Pablo Gobira, Emanuelle de Oliveira Silva*

Sobre o uso dos *Biometric Identification Systems* (BISs) e a Inteligência Artificial (IA): das biometrias autobiográficas às biografias biométricas [1]

*

Pablo Gobira é Professor doutor da Escola Guignard (UEMG), do PPGArtes (UEMG) e do PPGGOC (UFMG). Pesquisador Produtividade (CNPq). Membro pesquisador e gestor de serviços da Rede Brasileira de Serviços de Preservação Digital (IBICT/MCTIC). Coordenador do grupo de pesquisa (CNPq) Laboratório de Poéticas Fronteiriças [http://labfront.tk]. Escritor e editor de diversos livros e artigos das áreas de curadoria, criação e produção das artes digitais e relações entre arte, ciência e tecnologia. *<pablo.gobira@uemg.br>*
ORCID: 0000-0002-3054-2383

Emanuelle de Oliveira Silva é Mestranda em artes do PPGArtes (UEMG), membro do grupo de pesquisa (CNPq) Laboratório de Poéticas Fronteiriças [http://labfront.tk]. *<mrsmaahlem@gmail.com>*

Resumo Este artigo é fruto de pesquisa desenvolvida no Laboratório de Poéticas Fronteiriças (http://labfront.tk - CNPq/UEMG), um grupo de pesquisa, desenvolvimento e inovação que se propõe pensar as fronteiras das relações entre arte, ciência e tecnologia. Este texto, portanto, tem como objetivo apresentar uma análise das aplicações, influências e possíveis resultados do uso indiscriminado dos *Biometric Identification Systems* (BISs), os Sistemas de Identificação Biométrica. Propomos aqui debater como os requerimentos e aplicações específicas, necessárias para possibilitar as identificações biométricas, geram um problema social (no campo biográfico) que extrapola os limites da privacidade de dados de seus usuários, especialmente quando se passa a tratá-los com as Inteligências Artificiais (IAs).

Palavras chave Sistemas de Identificação Biométrica, Inteligência Artificial, Autobiografia, Biografia.

The use of Biometric Identification Systems (BISs) and the Artificial Intelligence (AI): from autobiographic biometry to biometric biographies

Abstract *The paper presented here comes from the research developed in Laboratório de Poéticas Fronteiriças (http://labfront.tk - CNPq/UEMG), a research, development and innovation group that proposes to think the barriers of the relationship between art, science and technology. Therefore, this paper aims to introduce an analysis of the applications, influences and possible results of the indiscriminate use of Biometric Identification Systems (BISs). We want to debate how all of the specific requirements and applications, needed in order to make biometric identifications possible, end up creating a social problem (in the biographic field) that goes beyond the matter of data privacy from its users, specially when they are applied with Artificial Intelligences (AIs).*

Keywords *Biometric Identification Systems, Artificial Intelligence, Autobiography, Biography.*

Sobre el uso de Biometric Identification Systems (BISs) y la Inteligencia Artificiales (AI): de las biometrías autobiográficas a las biografías biométricas

Resumen *Este artículo es resultado de una investigación realizada en el Laboratorio de Poéticas Fronterizas (http://labfront.tk - CNPq/UEMG), grupo de investigación, desarrollo e innovación que propone pensar las fronteras de las relaciones entre arte, ciencia y Tecnología. Este texto, por tanto, pretende presentar un análisis de las aplicaciones, influencias y posibles resultados del uso indiscriminado de los Sistemas de Identificación Biométrica (BISs), los Sistemas de Identificación Biométrica. Proponemos aquí discutir cómo los requisitos y aplicaciones específicas, necesarias para habilitar identificaciones biométricas, generan un problema social (en el ámbito biográfico) que va más allá de los límites de la privacidad de los datos de sus usuarios, especialmente cuando se trata de tratarlos con Inteligencia Artificial. (IA).*

Palabras clave *Sistemas de Identificación Biométrica, Inteligencia Artificial, Autobiografía, Biografía.*

Introdução

O futuro sempre foi uma janela pela qual olhamos na esperança de encontrar respostas ou desenvolvimentos aos quais ainda não temos acesso. Apesar de imprevisível, nós, seres humanos, entendemos que se uma coisa pode ser imaginada ela pode, muito provavelmente, ser criada em alguma instância da realidade. Foi essa a ideia que originou os aparatos futurísticos e tecnológicos criados para a série Star Trek - Jornada nas Estrelas, na década de 1960. Dentre todos os aparelhos alienígenas que foram introduzidos aos telespectadores graças ao show, provavelmente o mais intrigante e fascinante foi o fato de que a USS Enterprise, a nave espacial principal da série, não somente tinha um comando ativado por voz, como apresentava um sistema de reconhecimento de voz. Ela era capaz de diferenciar qual integrante da nave estava dando uma ordem.

Essa pode ter sido a primeira vez que tal tecnologia tenha sido introduzida ao público, mas definitivamente não foi a última. Séries de TV e filmes tiveram um papel importante na construção da ideia de uma tecnologia que pode reconhecer o usuário, de maneira recorrente através dos anos, despertando a curiosidade em seus telespectadores. Essa, talvez, pode ser considerada uma das razões pela qual estamos, agora no século XXI, tão bem adaptados e, de certa forma, dependentes em medidas de segurança e aplicações diversas que necessitam de alguma característica única do usuário, seja sua voz, sua digital, seus olhos ou seu rosto, para permitir acesso às suas funcionalidades.

