XXI ENANCIB
Encontro Nacional de Pesquisa em Ciência da Informação
50 anos de Ciência da Informação no Brasil: diversidade, saberes e transformação social
Rio de Janeiro • 25 a 29 de outubro de 2021

XXI Encontro Nacional de Pesquisa em Ciência da Informação – XXI ENANCIB

GT-5 – Política e Economia da Informação

PRÁTICAS DE COMPETÊNCIA CRÍTICA EM INFORMAÇÃO NO COMPARTILHAMENTO DE DADOS BIOMÉTRICOS EM APLICATIVOS

PRATICES OF CRITICAL INFORMATION LITERACY FOR SHARING BIOMETRIC DATA IN APPLICATIONS

Aneli Beloni - Instituto Brasileiro de Informação em Ciência e Tecnologia/Universidade Federal do Rio de Janeiro (IBICT/UFRJ**)**
Arthur Coelho Bezerra - Instituto Brasileiro de Informação em Ciência e Tecnologia/ Universidade Federal do Rio de Janeiro (IBICT/UFRJ**)**

Modalidade: Resumo expandido

Resumo: Atualmente, existem aplicativos para *smartphone* que coletam dados biométricos para diferentes fins, nem sempre éticos. Práticas de competência crítica em informação para quem compartilha seus dados pessoais são um caminho para a conscientização das possibilidades de uso das informações concedidas, e também para exigir transparência das empresas sobre a finalidade para a qual coletam e usam tais dados. Por meio de uma metodologia de investigação explicativa, nosso objetivo é indicar alguns passos que podem ser seguidos por quem utiliza aplicativos como Whatsapp e outros que fazem coleta de dados biométricos, a fim de estimular autonomia informacional e consciência crítica nos usuários.

Palavras-Chave: competência crítica em informação; dados biométricos; dados pessoais; privacidade; aplicativos.

Abstract: Currently, there are smartphone apps that collect biometric data for different purposes, which are not always ethical. Critical information literacy practices for those who share your personal data are a way to raise awareness of the possibilities of use of the information provided, and also to demand transparency from companies about the purpose for which they collect and use such data. Through an explanatory research methodology, our objective is to indicate some steps that can be followed by those who use applications such as Whatsapp and others that collect biometric data, in order to encourage informational autonomy and critical awareness in users.

Keywords: critical information literacy; biometric data; personal data; privacy; smartphones apps.

1 INTRODUÇÃO

Os dados que têm valor de destaque no atual regime de informação possuem uma vasta tipologia. Tais dados podem ser pessoais, médicos, estatísticos, de linguagem de programação,

de pesquisa e, dentre muitos outros tipos, podem ser biométricos. Os dados biométricos são compostos pelas características físicas ou comportamentais – como impressões digitais, íris dos olhos, DNA, rosto, voz, geometria da mão etc. – que são capazes de estabelecer a identidade de um indivíduo (JAIN; FLYNN; ROSS; 2008).

Para Guennouni, Mansouri e Ahaitouf (2019), a vantagem de usar os recursos biométricos é que todos são universais, mensuráveis, únicos e, geralmente, permanentes. Os mesmos autores consideram que os aplicativos que utilizam a biometria tentam, de alguma forma, facilitar o modo de vida e evitar fraudes.

A biometria apresenta benefícios, mas exige uma segurança muito grande para seu armazenamento e uso, porque no caso de vazamento dos dados biométricos a dificuldade para recadastramento é enorme ou nem mesmo é possível. Um cartão de crédito clonado, por exemplo, pode ser cancelado e adquirir-se um novo, mas quando há vazamento de uma impressão digital não há como fazer a troca.

> No cenário atual, o corpo humano vem se tornando fonte primordial de informações, com o uso e o tratamento cada vez mais veloz e sofisticado e gradativamente mais disseminado e banalizado de dados biométricos – dados que trazem informações da pessoa e são captados a partir do corpo humano, com o fim de identificá-las precisamente, tendo em vista a unicidade de cada pessoa e suas características físicas peculiares – baseada em uma mentalidade criada por uma atmosfera de medo que, em nome da segurança, incorpora os elementos físicos do corpo nas engrenagens tecnológicas, para múltiplos fins, desde a certificação da identidade até a ilimitada vigilância e o controle da pessoa humana (FRANCO, 2009, p. 13).

