Construtos de segurança a partir de suas atualizações em imagens técnicas; apontamentos sobre formas de login e serviços autenticadores na *web*[1].

Roberta Fleck Saibro KRAUSE[2]
Lucas Melo NESS[3]

Universidade do Vale do Rio dos Sinos, São Leopoldo, RS.

RESUMO

O presente artigo visa debater sobre os construtos de segurança na *web* a partir de suas atualizações em imagens técnicas. Com o alicerce do método cartográfico, observamos a apropriação de dois grandes serviços de autenticação via Facebook e Google e sobre os elementos que envolvem uma imageria em torno de comunicação segura e eficiente, nas interfaces culturais. Através do movimento de flanerie realizado, nos deparamos com iniciativas que dispensam a realização de cadastros, permitindo o usuário autenticar sua identidade a partir do login social, a quem chamamos de serviços autenticadores. A partir dessas manifestações, observamos um novo construto de segurança na tecnocultura, não apenas baseado em cadeados, escudos e chaves, mas na confiança prometida sobre essas páginas na internet.

PALAVRAS-CHAVE: construtos de segurança; usuário; comunicação digital; imagem; dados

INTRODUÇÃO

A presente reflexão busca apresentar um tensionamento envolvendo a apropriação de imagens na *web* a partir da dimensão de seu uso para fins de segurança. Partimos como proposta para objeto empírico duas ordens presentes na *web*, o Facebook (FB) e Google (GG), buscando o caráter de "serviço autenticador" de ambos. Como passo inicial para adentrar no debate proposto, apresentamos o problema que norteia o artigo, que busca responder: Como os construtos de segurança na *web* se atualizam a partir do FB e do GG? Encontramos uma potencialidade na discussão acerca de imagens técnicas, reproduzidas pelo FB e GG, a partir de sua característica de solicitação e liberação de acesso de usuários

[1] Trabalho apresentado no GP Comunicação e Cultura Digital, XX Encontro dos Grupos de Pesquisas em Comunicação, evento componente do 43º Congresso Brasileiro de Ciências da Comunicação.

[2] Doutoranda do Curso de Pós-Graduação em Ciências da Comunicação da UNISINOS, e-mail: robertakrause@hotmail.com

[3] Doutorando do Curso de Pós-Graduação em Ciências da Comunicação da UNISINOS, e-mail: lucasness@gmail.com

utilizando imagens como recursos para garantia de segurança. Propomos pensar o papel da imagem no controle de segurança ou vazamento de informação/dados dos usuários de contas nos empíricos citados previamente.

Para realizar o tensionamento entre o uso de imagens técnicas na *web* e os protocolos de segurança utilizados a partir de uma imageria vinculada a "eficiência de um segredo", avançaremos na reflexão a partir de conceitos relacionados às audiovisualidades e tecnocultura, levando em consideração autores como Henri Bergson (2006), Gustavo Fischer (2015), Lev Manovich (2014), Villém Flusser (2002) e Jacques Rancière (2003), e sobre segurança e uso de dados a partir de Peter Krapp (2019) e Shoshana Zuboff (2019). De forma complementar, no segundo momento do texto, faremos uma cartografia inspirada no movimento de *flaneur* de Walter Benjamin (2006) como apoio metodológico para ir em busca das manifestações do que estamos chamando por construtos de segurança na *web.*

Problematizando as imagens

Para avançar na perspectiva do pensamento sobre as imagens que estamos problematizando no artigo, precisamos ressaltar o conceito proposto por Villém Flusser (2002), onde articula sobre um tipo de imagem e sua relação com a tecnologia, denominada por ele como "imagens técnicas", resumidamente seriam imagens produzidas por aparelhos ou "[...] aparelhos são produtos da técnica que, por sua vez, é texto científico aplicado. Imagens técnicas são, portanto, produtos indiretos de textos – o que lhes confere posição histórica e ontológica diferente das imagens tradicionais" (FLUSSER, 2002, p. 10). É possível pensar que a representação imagética de algo seguro e confiável ao usuário da *web* permanece relacionada a associações tradicionais de segurança do "mundo offline", como cadeados, chaves, senhas, escudos, ícones de conteúdo criptografado, códigos QR, verificação de grupos de imagens semelhantes e até mesmo o uso do login social[4]. Portanto, vemos a proposta de refletir sobre como os construtos de segurança na *web* se atualizam nas imagens técnicas.