O uso de "características biológicas ou comportamentais distintas para identificar indivíduos", é conhecido como biometria. A biometria é um tipo de sistema que existe devido à união de diversos campos de conhecimento como ciência da computação, engenharia, ciências da cognição, biologia e segurança (DUNSTONE; YAGER, 2009, p. 3. Tradução nossa).

Desde o início do século XXI as várias facetas dos sistemas biométricos vêm sendo usadas em diversos aspectos da nossa vida, com um foco nas aplicações ligadas à segurança. O choque inicial em relação a tal tecnologia passou, deixando lugar para um debate de natureza ética e não tecnológica, no que diz respeito à maneira como os nossos dados são utilizados em tais aplicações.

Tendo isso em mente, este artigo apresenta uma análise das aplicações, influências e possíveis resultados do uso indiscriminado dessa tecnologia. Propomos aqui debater como os requerimentos e aplicações específicas, necessárias para possibilitar as identificações biométricas, geram um problema social (no campo biográfico) que extrapola os limites da privacidade de dados de seus usuários, especialmente quando se passa a tratá-los com as Inteligências Artificiais (IAs). Indo além, essa situação adentra um território até agora inexplorado, no modo como interagimos com as máquinas, uns com os outros e a maneira como nós nos entendemos enquanto indivíduos.

Para realizar tal análise, este artigo se divide em 2 seções, além desta breve introdução e das considerações finais. Na primeira seção vamos

abordar o tópico da biometria, o seu início, como está sendo desenvolvida, bem como as críticas a ela. A partir disso, na segunda seção enfocaremos a maneira como essa tecnologia é utilizada, e como os mecanismos necessários para o seu funcionamento agem em relação aos usuários, debatemos, assim, o impacto de sua utilização. [DAT_texto]

A evolução dos Sistemas de Identificação Biométrica

Há apenas algumas décadas atrás a tecnologia disponível a nós hoje seria considerada algo saída da ficção científica. Apesar de distante de desenvolvimentos científicos mais elaborados, como os especulados em filmes como De volta para o futuro 2 (1989), a ubiquidade presente nos aparelhos tecnológicos atuais nos permite dizer, finalmente, que este é, de fato, o futuro das especulações criadas em um passado que aqui referenciamos através de série e filme.

Com as "novidades" tomando lugar no cotidiano, graças a seu uso constante, diferentes análises das aplicações de certas tecnologias vêm sendo feitas partindo de um aspecto social, e não mais tecnocientífico. Como resultado disso, passamos a buscar entender se devemos usar certo tipo de tecnologia em vez de nos questionarmos se é possível criar tal tecnologia, que era a pergunta de há alguns anos. Com os campos científicos avançando além da nossa capacidade de compreender suas implicações, especialmente no que diz respeito à última década, nós podemos agora começar a entender o que a implementação de certos aparelhos nas últimas três décadas significa para nós e para o nosso modo de viver.

Hoje em dia estamos acostumados a tecnologias de *touch-screen* de tal forma que, quando celulares que se utilizavam de desbloqueio com base na leitura de digital do usuário foram introduzidos ao público, anos após o primeiro smartphone ter sido lançado, pouca foi a surpresa por parte da população. O seu uso foi, inclusive, algo imediatamente intuitivo para a grande maioria das pessoas. Este foi, talvez, o primeiro caso onde a biometria foi usada em larga escala, entretanto, não foi de fato o primeiro contato que tivemos com tal desenvolvimento em nossas vidas.

Conhecidos como Sistemas de Identificação Biométrica (em inglês *Biometric identification systems* - BISs), essas tecnologias são utilizadas para "identificação baseada em características biométricas" (LUIS-GARCÍA *et al*. 2003. Tradução nossa). Foi uma evolução natural da necessidade humana de identificar alguém desde que fotos, papéis e assinaturas passaram a ser facilmente forjados, e senhas podendo ser esquecidas, roubadas ou, até mesmo, adivinhadas. Com métodos de reconhecimento mais específicos para cada indivíduo, dificultaria o trabalho daqueles que pretendem se passar por outras pessoas, garantindo que o portador de alguma característica específica era, de fato, quem dizia ser (CHEN; JENKINS, 2017, p. 973). Dessa forma, a ideia de utilizar a digital, os olhos, ou a face do usuário para a sua identificação surgiu na mente de pesquisadores e cientistas da computação

(RASHID *et al*. 2008). A tecnologia, de fato, já existia, precisando somente de alguns desenvolvimentos complementares.

Em 1970, na World's Fair em Osaka, no Japão, uma atração tecnológica foi apresentada pela Nippon Electric Company (NEC), um aparato onde o visitante se sentava frente a uma câmera que fotografa seu rosto para então processar a imagem através de um programa de computador responsável por identificar características e categorizar o rosto do visitante dentre uma de 7 opções possíveis (GATES, 2011, p. 25). Era chamado de Computer Physiognomy (Fisionomia de Computador). Para que pudesse apresentar tal projeto para o público em 1970, ainda que com diversas falhas em seu sistema e funcionamento, podemos presumir que a pesquisa na área começou, ao menos, na década de 1960.

Existem patentes para sistemas utilizando identificação biométrica direta (com o objetivo de utilizar enquanto medida de segurança) desde 1995, com outros usando sistemas de reconhecimento que possuem recursos de identificação biométrica tecnologicamente assistidos em pesquisa desde 1987. No final da década de 1990, e no começo da década de 2000, teve um já esperado aumento no número de patentes com diferentes tipos de uso de sistemas de identificação biométrica, a maioria categorizados para segurança: segurança de passaporte, segurança de cartão de crédito, autenticação pessoal, segurança de passaporte, além de vários outros[2]. Esse movimento inicial de surgimento de mais e mais sistemas biométricos de identificação tecnologicamente mediados mostra a credibilidade e esperança não somente dos cientistas da computação, das empresas de segurança e de instituições governamentais nessa "nova" tecnologia, mas também do público geral, se sentindo progressivamente mais seguros com a ideia de seus pertences terem uma camada de segurança especial a eles adicionada.