A coleta dos nossos dados é feita por meio de uma vigilância constante, o que ameaça o direito à privacidade, muitas vezes esse direito é totalmente ignorado. A vigilância está ligada ao poder, especialmente para Foucault (1999) e Deleuze (1992) e, na atual conjuntura social, regida pela era dos dados e pelo "capitalismo de vigilância" (ZUBOFF, 2019), empresas como Google e Facebook possuem um poder que concede a elas uma certa soberania (BEZERRA, 2017).

Este trabalho se inicia e se justifica pelo fato de que estamos imersos na dualidade entre os benefícios e os perigos: os sistemas biométricos vêm sendo implantados em bancos, aeroportos, academias de ginástica, supermercados e outros estabelecimentos comerciais, e mesmo organizações governamentais e hospitalares vêm aderindo ao uso de ferramentas biométricas. A coleta dos dados biométricos em *smartphones*, por sua vez, tem naturalizado a presença dessa tecnologia entre o público em geral.

Os *smartphones*, na atualidade, podem ser desbloqueados pelas impressões digitais ou reconhecimentos faciais, um recurso prático que evita que outras pessoas, que não sejam o proprietário, acessem o aparelho. Porém, ao cadastrar a digital no *smartphone*, para quem o dado está sendo concedido? A digital do usuário está segura?

Muitos aplicativos também fazem uso da impressão digital e outros recursos como a voz e a face. Para utilizar o serviço, são exigidos dados pessoais e nem sempre os usuários são informados sobre a coleta, o armazenamento e a segurança desses dados, bem como sobre a finalidade e sobre o uso dos mesmos. Por essa razão, acreditamos que as práticas de competência crítica em informação podem auxiliar as pessoas, em geral, a entender o que estão compartilhando e as possibilidades de desdobramento desse compartilhamento. Consideramos de grande relevância este e outros estudos que estimulam e orientam os usuários desse universo digital ao desenvolvimento do pensamento crítico.

O uso de dados biométricos pode ser "bom" ou "mau", a depender dos envolvidos, da forma e da finalidade a qual os dados serão submetidos. Sendo assim, este trabalho segue o método de investigação explicativa, com o objetivo de mostrar a ambiguidade em torno da coleta e uso dos dados biométricos, assim como de orientar as pessoas, didaticamente, a observarem, por meio da prática da competência crítica em informação, como se dá a concessão e a coleta de seus dados em aplicativos de *smartphones*, especialmente o Whatsapp, atualmente com mais de 2 bilhões de usuários em todo o mundo.

A base para compreensão de que a competência crítica em informação é um caminho para amplitude do aprendizado, estímulo ao questionamento e compreensão de um sujeito parte da concepção de que:

> O conceito de competência crítica em informação aponta para as perspectivas de emancipação social, colocando-se como um dos possíveis caminhos para a práxis transformadora no cerne do regime de informação em vigor. Aqui, são destacadas as propostas teóricas que trazem, ainda que indiretamente, a presença dos preceitos da teoria crítica, como no caso dos estudos da *critical information literacy* que dialogam com a pedagogia crítica de Paulo Freire (BEZERRA, 2019, p. 30).

A competência crítica em informação tem em sua estrutura conceitual a preocupação com a liberdade, o empoderamento, o questionamento, a aprendizagem, a ética e, como o próprio nome já diz, a crítica. A prática da competência crítica em informação envolve todos esses elementos, seja como ação e/ou como finalidade (SCHNEIDER, 2019).

Tal prática estimula nos indivíduos a escolha consciente entre fazer ou não fazer algo, bem como entender o que já está sendo feito e as consequências disso para si e para outros envolvidos no contexto. Assim, surge a pergunta: como praticar a competência crítica em informação no compartilhamento de dados biométricos, de modo a garantir segurança e privacidade? Esse foi a questão que norteou esse trabalho, desse modo, apresentaremos, aqui, algumas ações que podem ser exercidas por qualquer indivíduo alfabetizado que utilize um *smartphone*, no que tange o compartilhamento de seus dados biométricos, a fim de estimular autonomia informacional e consciência crítica nos usuários.

2 *SMARTPHONES* E APLICATIVOS QUE COLETAM DADOS BIOMÉTRICOS

A apresentação de falhas na tentativa de que as máquinas identifiquem um sujeito específico foi a principal motivação para o uso dos dados biométricos, pois a biometria minimiza os erros na comprovação de que alguém seja, de fato, quem diz ser. Com as tecnologias avançadas, ferramentas e métodos para identificação biométrica estão cada vez mais precisos. Jain, Flynn e Ross (2008) afirmam que a última década viu um crescimento significativo nas buscas biométricas, o que culminou no desenvolvimento de algoritmos robustos e eficientes para extração e correspondência de recursos, de sensores inovadores, de metodologias de teste aprimoradas e novas aplicações. Esse rápido crescimento também destaca os desafios associados ao projeto e implementação de sistemas biométricos, pois a realidade é que o reconhecimento biométrico é um grande desafio por si só.

