. Retrieved from http://bloqueios.info/en/public-hearing-on-encryption-and-whatsapp-blockages-the-arguments-before-the-stf/.

Brandom, R. (2014). WhatsApp rolls out end-to-end encryption using TextSecure code. *The Verge*. November 18. Retrieved from https://www.theverge.com/2014/11/18/7239221/whatsapp-rolls-out-end-to-end-encryption-with-textsecure

Budington, B. & Gebhart, G. (2016). Where WhatsApp Went Wrong: EFF's Four Biggest Security Concerns. *EFF*. October 13. Retrieved from https://www.eff.org/deeplinks/2016/10/where-whatsapp-went-wrong-effs-four-biggest-security-concerns

Burgess, J. & Baym, N. (2016). @RT#: Towards a Platform Biography of Twitter. In Burgess, J., Baym, N., Bucher, T., Helmond, A., John, N., Nissenbaum, A., Cunningham, S., & Craig, D. (2016, October 5-8). Platform studies: the rules of engagement. Panel presented at *AoIR 2016: The 17th Annual Conference of the Association of Internet Researchers*. Berlin, Germany. Retrieved from http://spir.aoir.org.

Burgess, J. & Baym, N. (2017). Platform Biography [Powerpoint Slides]. *DMRC Summer School 2017*. Brisbane, Australia.

Burrell, H. (2017). How secure is WhatsApp? WhatsApp security and encryption explained. *Tech Advisor*. March 27. Retrieved from https://www.techadvisor.co.uk/feature/internet/how-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780/

Cadwalladr, C. & Graham-Harrison, E. (2018, Mar, 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Cardozo, N., Crocker, A., Lynch, J., Opsahl, K. & Reitman, R. (2017). Who has your back 2017. *EFF*. July 10. Accessed November 16, 2017. https://www.eff.org/who-has-your-back-2017#whatsapp-report.

Chadwick, P. (2017). Flawed reporting about WhatsApp. *The Guardian*. June 28. Retrieved from https://www.theguardian.com/technology/commentisfree/2017/jun/28/flawed-reporting-about-whatsapp

Cimpanu, C. (2015). Signal Encrypted Messaging App Comes to Desktops. *Softpedia News*. December 3. Retrieved from http://news.softpedia.com/news/signal-encrypted-messaging-app-comes-to-desktops-497084.shtml

[9] Expressão legal original em latim que significa que ninguém pode ser obrigado a realizar o impossível. Recuperado de http://www.oxfordreference.com/view/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-113.

Deleuze, G. (1992). "Postscript on the Societies of Control", *October*, 59, 3-7. Retrieved from https://www.jstor.org/stable/778828

Dencik, L. & Leistert, O. (2015) *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*. London: Rowman & Littlefield International. Kindle Edition.

Dwoskin, E. (2018, April, 30). WhatsApp founder plans to leave after broad clashes with parent Facebook. *The Washington Post.* Retrieved from https://www.washingtonpost.com/business/economy/whatsapp-founder-plans-to-leave-after-broad-clashes-with-parent-facebook/2018/04/30/49448dd2-4ca9-11e8-84a0-458a1aa9ac0a_story.html?noredirect=on&utm_term=.dd7d539d05e5

Foucault, M. (1975). Surveiller et Punir. Paris: Gallimard.

Ganguly, M. (2017). WhatsApp design feature means some encrypted messages could be read by third party. *The Guardian.* January 13. Retrieved from https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages

Gibson, J. J. (1977). The theory of affordances. In Shaw, R.E., & Brandford, J., (eds). *Perceiving, Acting, and Knowing: Toward an Ecological Psychology*. Hillsade, NJ: Erlbaum, 67-82.

Gibson, J. J. (1986). *The Ecological Approach to Visual Perception*. Hillsade, NJ: Erlbaum.

Greenberg, A. (2016). You Can All Finally Encrypt Facebook Messenger, So Do It. *Wired Magazine*. October 4. Retrieved from https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. June 6. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G. & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. June 7. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Gillespie, T. (2010). The politics of 'platforms'. *New Media & Society, 12*(3), 347-364.

Hintz, A. (2015). Social Media Censorship, Privatized Regulation and New Restrictions to Protest and Dissent. In Dencik, Lina & Leistert, Oliver (2015) *Critical Perspectives on Social Media and Protest: Between Control and Emancipation*. London: Rowman & Littlefield International. Kindle Edition.

