ARTIGO

ÉTICA NO USO DE DADOS BIOMÉTRICOS: HISTERIA OU UMA PREOCUPAÇÃO COERENTE?

POR

Anne Magály de Paula Canuto

anne.canuto@ufrn.br

Dados biométricos

O desenvolvimento de técnicas mais seguras na identificação de pessoas é uma necessidade vigente diante de uma sociedade imensamente interconectada. O constante avanço das tecnologias contribui para uma interação cada vez maior entre as pessoas, e à medida que essa interação e o acesso à informação aumenta, também se sobrepõem os golpes, surgindo assim, a necessidade do desenvolvimento de técnicas de segurança mais eficientes. Dentre as soluções com maior potencial para alcançar tais objetivos, destacam-se as análises de características biológicas [1]. É inegável que cada vez mais o uso de tais características biológicas, conhecidas como biometrias, tem sido utilizado em tarefas do nosso dia-a-dia, principalmente na determinação da autenticidade de uma pessoa. O uso destas características tem superado cada vez mais a utilização dos métodos tradicionais, tais como, senhas e cartões, em termos de eficiência e segurança [1]. Dentre as razões para a popularização, podemos afirmar que as biometrias são caracterizadas por serem únicas e por pertencerem ao indivíduo, não podendo ser perdidas, esquecidas ou roubadas. Isso faz com que sistemas de segurança baseados em seus princípios tenham surgido como uma evolução na autenticação e identificação de indivíduos.

Existe uma grande diversidade de modalidades de biometrias, dentre os mais populares estão o reconhecimento de assinaturas, faces e impressões digitais [2]. Concomitante a isso, existem outros sistemas biométricos que se utilizam de íris, retina, voz, geometria da mão, termogramas faciais entre outros [2].

Preocupações legais em torno de dados biométricos

Independente da modalidade de biometria utilizada, existem alguns aspectos éticos no uso de tais dados que precisam ser analisados de forma mais detalhada para não trazer mais perigos que benefícios, que envolvem o mal uso e ganho comercial das empresas com os dados, além de questões sociais de identidade, cidadania e vigilância, entre outras. Para tanto, dois aspectos são fundamentais para o correto uso de dados biométricos: segurança e legalidade do uso [3].

Segurança de dados biométricos: em sistemas de autenticação, por exemplo, a segurança é considerada um aspecto fundamental e, quando usamos biometrias, enfrentamos um problema ainda maior relacionado à segurança de dados biométricos, que ocorre quando há o comprometimento dos dados biométricos (roubo ou cópia das características). Esta preocupação é aumentada devido às características biométricas estarem relacionadas permanentemente ao usuário, elas não podem ser alteradas (revogadas), caso sejam comprometidas. Por exemplo, se uma base de dados de senhas de uma empresa é roubada, a empresa convoca seus clientes para fornecerem uma nova senha e o problema está resolvido. No caso de dados biométricos, em caso de furto, não é possível fornecer um novo conjunto de dados e o impacto do furto de dados biométricos tem um impacto enorme tanto para a empresa quanto para os seus usuários. Dessa forma, se torna necessária a utilização de técnicas de segurança de dados eficientes e que possibilitem a utilização de uma característica biométrica sem que haja comprometimento na segurança desses dados. Uma das técnicas empregadas em tais soluções é denominada de biometria cancelável (revogável), que aplica uma transformação sobre os dados biométricos e a consequente utilização apenas dos dados transformados nos sistemas de autenticação [3]. Assim, em caso de furto, os dados originais estão preservados. Uma técnica alternativa é aumentar o nível de segurança dos algoritmos de criptografia a serem utilizados nos dados biométricos.

Legalidade do uso de dados biométricos: é de conhecimento geral que os dados pessoais de qualquer pessoa são solicitados constantemente por diferentes entidades, públicas e privadas e, uma vez fornecidos, pouco controle temos sobre eles. É importante ressaltar que somos os titulares desses dados e que nosso CPF, RG, número de telefone pessoal, endereço, etc nos pertencem sim. A utilização indevida e sem consentimento destes dados configura uma infração. Com dados biométricos,

devido à característica de irrevogabilidade, a infração deveria ser considerada ainda mais grave.