Conforme defendido por Krapp (2020), a cultura digital está baseada na eficiência da comunicação, lembrando sobre as teorias da comunicação, como a proposta de Shannon e Weaver de 1949 (Wolf, 1992) onde a matemática explica a lógica de

[4] O login social permite que o usuário utilize seu cadastro já realizado em sites de redes sociais para acessar outros conteúdos online que exigem registros prévios. Ou seja, é possível entrar em um site através de login e senha cadastrados em terceiros.

transmissão dos impulsos elétricos entre um emissor e o receptor. Evitando ao máximo os ruídos para se obter sucesso na transmissão do sinal "tratava-se, portanto, de conseguir estabelecer o modo mais econômico, mais rápido, e mais seguro de *codificar* uma mensagem, sem que a presença do ruído tornasse problemática a transmissão" (Wolf, 1992, p. 100). Ao trazer a mesma lógica de comunicação segura para a contemporaneidade, onde a comunicação em rede está praticamente nas mãos de grandes empresas, detentoras de enormes territórios com servidores de armazenamento de dados para fins comerciais, é natural que os usuários desse sistema se sintam mais à vontade ao disponibilizar seus dados e deixar "rastros", na *web* sustentados por lógicas que apoiam o imaginário[5] de proteção ou segurança de informação.

O uso de símbolos a partir das ilustrações carrega um sentido que configura uma característica estética na cultura digital, como podemos verificar no nosso movimento de flanar pelo FB e pelo GG, onde encontramos diversas manifestações nesse sentido, seja através de cadeados, chaves, cofres, senhas e o próprio login social. Ao direcionar nosso olhar para essas manifestações de segurança, acreditamos ser adequada a apropriação do termo *"imagérie"* ou imageria (tradução nossa) do autor Jacques Rancière (2013) devido à sua característica que remete "a todas as formas de produção e reprodução de imagens, não especificamente às produzidas por "equipamento imageador", como repertório de imagens disponíveis (RANCIÉRE, 2013, p. 24). Portanto, encaramos que o grupo de figuras relacionadas ao imaginário de segurança formam essa imageria em torno de proteção de dados, facilitando e impulsionando o usuário a confiar naquele conteúdo. Nesse sentido, Penkala (2011) reforça a definição do termo ao dizer que

> Grosso modo, imageria é referente a um conjunto de imagens. Essas imagens formam um conjunto a partir de um elemento de coesão, que lhes é externo. Embora não seja um termo de uso corrente na língua portuguesa e não seja tratado na literatura consultada, uma definição pontual seria a de que a imageria envolve um senso coletivo e um envolvimento mental ou intelectual em sua construção. É um conjunto de imagens formadas a partir de um consciente que as agrupa por sua natureza figurativa, por semelhanças ou por importância relativa à dada coisa. (PENKALA, 2011. p. 18)

Ao apresentar imagens que enunciam essa memória de eficiência ao "manter o segredo" sobre o conteúdo pessoal do usuário, confere-se à imagem um papel de

[5] Estamos tratando como imaginário a definição de Kilpp (2002) em sua tese de doutorado, ao assumir "o imaginário como mediações, que são também um conjunto de marcas de enunciação das culturas (identidades coletivas), manifestas e visíveis nos discursos, na arte, nos produtos culturais..., ou que são por eles mediadas. (KILPP, 2002. P. 41)

verificador de segurança nas interfaces digitais atuais. Essa imageria não é restrita à *web* ou os produtos que ali circulam, mas confere-se à demais softwares e interfaces, como, por exemplo, caixas eletrônicos de ordem bancária, sistemas de segurança residenciais etc. De maneira complementar, Bruno Polidoro (2008, p.1) traz uma reflexão sobre como o uso e apropriação das imagens impactam na nossa realidade ao trazer uma busca "dessa remagicização, a sociedade atual está se tornando, outra vez, cada vez mais imagética. Somos invadidos a todo o momento por milhares de imagens: nas ruas, nas salas das casas e nas de cinema, nas telas dos computadores".

Vale lembrar que estamos buscando essas imagens a partir do pensamento de Henri Bergson (2006), e que conforme Bruno Polidoro (2008, p. 1) sintetiza "[...] busca perceber o audiovisual como uma virtualidade e, com isso, compreender o sentido de linguagem nesses diversos suportes de som e imagem".