Porém, o que vimos com esse desenvolvimento, nas décadas de 2000, 2010, e agora 2020, foi a constituição do controle biométrico da população no mundo. Existem diversos métodos que podem ser utilizados para identificar alguém, com novas maneiras sendo pesquisadas e implementadas todos os dias. Dentre eles, os métodos mais comuns são: reconhecimento de voz, reconhecimento de íris, reconhecimento facial e de digital. Hoje, praticamente todas as pessoas têm sua biometria aplicada enquanto medida de segurança em alguma camada de sua vida. Seja para acessar sua conta bancária, emitir o seu passaporte, a sua carteira de motorista ou o documento de identificação, vemos que a implementação de BISs está enraizada na sociedade atual.

A comercialização desse tipo de tecnologia, antes financiada e utilizada por agências de segurança nacional[3], também serviu como maneira de ter um controle maior sobre a população, um controle biométrico. Assim, não é mais possível viver uma "vida normal" sem ter suas fotos, suas digitais ou sua voz salvos em uma base de dados para ser acessada por diversas companhias ou instituições para provar que você é, de fato, quem diz ser. Enquanto essas bases de dados têm algoritmos de fórmula proprietária, existe um incentivo para a padronização do modelo de encriptação utili-

zado pelas biometrias vindo de uma esfera política e econômica (ALTERMAN, 2003, p. 139). Essa padronização se daria desde as fases iniciais de sua implementação como forma de tornar possível o compartilhamento de informações entre instituições. Isso permitiria, caso necessário, que as bases fossem acessadas por órgãos de vigilância governamental para categorizar, permitir ou negar acessos de certos indivíduos a certos lugares, atividades ou conhecimentos (VAN DER PLOEG, 1999, p. 296). Se tais planos, discussões e negociações já tivessem acontecido enquanto as BISs estivessem sendo implementadas em diversos aspectos da vida civil, o nível no qual teria se desenvolvido, duas décadas após sua criação e tendo sido fortemente consolidada na sociedade, seria ainda mais significante.

Todos os dados sendo coletados sobre nós, quase que recriando quem somos e o que demarca a nossa individualidade, é guardado e, caso acessado por qualquer pessoa, pode ser facilmente lido e analisado sem nosso consentimento. Isso traz um medo: de que tais dados possam ser obtidos de maneira legal e usados para criar um perfil e perseguir as pessoas por uma agência de segurança, por exemplo; ou de que nossos dados e nossos padrões de comportamento sejam usados contra nós por um comprador ou uma companhia trabalhando com o intuito de influenciar nossas ações de uma forma ou de outra (ALTERMAN, 2003, p. 140).

O governo chinês foi colocado em destaque em 2019 após anunciar seu novo sistema de crédito social. A ideia de pontuação de crédito não é inteiramente nova. Grande maioria dos países no mundo, e um grande número de companhias, se utilizam de alguma forma de pontuação para conferir o quanto o indivíduo pode "ser confiável", seja em relação a sua capacidade aquisitiva, sua condição financeira, se conseguem ou não quitar todas as contas dentro do prazo e, às vezes (especialmente no que diz respeito a empresas), dar a pessoa que foi considerada consistente e bem-intencionada algum brinde, ou presente.

A forma como o governo chinês adotou o sistema de pontuação, porém, tem suas especificidades: enquanto um modo de padronizar seu sistema de registro social, a China começou, em 2014, um plano para julgar todos os aspectos da vida de seus cidadãos, incluindo suas ações, tais como jogar lixo na rua, vandalismo, e qualquer outro tipo de desobediência civil, em suas respectivas pontuações e como forma de conseguir que utilizem, dentre outras BISs, tecnologia de reconhecimento facial (KOBIE, 2019). O governo, que fez parceria com o setor privado para ter acesso aos dados coletados das pessoas no país inteiro, combinado ao uso de suas informações, vêm determinando a pontuação pessoal dos indivíduos e se seu comportamento permite que ele tenha acesso ou sejam negados em atividades e ações como viajar dentro e fora do país, crédito social o suficiente que o permita comprar um carro ou uma casa, dentre outros, sem precisar de um processamento legal, ou aprisionamento, por exemplo.

A verdade é que a tecnologia sempre teve um papel importante na sociedade, mas tornou-se especialmente importante após o desenvolvimento industrial. Durante o século XX, em específico, arte e tecnologia

começaram a se conectar mais, no que Theodor Adorno e Max Horkheimer chamam de "Indústria Cultural" (GOBIRA, 2018a, p. 135). Dessa forma, a tecnologia, assistida por interfaces artísticas, se tornou mais rapidamente, e facilmente, aceita pela sociedade, transformando a vida com as inovações criadas pela indústria. A faceta única e aplicável citada no caso anterior só é, no momento, possível de encontrar espaço para funcionar e se desenvolver na China onde a grande maioria da população vive nos centros tecnológicos industrializados do país, cercados a todo o momento por câmeras de segurança e as mais diversas aplicações digitais, enquanto as áreas rurais e seus habitantes não são tão afetados ainda.