Destarte, com a abrangência do uso de dados biométricos, é preciso de leis que regularizem diferentes aspectos do seu uso, como cobertura variável dos dados, tanto para consumidores quanto para funcionários, e devem ser definidos para diferentes setores da indústria e do comércio. Estas leis têm o objetivo de contribuir para resolver este "labirinto" atual com várias incertezas legais. Nos EUA, por exemplo, as leis sobre o uso de dados biométricos são altamente fragmentadas – existem leis diferentes em diferentes estados americanos. Por outro lado, na União Europeia, existe o GDPR (do Inglês *General Data Protection Regulation*) que é o Regulamento Europeu 2016/679 que abrange a proteção de pessoa física no que se refere ao processamento de dados pessoais e à livre circulação desses dados. O GDPR tem delineamentos claros para categorizações de dados confidenciais, incluindo dados biométricos.

No Brasil, inspirada no GDPR, foi promulgada em 14 de agosto de 2018 a Lei nº 13.709, que ficou conhecida como a Lei Geral de Proteção de Dados (LGPD) [4]. De maneira geral, trata-se de um dispositivo legal que busca fornecer às pessoas um efetivo controle de seus dados pessoais. No seu art. 5, II, a LGPD define os dados pessoais sensíveis de forma taxativa e dados biométricos são considerados dados sensíveis. Para tal, a LGPD ainda dispõe de bases legais diferenciadas para o processamento destes dados sensíveis, no art. 11 da referida lei, restringindo as hipóteses do tratamento e disponibilização dos dados biométricos coletados. É inegável que a LGPD é um grande avanço na regulação do uso de dados biométricos, mas ainda precisamos definir formas de garantir o cumprimento da lei, assim como uma boa fiscalização do seu funcionamento. Além disso, ainda é preciso tratar de forma mais clara alguns aspectos importantes que são importantes para dados biométricos.

Passos necessários para o amplo e seguro uso de dados biométricos

Há muitos benefícios na utilização de dados biométricos, mas essas preocupações éticas não podem e não devem ser ignoradas. Os profissionais especialistas em segurança de dados devem analisar esse cálculo mais amplo quando resolver utilizar dados biométricos em uma empresa de forma segura e as seguintes sugestões podem ajudar.

1. Realize uma análise completa e contextualizada dos impactos do uso de dados biométricos: Esta análise é importante tanto no contexto da empresa quanto em todo o seu ecossistema. Por exemplo, o uso de dados biométricos na área da saúde pode ter um conjunto bem diferente de benefícios, ameaças e desafios técnicos e legais do que no contexto automotivo. Desta forma, uma análise completa também deve envolver uma abordagem multidisciplinar, incorporando conhecimentos em vários aspectos para um determinado contexto.

2. Priorize a diversificação de formas de autenticação de usuários.

A utilização de dados biométricos é uma das formas de autenticação. Outras formas incluem PINs, senhas e perguntas, entre outras. A diversificação pode ser feita dentro das diferentes modalidades de dados biométricos (reconhecimento biométrico multimodal [6]) ou misturando com outras formas de autenticação. Ao optar por outras formas de autenticação além dos dados biométricos pode preservar a segurança dos dados sem sacrificar a conveniência de sua utilização.

3. Garanta a segurança dos dados biométricos. Dada a diversidade de riscos associados ao uso de dados biométricos, é extremamente importante compensar as vulnerabilidades de varredura biométrica com segurança – por exemplo, exigindo fatores adicionais ao usar algoritmos de reconhecimento ou utilizando técnicas de criptografias que sejam mais eficientes. Quando se trata de dados biométricos, as preocupações com segurança excedem em muito as paredes de qualquer empresa e devem ser tratadas com muito cuidado.

Referências

1. DERBEL, Nabil; KANOUN, Olfa (Ed.). Advanced Methods for Human Biometrics. Springer, 2021.
2. SUN, Zhenan et al. Opportunities and Challenges for Biometrics. In: China's e-Science Blue Book 2020. Springer, Singapore, 2021. p. 101-125.
3. CAMPISI, Patrizio. Security and privacy in biometrics. London: Springer, 2013.
4. —-, https://gdpr-info.eu/.
5. —-, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
6. BALA, Neeru; GUPTA, Rashmi; KUMAR, Anil. Multimodal biometric system based on fusion techniques: a review. Information Security Journal: A Global Perspective, v. 31, n. 3, p. 289-337, 2022.

ANNE M P CANUTO é Professora Titular do Departamento de Informática e Matemática Aplicada (DIMAp) na Universidade Federal do Rio Grande do Norte. Atua na área de Inteligência Artificial, Aprendizado de Máquina e Autenticação biométricas, tendo publicado mais de 150 artigos científicos em congressos e periódicos. Sua pesquisa tem se focado na melhoria das estruturas de classificação existentes, visando melhorar seu desempenho na tarefa de classificação, incluindo a autenticação de usuários utilizando dados biométricos.