Imagem, tecnocultura e interfaces

Através do exercício de capturas de telas da rede social FB, por exemplo, é possível ver que há uma mistura de oferta de texto com ícones que indicam análise de senhas, critérios de segurança, políticas de privacidade, etc. Outra possibilidade para se pensar um objeto audiovisual é "desde a perspectiva de sua irredutibilidade a qualquer mídia, admitindo que o audiovisual também é uma virtualidade que se atualiza nas mídias, mas que as transcende" (KILPP; FISCHER, 2010, p. 6 in FISCHER, 2013, p. 42). Nesse sentido, vale resgatar o comentário de Fischer (2013, p. 46) sobre a tecnocultura e a relação com a proposta de Walter Benjamin para se pensar as mídias e o envolvimento com a tecnologia, envolvendo esta como papel importante na capacidade de reprodução ao desafiar a autenticidade (como em seu livro "A obra de arte da era de sua reprodutibilidade técnica" de 1986),

> Ainda que pensando em fonogramas e fotografia na cultura parisiense do século XIX, as reflexões de Benjamin sobre o que se toma a experiência humana a partir do imbricamento das tecnologias de (re) produção de imagens e sons são embebidas de uma perspectiva tecnocultural absolutamente essencial para as discussões contemporâneas que marcam as reflexões dos autores que observam a sociedade midiatizada e softwarizada (FISCHER, 2013, p. 46).

Como uma das características do ambiente da *web* é incentivar o compartilhamento e dispersão de conteúdo *online*, conforme Kilpp (2012). Portando, a ação de um usuário ao compartilhar para sua rede de amigos no FB um conteúdo

publicado anteriormente por outro usuário ou página, promove uma dispersão de conteúdo "sem limites", onde cada usuário compartilha, comenta ou curte e assim sucessivamente sua rede de amigos.

> A dispersão e convergência assim proposta como virtualidade, tal como as audiovisualidades, atualiza-se hoje especialmente nas plataformas de compartilhamento de vídeos na internet, nas quais a imagem aparece ao lado de outras tornadas afins segundo os mais diferentes critérios de afinidade imaginada pelos detentores do site ou imaginada por seus usuários, sejam eles realizadores, empresas de comunicação ou apenas colecionadores, sendo a dispersão um dos critérios da convergência. (KILPP, 2012, p. 224).

Há um incentivo constante da rede social para que o usuário publique alguma informação para ser compartilhada com suas conexões, gerando um fluxo constante de informações entre os usuários da rede, ou um modo de agir que como diz Fischer (2016, p. 6) sobre a *web* que gera um "fluxo permanente de atualização e substituição". Também precisamos levar em consideração que conforme há o surgimento no mercado de novas redes sociais e aplicativos disputando as possibilidades de interação entre usuários através da internet, a produção de formatos diferentes e "inovadores" de vídeo ou texto, lançados como novidades possibilita uma vida um pouco mais longa dentro de um mercado muito competitivo, e de uma "tecnocultura de obsolescência programada e interfaces líquidas" (FISCHER, 2016, P. 6).

Para Lev Manovich (2001) o conceito de interface está diretamente relacionado com a definição de uma interface cultural, ou seja, a interface gráfica realizando a mediação entre um computador e o usuário da máquina. Para o autor, "em termos semióticos, a interface do computador atua como um código que transporta mensagens culturais em uma diversidade de suportes (MANOVICH, 2001, p. 113). O hibrismo entre os meios não está restrito aos aplicativos de softwares, interfaces ou o ambiente digital da *web*, mas está presente nas produções estéticas das imagens, principalmente através de intervenções de cineastas, animadores e designers que sofreram forte influência principalmente nos anos 1990, lançando uma nova estética híbrida.

Para Manovich, "não nos comunicamos mais com um computador, mas com a cultura codificada em formato digital" (MANOVICH, 2001, p. 120). E o resultado dessa mistura entre formatos de mídia, como impressa, cinema e interface do usuário é o modelo que temos de interfaces culturais atualmente. A noção de movimento em uma tela, de representação de algo como um cadeado, uma chave, um cofre, de um roteiro padrão para

um filme ou o conceito de narrativa para determinado comando, são resultado da conexão direta entre formatos midiáticos que são capazes de compor a lógica de raciocínio do usuário com a interface gráfica.

De forma complementar, Gustavo Fischer (2015) comenta sobre o termo interface gráfica cultural que o entendimento deve passar pela visão de Lev Manovich que

> [...] afirma que a linguagem – própria – das interfaces gráficas – às quais ele prefere denominar como "interfaces culturais" – está muito ligada a elementos de outras formas culturais consagradas advindas do impresso (printed word), do cinema e das interfaces humano-computador (Human-computer Interface, HCI). Manovich crê que o impresso, o cinema e a interação humanocomputador possuem suas modalidades específicas de organizar a informação, estruturando a experiência humana, correlacionando tempo-espaço. Assim, a facilidade de compreensão imediata da linguagem da interface resultaria do fato de que esta seria baseada em formas culturais prévias e familiares (FISCHER, 2015, p. 77).