Atualmente, um dos maiores coletores de dados biométricos é o *smartphone*, um item individual que o proprietário utiliza para diversas finalidades pessoais. A privacidade é o que justifica que o aparelho seja bloqueado e que o seu desbloqueio seja realizado por meio de senhas e, também, por dados biométricos, como reconhecimento facial e leitores de impressão digital. Entendemos que esse formato se caracteriza pela intenção de garantir que somente o dono possa ter o controle de acesso conforme ao *smartphone*, conforme seu desejo e autorização.

Os aplicativos (ou *apps*) que são baixadas em um *smartphone* são de interesse do proprietário e se entende que ele a usará por vontade própria. Existem diversos aplicativos que se baseiam nos dados biométricos, como nos exemplos apresentados abaixo:

a) aplicativos de banco: utilizam a digital gravada no smartphone e comparam com a digital gravada no próprio banco para autenticar sua identidade. Atualmente, alguns já estão aderindo, também, ao reconhecimento facial;
b) aplicativos relacionados ao Tribunal eleitoral: utilizam a digital gravada no smartphone e comparam com a digital gravada no próprio Tribunal Regional eleitoral;
c) aplicativos para mídias sociais (*Facebook, Instagram, Whatsapp*): utilizam a câmera do *smartphone* para o uso de técnicas de reconhecimento facial e conseguem acesso à face, utilizam microfone e ganham acesso à voz dos usuários;
d) Aplicativos de edição de fotos: utilizam câmera e ficam com acesso à face;
e) Aplicativos de videoconferência (*Skype, Google Meet, Zoom*): utilizam câmera e conseguem acesso à face; utilizam microfone e ganham acesso à voz;
f) aplicativos relacionados à vida saudável: monitoram e registram comportamentos informados pelo usuário, como os *apps* para corrida, controle menstrual, ingestão de água etc.;
g) aplicativos vinculados a *smartwhatches*: monitoram e registram dados biológicos e comportamentais.

É cada vez mais notório que nossos dados circulam pela rede e que empresas e governos coletam nossos dados, inclusive os biométricos, a todo instante, mas raramente é esclarecido para quê e como esses dados serão utilizados. Infelizmente, em muitas situações, se não compartilharmos os nossos dados, não teremos como utilizar o aplicativo que desejamos; porém, é um direito sermos informado sobre a finalidade da coleta e aplicabilidade da informação que nossos dados irão gerar. Desse modo, estabelecemos a conexão com a competência crítica em informação para que a população entenda esse cenário e possa conhecer e seus direitos. Para Franco,

> A total falta de reflexão e debate sobre os pertinentes limites éticos e jurídicos vem permitindo que este cada vez mais sofisticado e invasivo mecanismo de intervenção, constituído pela coleta e armazenamento de dados biométricos, possa se agigantar em um abastado arsenal de informações pessoais de caráter sensível, armazenadas não apenas pelo Estado, mas, também, por diversas instituições privadas (FRANCO, 2009, p. 14).

Kindt (2013) corrobora com a autora acima e, numa perspectiva jurídica, defende a explicação do funcionamento dos sistemas biométricos, em termos gerais, para não

especialistas. O autor compartilha várias sugestões para um marco regulatório visando reduzir os riscos dos sistemas biométricos, o que inclui uma determinada limitação à coleta e ao armazenamento de dados biométricos, bem como medidas técnicas, que podem influenciar a proporcionalidade do processamento.

Sabemos que uma das missões mais árduas nesse cenário é equilibrar os benefícios dos aplicativos que queremos utilizar e os dados que realmente precisamos compartilhar com as empresas, com o governo, com hospitais e demais instituições governamentais e comerciais que, de forma generalista, possuem seus próprios interesses políticos e econômicos.

3 A PRÁTICA DA COMPETÊNCIA CRÍTICA EM INFORMAÇÃO

A seguir, utilizando como exemplo o WhatsApp em um aparelho com sistema operacional Android, apresentaremos alguns passos que qualquer usuário pode seguir com relação ao compartilhamento de seus dados biométricos em aplicativos. Destacamos que o desenvolvimento desses passos foi inspirado na perspectiva crítica da socióloga Shoshana Zuboff (2019) que apresenta diversos estudos nos alertando sobre as estratégias adotadas pelo capitalismo de vigilância.