Então, porque isso acabou gerando tanta repercussão? Da maneira como acontecem, as notícias sobre os últimos estágios de implementação vieram no meio de uma mudança na maneira como as pessoas se posicionavam em relação às BISs e tecnologias relacionadas, após anos de vigilância de dados pessoais, vazamento de informações e abuso do uso de dados. Em vez de elogiar a, então chamada, segurança e intuitividade do sistema, o público geral começou a demonstrar preocupação em relação ao que significa ter tantas informações pessoais nas mãos do governo e de empresas, e de que maneiras tais informações seriam usadas e como tudo isso poderia lhes afetar. O sistema de crédito social chinês virou tópico de discussão devido ao entendimento de que, da forma como as coisas estão progredindo, tal sistema se apresentou enquanto um caminho de evolução natural para países ao redor do globo, tendo sua implementação pensada da mesma forma como acontece na China, ou de maneira adaptada às especificidades locais, setorizado e com características mais "suaves".

Nós estamos distantes da época em que o medo de ser espionado era algo da ficção. Nos anos recentes está surgindo um número constante de *whistleblowers*[4] e vazamentos que têm provado que, através dos aparelhos que temos em casa, como computadores, celulares, assistentes virtuais, entre outros, nossos dados estão sendo coletados sem nosso conhecimento ou consentimento.

Os patamares que a vigilância vêm alcançando são preocupantes até para aqueles que não acreditam nos abusos de segurança praticados por diversas instituições, com notícias sendo publicadas de que não somente a nossa localização, mas os websites que acessamos, as compras que fazemos online, enfim, a nossa própria existência está sendo coletada e arquivada em algum lugar.

Aplicativos de celulares, tablets e computadores que se utilizam da câmera dos aparelhos, como Snapchat, Instagram e TikTok, são famosos por usar "filtros" faciais, uma tecnologia que tem como objetivo alterar as feições faciais em tempo real. Para poder possibilitar tais alterações, o rosto do usuário é, primeiramente, escaneado. A maneira como funcionam tais escaneamentos faciais é a exata tecnologia aplicada das BISs e, dessa forma, não seria errado classificá-las como uma faceta das BISs. Há, inclusive, diversas denúncias que apontam que as empresas guardam em suas respectivas sedes e servidores, os dados de tais escaneamentos, vindo a utilizá-los

para construir algoritmos melhores de reconhecimento facial, mais rápidos e precisos (REID, 2020; PASCU, 2020).

O problema, no que diz respeito ao uso e abuso dos sistemas biométricos, vem sendo levantado desde a sua implementação nas mais diversas áreas. Uma das questões que foi explicitada diz respeito a como a ligação entre corpo e identidade vai afetar a maneira como nos entendemos, e a maneira como somos entendidos.

Nós passamos a nos entender enquanto pessoas vivendo em um contexto pós-digital, onde os aspectos digitais, ou virtuais, das coisas não são algo novo em nossas vidas, tendo se integrado completamente e sendo impossível de dissociá-las do modo de viver (GOBIRA, 2018b, p. 89).

Entretanto, o sentido de "quem, exatamente, deve ter acesso a tal tecnologia" abre campo para a discussão em relação a maneira como as BISs são usadas e implementadas para manter a "ordem social ao regular - e excluir - acesso a bens socioeconômicos, espaços geográficos e liberdades" (VAN DER PLOEG, 1999, p. 296. Tradução nossa). O potencial para afetar, vitimizar, ostracizar, demonizar ou até mesmo privilegiar demografias específicas, como já era temido, pode ser agora visto em seu total efeito, por exemplo, quando escutamos notícias sobre a disparidade de função ao tentar fazer funcionar sistemas de reconhecimento facial em pessoas de diferentes "raças" (LOHR, 2018). Outros debates, que vêm sendo levantados desde a virada do século XXI, têm relação com a privacidade dos dados.

Apesar dessas críticas serem válidas até os dias de hoje, a maneira como nos aproximamos da discussão aqui propõe uma perspectiva diferente que, apesar de lidar com os assuntos de privacidade, vai além das preocupações levantadas pelos pesquisadores de BISs nos primeiros momentos da tecnologia no mercado. Existe um novo fator adicionado que tem relação com os problemas éticos trazidos pelas BISs: Inteligência Artificial (IA). Apesar da possibilidade de usar a inteligência de um computador enquanto forma de desenvolver funções não programadas, sem a necessidade de um input humano (POOLE; MACKWORTH; GOEBEl, 1998), já esteja sendo trabalhada há algumas décadas, é o seu acoplamento com o reconhecimento facial que tornou possível corrigir os erros e aprimorar a performance onde tais algoritmos tinham dificuldade anteriormente. Assim, tornou-se possível ir além da sua análise típica em "situações estritamente programadas" (O'CONNOR; ROY, 2013, p. 25), usando dados colocados em sistemas de IA que vão além das condições otimizadas de visualização de uma estrutura facial de maneira a reconhecê-la. Enquanto desenvolvimento tecnológico que irá, sem dúvidas, afetar diversos outros espaços, é também componente principal na era da vigilância em que vivemos (ZUBOFF, 2019).

É a tecnologia que torna possível o controle que o governo chinês tem com seu sistema de crédito social, que é tão criticado no Ocidente, mas que apenas explicita uma característica dessa nossa época: a incapacidade de anonimato na era da tecnologia. Não é mais possível andar pelas ruas sem ser visto por câmeras de segurança, sejam elas do governo ou do setor privado. É possível usar IAs nessas gravações, mesmo que não haja sistemas

BISs em funcionamento durante a captação, para reconhecer, localizar o indivíduo e tomar conhecimento de suas ações. Tudo isso pode significar uma sociedade mais segura, onde pode-se encontrar os autores de um crime em questão de minutos, mas o custo não é somente a mudança do status de liberdade das pessoas e o controle sobre seus dados, mas a confirmação de um modo de vida que vem sendo construído através do uso das máquinas semiautônomas e autônomas desde o século XVIII.