Seguindo o argumento de Fischer e a visão de Manovich (2011) sobre a interface do usuário estar relacionada, como mencionamos anteriormente, com uma tradição da nossa cultura, e nas palavras do autor, como "uma linguagem cultural que oferece seus próprios modos de representar a memória e a experiência humanas" (MANOVICH, 2011, p. 123), é importante dizer que para Fischer (2011) o modelo de interface, a maneira como as informações são disponibilizadas através de um banco de dados representadas na tela ainda carregam muitas representações de outras mídias, como a mídia impressa e audiovisual. Nesse sentido, o autor comenta uma genealogia entre as mídias, que vai ao encontro do que Lev Manovich defende, além dos conceitos de McLuhan (1964) alegando que um meio "carrega" em si características de outros meios.

Movimento cartográfico

Nessa "correnteza" infinita de fluxo de dados, expõe a busca por o que Krapp (2019) argumenta sobre o "caminho seguro" proposto pelo discurso do próprio mercado da comunicação para evitar as falhas e supostos usos indevidos de dados de seus usuários. Nesse sentido, a criptografia carrega uma possibilidade de proporcionar a sensação de produzir menos ruído, ou falhas para os usuários. Segundo Krapp (2020) a criptografia se baseia no envio de uma mensagem por meio de códigos que somente podem ser desvendados pelo receptor, ou seja, a segurança na troca de informação é sustentada na baixa probabilidade de vazamento ou de haver algum ruído. Porém, assim como acreditamos haver as representações visuais mais populares difundidas pelas mídias sobre

segurança dos dados na *web*, há também uma construção extremamente fantasiosa em relação ao vazamento ou erro. Um ataque cibernético que invade um sistema operacional, por exemplo, comumente o faz em "silêncio", sem avisar o usuário com letras garrafais ou pirotecnia.

> Como é a comunicação criptografada? O problema das representações audiovisuais de cibersegurança em particular e redes de computadores em geral, é que eles são muitas vezes transformados em caricaturas ridículas na tela. Até mesmo dramas de TV focados em computador, como CSL Cyber (2015), obtêm numerosos detalhes tão errados que poucos espectadores com o mínimo de intimidade por computadores podem assistir. A computação não se trata de luzes e pixels piscantes – e não ajuda a banir o script com uso indevido e jargão pronunciado incorretamente. O Código malicioso não vai aparecer em destaque ou vermelho na tela. A revisão leva mais de alguns minutos. É mais provável que o crime cibernético envolva *phishing* para números de cartão de crédito ou segredos comerciais, em vez de sequestro de informação. Quando se trata de real ou imaginário de riscos on-line, filmes e programas de TV cansam ao produzir e perpetuar estereótipos de hacking como flerte adolescente (geralmente masculino) com crime, mas talvez ofenda ainda mais a maneira como retratam o 'espaço' dos dados como um jogo de videogame. (KRAPP, 2019. p. 80)

Compreendemos pelas palavras de Krapp que se criou uma imageria sobre segurança e hackeamento de dados na rede que reside em ter no apelo visual a capacidade de transmitir a sensação de segurança da informação. Para desvendar os objetos de estudo sem imputar-lhes preconcepções, engessar as possibilidades ou mesmo propor ideias meramente tautológicas, conduzimos nossos passos a partir do olhar metodológico da cartografia. É preciso lançar-se ao campo a partir de uma *flanerie* e se deixar permitir que conduzir pelo terreno da *web* para dar a ver o que estamos chamando de construtos de segurança. Segundo Kilpp, as cartografias constituem uma metodologia capaz de suficientemente fazer emergir o objeto, sem sufocá-lo ou ser leviano, nas palavras da autora:

> "Com tal metodologia instituem-se mapas dinâmicos e nunca finalizados, que autenticam linhas de fato e de fuga relativos ao movimento do objeto (uma sua tendência ou devir) que evolui, distinguindo-se de si rizomaticamente. As autenticações remetem, por sua vez. Àquelas características do objeto que vão sendo percebidas pelo pesquisador de acordo com suas afecções (fundamentais também no método intuitivo, que mencionaremos adiante), tornadas em percepções no decurso do processo investigatório (no que Bergson chamou de "reviravolta"), e que, como tais, retornam à memória do objeto, reinventando-o (ou atualizando-o criativamente)." (KILPP, 2010, p. 27)