Passo 1: Pergunte-se e verifique **qual a finalidade do aplicativo**; antes de baixar, veja o que ele oferece, se é o que você procura e se você realmente precisa. O Whatsapp, por exemplo, é um *app* para troca de mensagens instantâneas; se a intenção é interagir, conversar e trocar mensagens, o aplicativo atenderá seu desejo.

Passo 2: Verifique **qual é a empresa responsável**, se há uma identificação de quem está disponibilizando aquele *app* (em alguns casos a informação é visível na própria loja onde o *download* é feito, em outros casos só fica explicito após abrir aplicação depois de baixar). O Whatsapp apresenta a responsável como Whatsapp LLC. Todavia, essa é uma empresa que faz parte da grupo comercial do Facebook e essa informação só aparece após baixar o aplicativo; por isso, nesta etapa recomendamos pesquisar pela empresa que está disponibilizando o *app*.

Passo 3: Verifique **quais são os recursos que o aplicativo pede permissão para ter acesso** em seu *smartphone*. Esse é um passo que exige atenção, pode ser feito dentro da Playstore ou Apple Store em “mais informações”. Nesse momento, você saberá quais dados, além dos que você informa, poderão ser coletados, e é nesta etapa que identificamos se o

aplicativo fará uso de dados biométricos. Aconselhamos comparar as ferramentas solicitadas com as finalidades do aplicativo para verificar se são compatíveis, pois no caso de um aplicativo de edição de fotos pedir acesso ao microfone, por exemplo, é fundamental estar em alerta e avaliar se vale a pensa fazer uso daquele aplicativo, uma vez que o recurso exigido não condiz com a finalidade do *app*. No Whatsapp, vemos que alguns dados biométricos são coletados, mas percebemos que são condizentes com a finalidade do aplicativo, como apresenta a figura 1.

Figura 1 - Recursos requeridos para uso do Whatsapp.

Fonte: Elaborado pelos autores.

Passo 4: Verifique se possui **políticas e termos de serviços**; se sim, verifique se é uma leitura curta ou extensa e, no caso de ser extensa, o que geralmente é, concentre-se em verificar se é obrigatória a aceitação dos termos para utilizar o aplicativo. Se novamente a resposta for sim, não recomendamos aceitar sem ler, mas entendemos que a leitura nem sempre é compreensível e, para esses casos, temos o direito de exigir que a política e os

termos sejam apresentados para leitura de não especialista. Entretanto, sabemos que é comum a aceitação dos termos sem que haja uma análise, minimante, superficial; Romeiro (2012), em seu texto intitulado “Não li e concordo”, apresenta o resultado de uma pesquisa da Universidade Stanford que revela que 97% das pessoas não leem os termo e vão direto até o “Li e concordo”. O Whatsapp tem políticas extensas, os termos também são extensos, e na própria Play Store é possível que só é possível usar a aplicação após a concordância com os termos de serviços e políticas da empresa fornecedora, como apresenta a figura 2.

Figura 2 - Obrigatoriedade de aceitação de Termos de serviço para uso do aplicativo Whatsapp.

Fonte: Elaborado pelos autores.

Passo 5: Observe o **comportamento do aplicativo durante o uso**. Uma vez que a coleta dos dados biométricos for autorizada, é possível que sua fala esteja sendo gravada ou que sua câmera seja ativada, mesmo sem sua solicitação. Como identificar isso? No caso do Whatsapp, veja se aparecem propagandas relacionadas às suas conversas fora da aplicação; se sim, não significa que você tenha que desinstalar o aplicativo, mas fará perceber como a empresa se comporta no uso das ferramentas de seu *smartphone* e de seus dados biométricos.

Se durante a realização de algum desses passos algo incomodar, você pode desistir da aplicação ou prosseguir, porém a continuidade do processo deve ser pautada na busca pelos seus direitos e sem se eximir do comprometimento de uso envolvido. Também é importante salientar que as empresas têm deveres para com os usuários, embora nem sempre os cumpra. Nesse caso, podemos e devemos fazer valer o que nos cabe. Finalmente, defendemos que, além de uma postura legal, dentro das exigências legislativas, a questão ética seja pautada e aderida por todas as partes envolvidas: isso é competência crítica em informação na prática.