Conforme a preocupação social aumenta, em relação à segurança, liberdade, os vieses étnicos e de gênero utilizados nesses sistemas, possibilita-se uma retórica da indústria e do mercado econômico que permitiria (e permitirá) que se beneficiem o máximo da aplicação de tais desenvolvimentos tecnológicos em mais aspectos inclusivos do nosso dia-a-dia. Parece que a ameaça que se apresenta a nós, enquanto sociedade, aparenta ser um "sacrifício justo" desde que "utilizado da maneira correta" pelas companhias que a estão implementando.

Vemos tentativas de um movimento contrário ao uso das BISs por forças de segurança, como a cidade de São Francisco, nos Estados Unidos, que baniu o uso de reconhecimento facial pela polícia e outras instituições enquanto um "posicionamento contra um possível abuso [de autoridade]" (CONGER; FAUSSET; KOVALESKi, 2019. Tradução nossa), e a abordagem de organizações como a IBM que anunciaram que não mais disponibilizariam seu sistema para uso da polícia enquanto forma de lutar contra alvo racial tecnológico[5] (BBC, 2020). Um ato simples e inútil de tentar responder às demandas do público, de uma forma superficial e aparente de lidar com um problema que, como se viu até aqui, está mais enraizado em nossa forma de viver do que a maioria das pessoas sequer compreende ainda[6].

O debate sobre se os sistemas de reconhecimento facial utilizados pela polícia têm ou não algum tipo de preconceito racial ou de gênero é bastante utilizado pelas empresas. Elas usam essa discussão, de maneira extremamente pública, como forma de divergir a atenção para o fato de que não temos (nem nunca tivemos) a capacidade de escolher diretamente se, quando e como nossas biometrias são usadas e se são ou não capturadas com ou sem nosso conhecimento por milhares de organizações cuja existência depende justamente dos dados que obtém. Ainda que sem o nosso conhecimento explícito, nós, enquanto sociedade, já fizemos a escolha de usar e confiar no controle das BISs. É, afinal de contas, algo amplamente normalizado, de uma perspectiva histórica, visto que, como aqui já comentado, temos há muito mesclado todos os aspectos de nossa existência com uma forma ou outra de tecnologia e, apesar de minúsculas mudanças em relação a especificidade que tais tecnologias conseguem realizar, é, em sua essência, nada novo para o desenvolvimento humano.

De biometrias autobiográficas a biografias biométricas através de Inteligência Artificial

Apesar de as tecnologias de reconhecimento facial não serem amplamente utilizadas pelo público geral, devido a razões econômicas – tendo mais acesso a biometrias como leitores de digital para sua conta bancária e escaneamento de íris, agora utilizado também na segurança de seus smartphones –, elas certamente estão dentre as BISs mais populares. Ao menos é uma das que mais se faz presente em nossa imaginação, certamente.

Ainda que o público geral não possua acesso direto a essa tecnologia, várias empresas e instituições governamentais, aparentemente focadas no aspecto da segurança, a usam na identificação das pessoas, na construção de seu histórico e seus hábitos de uma forma automatizada, rápida e eficiente. Se aproveitando do, ainda, não regulamentado campo das biometrias (WRIGHT, 2019, p. 614), uma variedade de instituições vêm utilizando o reconhecimento facial sem o conhecimento ou consentimento das pessoas como forma de: identificar figuras importantes; realizar uma personalização de clientes; e/ou aprimorar bases de dados. Esta última faceta é uma necessidade indispensável não somente no setor do reconhecimento facial, mas das BISs como um todo: a necessidade de uma base de dados onde se possa guardar informações e, posteriormente, acessá-las para conseguir pôr a prova a identidade ou os elementos da biografia do indivíduo em questão.

Como dito anteriormente, é esse exato aspecto que diz respeito ao medo e aos debates que surgem sobre a liberdade e privacidade de dados no mundo atual. Apesar do aprimoramento apresentado, no que diz respeito à dificuldade de falsificação garantida pelas biometrias, nós não podemos ignorar o fato de que um vazamento de alguma das bases de dados específica pode ser utilizado para "reconstruir uma imagem biométrica" (ANNAMALAI; RAJU; RANGANAYAKULU, 2018, p. 423. Tradução nossa). É nesse sentido que conseguimos vislumbrar o uso das IAs no tratamento da big data (WU *et al*. 2013), sobretudo nessas bases de dados biométricos. As IAs promovem uma passagem dos processos biométricos pessoais que geram autobiografias (pois neste caso é o próprio indivíduo que as cria no uso dos BISs) para a formação de "biografias biométricas", tendo em vista que o uso aplicado das IAs passam a construir biografias no tratamento automático dos dados do indivíduo e seus elementos biográficos objetificados por uma terceira pessoa algorítmica.

Ao andarmos nas ruas, entrarmos em lojas, bancos, restaurantes, e diversos outros estabelecimentos, somos sujeitos a auxiliar na criação de tais bases de dados. Todas as imagens capturadas por nós, ou de nós até mesmo por câmeras de segurança, podem ser utilizadas, com a assistência de programas de IA, como um método de reconhecimento facial. Entendemos, atualmente, a IA como algo que "possui papel central no desenvolvimento da próxima geração de soluções biométricas" (KAIRINOS, 2019, p. 8. Tradução nossa). Ela pode ser utilizada para aprimorar programas que se

utilizam de algum tipo específico de biometria e que era, anteriormente, impreciso de alguma forma, aprendendo e se desenvolvendo sozinho, na medida em que é utilizado, diminuindo a chance de uma identificação ou autenticação incorreta.