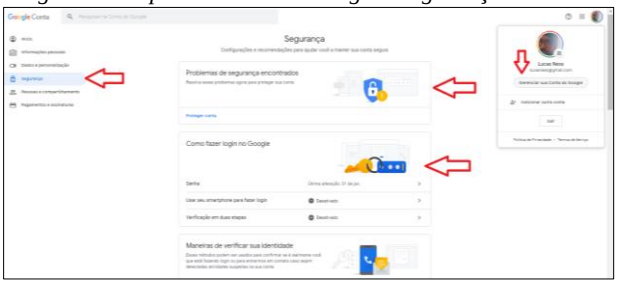
Os construtos de segurança na *web* emergem do caminho percorrido, revisitamos passos e olhamos às suas margens - o cadeado, o código *https*, os construtos de segurança vão se banalizando ao olhar, percorremos os vestígios marginais que se mantém como potência e são soterrados pela história principal, como Benjamin fez com a Paris do início do século XX (BENJAMIN, 1989). Ao passearmos por FB e GG e os serviços de terceiros autenticados por eles - olhamos aquilo que é diariamente menos olhado - o acesso, a entrada, o meio. O agir cartográfico nos encontra para produzirmos esse olhar.

Destacamos o movimento realizado através de capturas de tela/prints do FB e do GG, construímos, em primeiro lugar um paralelo das áreas destinada à segurança dos dados pessoais dos usuários em cada um dos ambientes. Notamos que há diversas indicações de "proteção" para os campos de preenchimento: no FB a área do menu "segurança e login" apresenta uma ilustração semelhante a distintivos policiais, a área de privacidade com um cadeado, a senha é associada a uma chave e a opção de autenticação de dois fatores com um escudo (destaques figura 1). Já no caso do GG, a área de segurança é associada a um cadeado, a seção que evidencia eventuais problemas de acesso é fortemente marcada com um escudo que ostenta um cadeado aberto, enquanto a seção que se refere à senhas tem uma chave em cujo chaveiro encontramos asteriscos, símbolo que aparece na tela quando digitamos uma senha que não está em modo de visualização aberto (figura 2).

Figura 1 - Captura de tela do FB - Segurança da conta

Fonte: Disponível em <https://www.facebook.com/about/privacy> acesso em 24 abr. 2020.

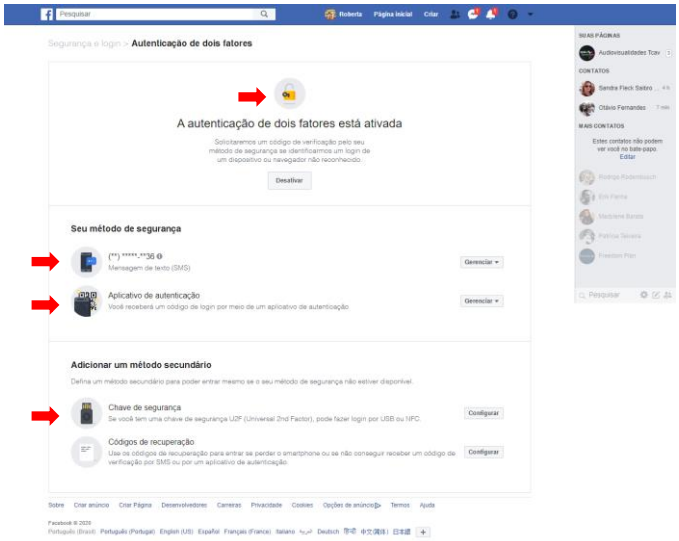
Figura 2 - Captura de tela do Google - Segurança da conta



Fonte: Disponível em <https://myaccount.google.com/secutiry> acesso em 20 jun. 2020.

Acreditamos que através da produção dessas imagens é que também se conduz essa sensação de proteção. Observemos nossos objetos: o FB fornece ao usuário a possibilidade de dupla autenticação de login, como é possível ver na captura de tela a seguir. Utilizando ferramentas como leitura de códigos QR, envio de mensagem via outro dispositivo, como o celular cadastrado na conta ou ainda chave de segurança via entrada USB, as ilustrações utilizadas para indicar as opções de autenticação também estão relacionadas com comunicação sigilosa.

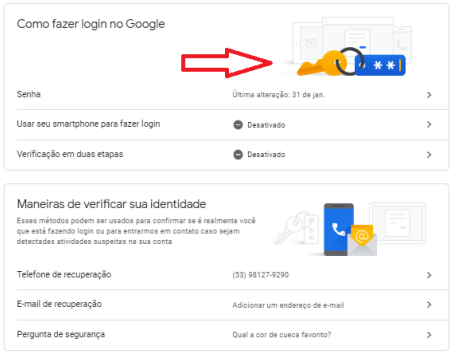
Figura 3 - Captura de tela do FB - Autenticação de conta



Fonte: Facebook. Disponível em <https://www.facebook.com/about/privacy> acesso em 24 abr 2020.