Hutchby, I. (2001). Technologies, texts and affordances. *Sociology* 35(2), 441-456.

Koum, J. & Acton, B. (2016). end-to-end encryption. *WhatsApp Official Blog.* April 5. Retrieved from https://blog.whatsapp.com/10000618/end-to-end-encryption?l=en

Langlois, G. (2014). *Meaning in the age of social media*. New York, USA: Palgrave MacMillan.

Lévrier A. & Wrona, A. (eds.). (2013). Matière et esprit du journal. Du Mercure Galant Mercure à Twitter, Paris : PUPS [Histoire de l'imprimé].
Liao, S. (3 de dezembro de 2018). Tumblr will ban all adult content on December 17th *The Verge.* Retrieved from https://www.theverge.com/2018/12/3/18123752/tumblr-adult-content-porn-ban-date-explicit-changes-why-safe-mode.

McCarthy, T. (2015). NSA director defends plan to maintain 'backdoors' into technology companies. *The Guardian.* February 23. Retrieved from https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies

Meyrowitz, J. (1994). Medium theory. In Crozley, D., & Mitchell, D. (eds). *Communication Theory Today*, Standford, CA: Standford University, 50-77.

Naughton, J. (2016). Your WhatsApp secrets are safe now. But Big Brother is still watching you… *The Guardian.* April 10. Retrieved from https://www.theguardian.com/commentisfree/2016/apr/10/whatsapp-encryption-billion-users-data-security

Norman, D. (1999). Affordance, Conventions and Design. *interactions, 6*(3), 38-43. Retrieved from http://www-ihm.lri.fr/~mbl/ENS/DEA-IHM/papers/Norman-Affordances.pdf

Portnoy, E. & Bonneau, J. (2017). Google Launches Key Transparency While a Trade-Off in WhatsApp Is Called a Backdoor. *EFF*. January 14. Retrieved from https://www.eff.org/deeplinks/2017/01/google-launches-key-transparency-while-tradeoff-whatsapp-called-backdoor

Rowan, D. (2014). WhatsApp: The Inside Story. *Wired Magazine*. February 19. Retrieved from http://www.wired.co.uk/article/whatsapp-exclusive.

Scriberia, Cawley, S., Kiss, J., Boyd, P. & Ball, J. (2013). The NSA and surveillance... made simple. *The Guardian.* November 26. Retrieved from https://www.theguardian.com/world/video/2013/nov/26/nsa-gchq-surveillance-made-simple-video-animation

Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.

Statt, N. (2018, April 30). WhatsApp co-founder Jan Koum is leaving Facebook after clashing over data privacy. *The Verge*. Retrieved from https://www.theverge.com/2018/4/30/17304792/whatsapp-jan-koum-facebook-data-privacy-encryption

STF (Supremo Tribunal Federal do Brasil). (2017). Audiência pública - Bloqueio judicial do WhatsApp e Marco Civil da Internet (1/4). [Direct link to Brian Acton deposition] *STF YouTube Channel*. June 5. Retrieved from https://www.youtube.com/watch?v=3TNsQCNIOO0&feature=youtu.be&t=43m30s

Trottier, D., & Fuchs, C. (2015). Theorising social media, politics and the state. In *Social Media, Politics and the State. Protest, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and YouTube*. New York: Routledge, p.3-38.

Tufekci, Z. (2017). In Response to Guardian's Irresponsible Reporting on WhatsApp: A Plea for Responsible and Contextualized Reporting on User Security. Author's Blog. Retrieved from. http://technosociology.org/?page_id=1687.

Van Dijck, J. (2009). Users like you? Theorizing agency in user-generated content. *Media, culture & society*, 31(1), 41-58.
Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social* Media. Oxford University Press. Kindle Version.

WhatsApp Inc. (2016). Un vistazo al futuro de WhatsApp. *WhatsApp Official Blog*. August 29. Retrieved from https://blog.whatsapp.com/10000627/Un-vistazo-al-futuro-de-WhatsApp.

Zuckerberg, M. (2015). Facebook Post (December 17, 2015). Retrieved from https://www.facebook.com/zuck/posts/10102530374780451?pnref=story.

Original recebido em: 11 de fevereiro de 2019
Aceito para publicação em: 15 de maio de 2019

Esta obra está licenciado com uma Licença
Creative Commons Atribuição-NãoComercial-CompartilhaIgual 4.0 Internacional