A acumulação de nossas informações não é mais restrita apenas ao campo digital. Com os softwares gravando e analisando nossos padrões de uso e nossas preferências, interconectados entre si através da internet (GOBIRA, 2016, p. 11), a transformação em dados de nossa existência (*datafication* em inglês), se relaciona com as ações que realizamos fora da internet.

Não somente fotos e informações tiradas de nós sem nosso conhecimento, sem distinção de online ou offline, são utilizados para melhorar a precisão das tecnologias biométricas, como também os dados que disponibilizamos sobre nós, e sobre os outros, podem ser utilizados indiscriminadamente. As fotos que postamos, as palavras que digitamos, nossas "curtidas" e "compartilhamentos" nas redes sociais, são dados prontos para serem coletados e agregados para realizar uma versão de quem somos, uma biografia biométrica.

Já é possível perceber que não importa se temos acesso ou não a um meio digital. Conforme o tempo passa, processos históricos e tradicionais vão se aprimorando tecnologicamente. Coisas como certificados de nascimento, informações bancárias, processos jurídicos, entre outros, são arquivados digitalmente em suas próprias bases de dados, de maneira que eles também se tornam parte das informações sobre quem somos (GOBIRA, 2016). Essas informações sobre as quais não temos controle ou acesso se somam às informações geradas ao utilizarmos filtros em fotos de aplicativos, onde contribuímos para o desenvolvimento das plataformas e suas aplicações em IA.

Decodificar toda a informação coletada é possível através de aplicações desenvolvidas com função de data mining (mineração de dados), como as IAs utilizadas em sistemas biométricos. Elas são aplicadas à big data para identificar separadamente cada um de nós partindo de toda aquela informação a qual esses mecanismos podem ter fácil acesso.

O impacto de tal conhecimento (a ser comprado pela empresa ou instituição que pagar mais caro) está, pouco a pouco, se tornando clara para a sociedade. A preocupação vai além das questões de privacidade de dados, liberdade de se manter anônimo em uma sociedade hiper-vigilante, chegando a questionamentos mais práticos, como a possibilidade de se viver em uma sociedade que se molda a partir de um sistema de crédito social: de ser impedido de ir a um aeroporto, dependendo das opiniões que expressa online; ou, também, se o sistema de segurança da sua casa consegue reconhecer você e seus familiares, permitindo-os acesso à propriedade (KAIRINOS, 2019, p. 9).

Devemos saber que tudo isso já está dado nesse modo de viver implementado por processos construídos há bastante tempo. Os processos tecnológicos e avanços sistêmicos que abordamos aqui criaram as condições materiais da sociedade para se estabelecer as biografias biométricas. Confor-

me a tecnologia vai ficando significativamente mais barata, nós passamos a utilizá-la em mais e mais aspectos de nossas vidas. A necessidade de deixar acessível cada aspecto de nós, de quem somos em nossa sociedade, pode ser vista desde o início do uso de máquinas digitais (GOBIRA, 2016, p. 10).

Talvez a razão pela qual tal nível de desenvolvimento recente tenha sido tão amplamente aceito se deva ao fato de que, a existência de reconhecimento facial "conversa" diretamente com nossa imaginação e nosso subconsciente através do acesso que tivemos a essas tecnologias na ficção científica de antigamente. A razão pela qual tal tecnologia se tornou tão popular, em filmes e séries de televisão, é porque somos atraídos a interagir com outros que se parecem conosco, aqueles que agem e falam como nós. Na maior parte da história humana falamos uns com os outros presencialmente, olhando uns nos olhos do outros. Sendo assim, aplicar reconhecimento facial em um sistema computadorizado parece ser uma forma de trazer a interação entre pessoas para a interação com as tecnologias (LISETTI; SCHIANO, 2000).

Essa hipótese se alia à promessa constante de medidas de segurança que nós, enquanto sociedade, estamos tão dispostos a implementar, preferindo confiar que nossas biografias serão bem tratadas pelas corporações e governos no lugar de confiarmos uns nos outros. Podemos nos deixar ser enganados e controlados pelas IAs que executam operações treinadas (machine learning/deep learning) para processar todos os dados necessários para sua funcionalidade completa, porque nós, assim como governos e instituições públicas e privadas, passamos a depender de tais aplicações nos mais diversos aspectos de nossas vidas (VAN ZOONEN, 2016, p. 474). Por conta de tudo isso, apesar do risco iminente vindo da possibilidade de quebra de segurança e ataques aos sistemas inteligentes (SARKAR; BENKRAOUDA; MANIATAKOS, 2020), estamos dispostos a nos sujeitar a ter nossos dados alterados por terceiros, uma vez que já não temos como substituí-los, ou frear o seu desenvolvimento.

De biometrias autobiográficas a biografias biométricas através de Inteligência Artificial

Atualmente é quase impossível viver uma vida sem interações com os BISs conforme o mundo se torna, diariamente, mais tecnológico, e essa tecnologia mais ubíqua. Até mesmo aqueles que vivem em áreas remotas, rurais, utilizam os BISs, uma vez que a maioria dos países fazem uso ao menos da leitura de digitais para documentos oficiais. Desde cedo em nossas vidas, a nossa existência em sociedade está diretamente condicionada a acumulação de nossos dados que, de uma forma ou outra, são coletados por algum tipo de organização privada ou pública. Algo do qual não podemos escapar.