O GG também possibilita uma série de formas de autenticação do usuário, cujas ilustrações reforçam a ideia de interdependência entre as opções - o smartphone em segundo plano ao lado da chave ganha destaque quando o serviço passa a falar sobre recuperação de senha, deixando-a em menor destaque, conforme abaixo:

Figura 4 - Captura de tela do Google - Segurança da conta



Fonte: Disponível em <https://myaccount.google.com/secutiry> acesso em 20 jun. 2020.

O duplo *check* de verificação também sustenta a ideia de segurança e redução de chance de vazamento (ou uso não autorizado) de dados de usuários. Porém, se torna um paradoxo desde que o FB foi acusado por vazamento de informação "privada" de usuários para uma empresa de tecnologia, a Cambridge Analytica. Conforme recente livro de Brittany Kaiser[6] relatando um dos maiores escândalos envolvendo as redes sociais. Nesse ponto, é necessário trazer o conceito de capitalismo de vigilância proposto por Shoshana Zuboff (2019) ao afirmar que hoje o colonialismo de dados é o novo capitalismo, partindo do uso de informação de usuários para aprimoramento de produtos e serviços, mas também para realizar análise preditiva de comportamento humano para fins financeiros. Nas palavras da autora "o capitalismo de vigilância reivindica unilateralmente a experiência humana como matéria-prima gratuita para tradução em dados comportamentais[7]" (ZUBOFF, 2019, p. 27).

Pela lógica de operação do mercado, os usuários do FB e GG, autenticam muitas entradas em outros sites na internet através de login social, nos quais não há qualquer indicação de cadeado, escudo, chaves, etc. Então pode-se propor que o serviço autenticador conduz a sensação de segurança quando intermedia a entrega de dados e informações confidenciais fornecidos - a princípio, exclusivamente a ele - a um terceiro *player* de mercado (ao qual optou-se por não fornecer informações diretamente). Ou seja, o serviço autenticador parece ganhar o "status" de confiabilidade e segurança - suprimindo a necessidade de preencher um novo cadastro e seu fornecimento de dados, ou mesmo de memorizar uma nova senha de acesso para acessar aquele conteúdo ou serviço.

[6] Ex-diretora de desenvolvimento de negócios da Cambridge Analytica, no livro "Manipulados: Como a Cambridge Analytica e o Facebook Invadiram a Privacidade de Milhões e Botaram a Democracia em Xeque" (2020)
[7] Surveillance capitalism unilaterally claims human experience as free raw material for translation into beharioral data (ZUBOFF, 2019, p. 27) (tradução nossa).

> "[...] sobre seu dispositivo, os sites que você acessa, as compras que faz, os anúncios que visualiza e sobre o uso que faz dos serviços deles, independentemente de ter ou não uma conta ou de estar conectado ao Facebook. Por exemplo, um desenvolvedor de jogos poderia usar nossa API para nos informar quais jogos você joga, ou uma empresa poderia nos informar sobre uma compra que você fez na loja dela. Além disso, recebemos informações sobre suas ações e compras online e offline de provedores de dados de terceiros que têm autorização para nos fornecer essas informações.
> (Disponível em https://www.facebook.com/about/privacy acesso em 28 abr 2020)

Esse tipo de autenticação, ou autorização (conforme exemplos destacados na figura 5) é conhecida por OAUTH (que em tradução livre significa padrão aberto para autorização). Nele o serviço de terceiro para o qual não queremos criar um novo par login/senha solicita ao FB ou GG que confirme, via token, que aquele usuário é realmente quem ele alega ser.

Figura 5 - Exemplos de autorização a serviços de terceiros operados a partir de OAUTH Facebook e/ou Google – Folha de São Paulo

Fonte: Folha de São Paulo. Disponível em: <https://www1.folha.uol.com.br/poder/2020/03/apos-ignorar-ministro-bolsonaro-diz-ter-vontade-de-baixar-decreto-para-populacao-poder-trabalhar.shtml> acesso em 29 abr 2020

O serviço de terceiro não tem acesso a senha, nem a dados que a política de privacidade dos serviços autenticadores prometem proteger ou não divulgar. O login social passa assumir o status de uma espécie de passaporte, apresentando os dados mínimos, ele é aceito como verdadeiro em função da confiança que o terceiro tem no emissor daquela autenticação. Conhecendo o funcionamento do OAUTH ele traz consigo as mesmas negociações e autorizações confiadas ao serviço que autentica o token - FB ou GG - mas não apresenta ícone que indique segurança. Portanto, acreditamos que a

segurança e confiança também são assumidas pelo serviço de terceiro ao aceitar esses dados. Tanto a relação entre serviço e usuário, quanto a imageria de segurança é substituída e assumida pelo serviço autenticador e seu logo.