Lembramos que dados biométricos, diferentemente de outros dados, não são alteráveis. Salvo em casos de acidentes e deformações, o vazamento ou exposição de um dado biométrico tem efeitos maiores que os demais, e essa é a razão deste alerta. Promovemos a competência crítica em informação a fim de despertar o questionamento, o pensamento crítico, a privacidade e o uso ético para com os dados biométricos no cenário atual.

4 CONSIDERAÇÕES FINAIS

O arcabouço teórico da competência crítica em informação tem crescido e está ganhando robustez, mas consideramos cada vez mais pertinente a apresentação didática para a aplicabilidade. Essa percepção é uma reflexão concernente à importância do fortalecimento da relação entre a academia e a sociedade, da promoção da comunicação científica para que aquilo que a academia produz seja acessível à população em geral, o que motiva nossa intenção de demonstrar a complementaridade de um estudo e uma orientação para prática.

Frente à realidade do negacionismo científico e todas as táticas de desinformação que são desenvolvidas frequentemente e assolam a sociedade, a proposta de ações com objetivos informativos e estímulo ao pensamento crítico é uma maneira de minimizar os males causados a diversos indivíduos por causa da ausência ou pelo uso malicioso da informação. Consideramos que a apresentação de práticas de competência crítica em informação seja uma forma de incentivar a aproximação da academia à sociedade.

Teoria e prática devem andar juntas e este trabalho apresenta apenas uma das possíveis ações que podem ser realizadas com os estudos advindos da teoria crítica, da pedagogia crítica, da ética da informação, da promoção da cidadania e tudo que envolve a competência crítica em informação. Deste modo, concluímos que este trabalho pode ser compartilhado com qualquer indivíduo no intuito de informar e pode ser um forma de estímulo para realização de outras ações e práticas da competência crítica em informação.

REFERÊNCIAS

BEZERRA, Arthur. Teoria Crítica da Informação: proposta teórico-metodológica de integração entre os conceitos de regime de informação e competência crítica em informação. *In*: BEZERRA, Arthur; SCHNEIDER, Marco; PIMENTA, Ricardo; SALDANHA, Gustavo (org.). **iKritika**: estudos críticos em informação. Rio de Janeiro: Garamond, 2019. p. 15-72.

BEZERRA, Arthur. Vigilância e cultura algorítmica no novo regime de mediação da informação. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 22, n. 4, p. 68-81, dez. 2017. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2936/1979. Acesso em: 11 ago. 2021.

DELEUZE, G. Post-scriptum sobre as sociedades de controle. *In*: DELEUZE, Gilles. **Conversações**: 1972-1990. Rio de Janeiro: Ed. 34, 1992, p. 219-226.

FRANCO, Carolina Mendes. **A pessoa humana resumida a um dado corporal**: considerações sobre o tratamento adequado aos dados biométricos. 2009. 105 f. Dissertação (Mestrado em Direito) – Universidade do Estado do Rio de Janeiro, Faculdade de Direito, 2009.

FOUCAULT, M. **Vigiar e punir**: nascimento da prisão. 20. ed. Petrópolis: Vozes, 1999.

GUENNOUNI, Souhail; MANSOURI, Anass; AHAITOUF, Ali. Biometric systems and their applications. **IntechOpen**. [*S.l*], march 2019. Disponível em: https://www.intechopen.com/books/visual-impairment-and-blindness-what-we-know-and-what-we-have-to-know/biometric-systems-and-their-applications. Acesso em: 17 abr. 2021.

KINDT, Els J. **Privacy and data protection issues of biometric applications**. [*S.l.*]: Springer, 2016.

JAIN, Anil; FLYNN, Patrick; ROSS, Arun. **Handbook of Biometrics**. [New York]: Springer-Verlag, 2008.

ROMEIRO, Luiz. Não li e concordo. **Super Interessante**. [*S.l.*], 19 ago. 2012. Disponível em: https://super.abril.com.br/tecnologia/nao-li-e-concordo/. Acesso em: 19 jun. 2021.

SCHNEIDER, Marco. Competência crítica em informação (em 7 níveis) como dispositivo de combate à pós-verdade. *In*: BEZERRA, Arthur; SCHNEIDER, Marco; PIMENTA, Ricardo; SALDANHA, Gustavo (org.). **iKritika**: estudos críticos em informação. Rio de Janeiro: Garamond, 2019. p. 73-116.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. Nova York: PublicAffairs, 2019.