De alguma forma, a maior ameaça para nós, enquanto sociedade, não são os possíveis ataques de hackers nos sistemas de IA utilizados para operar programas biométricos (GAO *et al*. 2020). Ainda que a informação compartilhada entre os sistemas seja de dados sensíveis, e a padronização

das linguagens venha aumentando, facilitando as ações maliciosas de terceiros (SOUTAR, s/a), olhar somente para este aspecto seria escolher tomar uma postura superficial sobre o assunto.

O fato é que a big data está sendo construída tendo as bases de dados que a compõem sendo tratadas e controladas por IAs que se utilizam de machine learning/deep learning para terem seus usos aperfeiçoados. Hoje não é mais uma prioridade pensar como o controle, a alimentação e o acesso a tais informações estão acontecendo e se tais ações são feitas conscientemente pelos usuários ou não.

Acreditamos que é importante nos preocuparmos com o caráter biográfico que esse acúmulo de dados constitui. Temos a nossa frente um outro tipo de inteligência que é capaz de entender, criar e/ou tratar e controlar as nossas biografias baseadas nos dados coletados (ou "hackeados", ou "vazados" etc.) sobre nós durante nossas vidas, dados que vão continuar a existir e fazerem parte de arquivos depois que não estivermos mais aqui (GOBIRA, 2016, p. 15). E sabemos, hoje, que "estar arquivado" não significa que esses dados e, consequentemente, nós não seremos encontrados, revistos, revividos. Em uma sociedade cuja base de operação cotidiana é a big data, não existe "arquivo morto".

Notas de fim

1. Agradecemos ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), à Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) e à PROPPG/UEMG pelo apoio à pesquisa do grupo de pesquisa, desenvolvimento e inovação Laboratório de Poéticas Fronteiriças [http://labfront.tk] da qual este artigo resulta.

2. Estas informações foram extraídas de uma pesquisa realizada por nós na base de dados de patentes do Google (ver: https://patents.google.com/), utilizando-se de termos como "biometrics", "biometria", "recognition", "fingerprint", "security measures", entre outras, analisando as datas de pedido de patente e o campo de pesquisa/utilização nelas apontados pelos seus autores para poder ter o contexto explicitado neste trecho.

3. Este é o caso da pesquisa feita na década de 1960 em tecnologia de reconhecimento facial financiada pelo Departamento de Defesa dos Estados Unidos e outras agências de inteligência. Para mais informações ver Gates (2011, p. 27).

4. Termo em inglês utilizado para nomear funcionários de empresas, governos, e outras instituições, que realizam denúncias públicas por abusos cometidos contra seus funcionários ou a população em geral.

5. A decisão surge após os protestos do movimento Black Lives Matter (Vidas Negras Importam), nos Estados Unidos, no final de maio de 2020, após a morte de George Floyd por abuso policial. Nesses protestos, órgãos governamentais e a polícia americana passaram a usar tecnologia de reconhecimento facial assistido por IA, cedido pela IBM, para coletar e analisar fotos tiradas pelo público para identificar e criminalizar os manifestantes negros.

6. Justamente por isso que vimos em 2022, logo no início da guerra da Ucrânia, o governo ucraniano utilizar o reconhecimento facial "para informar russos sobre perdas militares". Ver mais em: https://oglobo.globo.com/mundo/ucrania-usa-reconhecimento-facial-para-informar-russos-sobre-perdas-militares-diz-vice-premier-25445632. Acesso em: <25/03/2022>.

Referências

ALTERMAN, Anton. "'A piece of yourself': Ethical issues in biometric identification", in: **Ethics and Information Technology**, Kluwer Academic Publishers: Netherlands, v.5, no.3, 2003, p.139–150.

BBC. "IBM abandons 'biased' facial recognition tech." Disponível em: <https://www.bbc.com/news/technology-52978191> Acesso em: <24/01/2021>.

CHEN, Jiachen; JENKINS, Kenneth. "Facial recognition with PCA and machine learning methods", In: Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), 2017, p.973-976.

CONGER, Kate; FAUSSET, Richard; KOVALESKI, Serge F. "San Francisco Bans Facial Recognition Technology" in: **The New York Times**, 14 de Maio/2019. Disponível em:< https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-s>. Acesso em: <04/02/2021>.

DUNSTONE, Ted; YAGER, Neil. "**Biometric System and Data Analysis**: Design, Evaluation, and Data Mining". Springer: Eveleigh, Australia, 2009, 266pp.

GATES, Kelly A. "Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance". **NEW YORK UNIVERSITY PRESS**: New York and London, 2011, 276pp.

GAO, Yansong; BAO, GiaDoan; ZHANG, Zhi; MA, Siqi; ZHANG, Jiliang, FU, Anmin; NEPAL, Surya; KIM, Hyoungshick. "Backdoor Attacks and Countermeasures on Deep Learning: A Comprehensive Review". **ArXiv e-prints**, 2020.

GOBIRA, Pablo. Arte, corpo e máquina: jogos digitais, sociedade do espetáculo e sex appeal do inorgânico. In: SILVA, Rogério B.; GOBIRA, Pablo; MARINHO, Francisco. (Org.). **Múltiplas interfaces**: livros digitais, criação artística e reflexões contemporâneas. 1ed.Belo Horizonte: Scriptum, 2018b, v. 1, p. 133-144.

GOBIRA, Pablo. Museus e paisagens culturais pós-digitais. In: GOBIRA, Pablo. (Org.). **Percursos contemporâneos**: realidades da arte, ciência e tecnologia. 1ed.Belo Horizonte: EdUEMG, 2018a, v. 1, p. 83-98.