Os serviços autenticadores, parte do objeto deste estudo, não servem como acesso a qualquer serviço de terceiro, eles constroem padrões de segurança que são protocolos que garantem uma díade segurança-confiança (entre os serviços autenticador e de terceiros - conforme figura 6).

Figura 6 - Exemplos de autorização a serviços de terceiros operados a partir de OAUTH FB e/ou Google – Spotify

Fonte: SPOTIFY. Disponível em https://accounts.spotify.com/pt-BR/login/ acesso em 20 jun 2020

O GG não proíbe que seus usuários autentiquem sua entrada em serviços de menor confiança, mas recomendam sua não feitura, conforme visualizamos na figura a seguir:

Figura 7 - Captura de tela da seção Apps menos seguros e a Conta do Google (dentro da área Central de Ajuda > Atividade suspeita)

Fonte: https://support.google.com/accounts/answer/6010255?hl=pt-BR acesso em 20 jun 2020

As respectivas áreas vinculadas a segurança em serviços autenticadores permitem visualizar a quais serviços de terceiros e qual tipo de informação foi fornecida a esses serviços, sendo possível revogar a autenticação, bem como denunciar sites e apps que esteja utilizando indevidamente os dados:

Figura 8 - Captura de tela do Google - Segurança da conta

Fonte: Google Disponível em <https://myaccount.google.com/secutiry> acesso em 20 jun. 2020.

É importante lembrar que os dados de usuários fornecidos para as grandes empresas globais de tecnologia em comunicação, como FB e GG, são utilizados para fins comerciais, ou seja, para monetização do modelo de negócio que sustenta o mercado: informação e publicidade, operacionalizando o "capitalismo de vigilância" (ZUBOFF, 2019). O que é fornecido ao FB sobre interesses pessoais, personalidade, emoções, deveria estar apresentado em sua política de privacidade[8], mas permitir o fornecimento de dados para terceiros via FB ou GG faz parte do que sustenta um ciclo. Ou seja, esses "parceiros" retroalimentam o FB, por exemplo, com informações sobre atividades de seus usuários através de uma espécie de vigilância na navegação que se perpetua mesmo fora da ambiência do FB.

Considerações Finais

Um dos importantes pesquisadores da comunicação das "novas" mídias, Lev Manovich (2001) defende que a ligação entre a interface e o usuário está relacionada, como mencionamos anteriormente, com uma tradição da nossa cultura "uma linguagem cultural que oferece seus próprios modos de representar a memória e a experiência humanas" (MANOVICH, 2001, p. 123). Portanto, observamos uma potencialidade na discussão das práticas de segurança e privacidade dos usuários de serviços autenticadores através do estudo da imageria da comunicação confidencial e segura. Como os dispositivos foram se tornando cada vez mais complexos, a tentativa de assegurar e criptografar o conteúdo tem um papel importante na história da comunicação e sua relação com outras áreas de estudo, desde a estatística, engenharia e a matemática.

Nesse sentido, é interessante pensar as imagens que são produzidas na rede para conduzir a experiência de segurança e que sugerem uma preocupação com a eficiência do segredo, seja por ferramentas de reconhecimento de imagens, checks de verificação,

[8] https://www.facebook.com/settings?tab=privacy&section=search&view e também https://www.facebook.com/about/privacy

chaves, mensagens codificadas, cadeados ou escudos, propõe pesquisar caminhos, que a partir do agir cartográfico, nesse perambular da web, vimos que serviços autenticadores funcionam como crachás, "chaves" e passaportes, abrindo-nos portas para o acesso a outros serviços de inúmeras ordens. Eles autenticam com certa presunção de veracidade os dados que fornecem aos terceiros, enquanto deixam seus usuários com a sensação de segurança e proteção daquele grande serviço ao qual confiam seus dados. Mas uma comunicação segura e sem erros é uma ilusão, a partir do conceito de capitalismo de vigilância, vimos que o sistema de codificação da internet hoje apresenta um tema de grande importância na discussão do espaço acadêmico, principalmente partindo de pesquisas que estimulem o debate acerca de melhores políticas de privacidade e segurança e o uso comercial a partir da retenção de dados de usuários fornecidos a terceiros por serviços autenticadores.

REFERÊNCIAS

BENJAMIN, Walter. **Magia e técnica, arte e política.** São Paulo: Brasiliense, 1989.

BENJAMIN, Walter. **Passagens**. Belo Horizonte: UFMG, 2006.

FACEBOOK. Disponível em**: <https://www.facebook.com/about/privacy>.** Acesso em: 20 mar. 2020.

FISCHER, G. D. Tecnocultura: aproximações conceituais e pistas para pensar as audiovisualidades. In: Kilpp, Suzana; Fischer, Gustavo Daudt. (Org.). **Para entender as imagens: como ver o que nos olha?.** 1ed. Porto Alegre: Entremeios, 2013, v. 1, p. 41-54.

FISCHER, Gustavo. Do audiovisual confinado às audiovisualidades soterradas em interfaces enunciadoras de memória. In: KILPP, Suzana (Org.); FISCHER, Gustavo D; LADEIRA, João Martins; MONTAÑO, Sônia. Tecnocultura audiovisual Temas, metodologias e questões de pesquisa. 1. ed. Porto Alegre: Sulina, 2015. p. 61-111.

FISCHER, Gustavo. Vida, morte e pós-morte do GeoCities: memória em denegeração/regeneração e nostalgia como crítica no Projeto One Terabyte of Kilobyte Age. **Anais do XXXIX Congresso Brasileiro de Ciências da Comunicação – INTERCOM**: São Paulo, 2016. Disponível em: http://portalintercom.org.br/anais/nacional2016/resumos/R11-2977-1.pdf

FLUSSER, Vilém. **Filosofia da caixa preta:** ensaios para uma futura filosofia da fotografia. Rio de Janeiro: Relume Dumará, 2002.

GOOGLE. Disponível em <**https://myaccount.google.com/secutiry**> acesso em 20 jun. 2020.

KAISER, Brittany. **Manipulados:** Como a Cambridge Analytica e o Facebook Invadiram a Privacidade de Milhões e Botaram a Democracia em Xeque. São Paulo: HarperCollins, 2020.

KILPP, Suzana. Dispersão-convergência: apontamentos para a pesquisa de audiovisualidades. In: MONTAÑO, Sonia; FISCHER, Gustavo; KILPP, Suzana (Org.). **Impacto das novas mídias no estatuto da imagem**. 1. ed. Porto Alegre: Sulina, 2012. v. 1, p. 223-238.

KILPP, Suzana. **A traição das imagens: espelhos, câmeras e imagens especulares em reality shows.** Porto Alegre: Entremeios, 2010

KRAPP, Peter. A short media history of influence operations. In: **Seminário Capes/PRINT Digital transformation and the humanities: contemporary technocultural dimensions for research in the social and human sciences.** São Leopoldo. Brasil, março 2020. Disponível em: https://www.dropbox.com/s/53664916whfyq51/Brazil%20slides-Peter_Krapp.zip?dl=0&file_subpath=%2FBrazil+slides%2Fmemes-brazil.pdf. Acesso em 20 abr. 2020.

KRAPP, Peter. **Beyond Schlock on Screen:** Teaching the History of Cryptology Through Media Representations of Secret Communications. Disponível em https://www.ep.liu.se/ecp/158/009/ecp19158009.pdf. Acesso em 20 abr. 2020.

MANOVICH, Lev. El software en acción. IN **El software toma el mando** (2014). Disponível em:https://www.academia.edu/7425153/2014_-_El_software_toma_el_mando_traducci%C3%B3n_a_Lev_Manovich_ (p. 213-250)

MANOVICH, Lev. **The Language of New Media**. Massachusetts: The MIT Press, 2001.

PENKALA, Ana Paula. **O mal-estar na visualização e outras estéticas**: da imageria do audiovisual pós-moderno. Tese de doutorado. 2011. Disponível em: http://hdl.handle.net/10183/30199. Acesso em 20 jun. 2020.

POLIDORO, Bruno. Cinema, vídeo, digital: a virtualidade do audiovisual. **Revista Famecos**
http://revistaseletronicas.pucrs.br/ojs/index.php/famecos/article/download/4153/3165

RANCIÈRE, Jacques. **O Destino das imagens**. Rio de Janeiro: Contraponto, 2013.

SPOTIFY. Disponível em <**https://accounts.spotify.com/pt-BR/login/**> acesso em 20 jun 2020

WOLF, Mauro. **Teorias da Comunicação.** 2ª ed. Lisboa: Editorial Presença, LDA. 1992.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism:** The Fight for a Human Future at the New Frontier of Power. Londres: Profile Books Ltd. 2019.