GOBIRA, Pablo. Os desafios da crítica biográfica na sociedade espetacular: a tecnologia digital, a biografia perpétua e o controle da memória. In: AGUIAR, Ana Lígia Leite; SERAFIM, José Francisco; LIMA, Rachel Esteves; COELHO, Sandra Straccialano. (Orgs.) **O**

espaço biográfico: perspectivas interdisciplinares.1 ed. Salvador: EdUFBA, 2016, v.1, p. 8-16.

KAIRINOS, Nikolas. "The integration of biometrics and AI", in: **Biometric Technology Today**, vol.5, maio de 2019, p.8–10. doi:10.1016/s0969-4765(19)30069-4.

KITCHIN, Rob. "The ethics of smart cities and urban science", in: **Philosophical Transactions A**: The Royal Society Publishing, A 374, 15 de janeiro 2016, p.1-15.

KOBIE, Nicole. "The Complicated Truth about China's social credit system", in: **WIRED**, Junho 7/2019. Disponível em: <https://www.wired.co.uk/article/china-social-credit-system-explained>. Acesso em: <22/01/2021>.

LISETTI, Christine L.; SCHIANO, Diane J. "Automatic Facial Expression Interpretation: Where Human-Computer Interaction, Artificial Intelligence and Cognitive Science Intersect", In: **Pragmatics and Cognition** (Special Issue on Facial Information Processing: A Multidisciplinary Perspective), vol.8, ed.1, 2000, p.185-235.

LOHR, Steve. " Facial Recognition Is Accurate, if You're a White Guy", in: **The New York Times**, Fev. 9, 2018. Disponível em: <https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html>. Acesso em: <27/01/2021>.

LUIS-GARCÍA, Rodrigo; ALBEROLA-LÓPEZ, Carlos; AGHZOUT, Otman; RUIZ-ALZOLA, Juan. "Biometric identification systems", in: **Signal Processing**, vol.83, no.12, 2003, p.2539-2557. 10.1016/j.sigpro.2003.08.001.

O'CONNOR, Brian; ROY, Kaushik. "Facial Recognition using Modified Local Binary Pattern and Random Forest", in: **International Journal of Artificial Intelligence & Applications (IJAIA)**, vol. 4, n. 6, novembro de 2013, p.25-33.

PASCU, Luana. "Researchers use Instagram mask selfies to improve biometric facial recognition algorithms". in: **BIOMETRIC Update.com**, Maio 20/2020. Disponível em: <https://www.biometricupdate.com/202005/researchers-use-instagram-mask-selfies-to-improve-biometric-facial-recognition-algorithms>. Acesso em: <23/01/2021>.

POOLE, David; MACKWORTH, Alan; GOEBEL, Randy. Randy. "Computational Intelligence: A Logical Approach". Oxford University Press: Londres, 1998.

PRAKASH, Annamalai; KRISHNAVENI, Raju; DHANALAKSHMI, Ranganayakulu. "Soft Biometrics Traits for Continuous Authentication in Online Exam Using ICA Based Facial Recognition", in: **International Journal of Network Security**, vol.20, n.3, maio de 2018, p.423-432.

RASHID, Rozeha A.; MAHALIN, Nur H.; SARIJARI, Mohd A.; AZIZ, Ahmad A. A. "Security System Using Biometric Technology: Design and Implementation of Voice Recognition System (VRS)", in: **Proceedings of the International Conference on Computer and Communication Engineering 2008**: Kuala Lumpur, Malaysia, 13-15 de maio, 2008, p.898-902.

REID, Alana. "Are filters on social media being used to collect your identity?", in: **8MS**, Abril 6/2020. Disponível em: < https://8ms.com/blog/are-filters-on-social-media-being-used-to--collect-your-identity/> Acesso em: <23/01/2021>.

SADOWSKI, Jathan; PASQUALE, Frank. "The Spectrum of Control: a social theory of the smart city", in: **First Monday**, vol. 20, n. 7, 6 de julho de 2015, p.1-22.

SARKAR, Esha; BENKRAOUDA, Hadjer; MANIATAKOS, Michail. "FaceHack: Triggering backdoored facial recognition systems using facial characteristics", **arXiv preprint**, arXiv:2006.11623, 2020.

SOLTAR, Colin. "**Biometric System Security**". Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=B013D67DACE34C0A365D77E3CD63CE80?doi=10.1.1.453.4790&rep=rep1&type=pdf>. Acesso em: <10/10/2021>.

SOUTAR, Colin. "Security Considerations for the Implementation of Biometric Systems". In: RATHA, Nalini; BOLLE, Ruud. (Eds.) **Automatic Fingerprint Recognition Systems**, Springer: Heidelberg, 2004, p.415–431.

VAN DER PLOEG, Irma. "The illegal body: 'Eurodac' and the politics of biometric identification". in: **Ethics and Information Technology**, Kluwer Academic Publishers: Netherlands, v.1, 2000, p.295–302.

VAN ZOONEN, Liesbet. "Privacy concerns in smart cities", in: **Government Information Quarterly**, vol. 33, ed. 3, 2016, p.472-480.

WRIGHT, Elias. "The Future of Facial Recognition Is Not Fully Known: developing privacy and security regulatory mechanisms for facial recognition in the retail sector", **The Fordham Intellectual Property, Media & Entertainment Law Journal**, Vol.29, n.6, 2019, p.611-685.

WU, Xindong; ZHU, Xingquan; WU, Gong-Qing, DING, Wei. "Data Mining with Big Data", in: IEEE Transactions on Knowledge and Data Engineering. **IEEE Transactions on Knowledge and Data Engineering**, vol. 26, p.97–107.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. 691p.

Recebido: 24 de abril de 2022.

Aprovado: 17 de maio de 2022.