Correio da AESE
PANORAMA
21.mar.2018
N.715
AESE BUSINESS SCHOOL
www.aese.pt

Índice

Biometria: o nosso rosto digital

A tecnologia biométrica deixou de ser um fenómeno próprio das histórias de ficção científica. Os governos de alguns países têm vindo a utilizá-la há algum tempo para reconhecer os seus cidadãos, algo que levanta novos desafios éticos e que já chegou a casos extremos, por exemplo, na China.

Embora a palavra “biometria” possa ser desconhecida do público em geral, a sua aplicação está, desde há uns tempos, mais do que presente nas nossas vidas. Consiste em identificar as pessoas através de uma caraterística física exclusiva: primeiro foram as impressões digitais e, mais recentemente, a íris, ou o rosto.

Se é cada vez mais fácil aceder à informação pessoal de quase toda a gente e grande parte das transações são realizadas de modo virtual, decorre que a necessidade de identificar bem as pessoas se torna premente. Embora as empresas tecnológicas também utilizem este sistema para, por exemplo, etiquetar pessoas numa rede social ou desbloquear um dispositivo móvel, o maior desafio apresenta-se para dois agentes diferentes: governos e instituições financeiras.

Até há pouco tempo, para fazer uma transferência ou aceitar a minuta da Declaração de Rendimentos, bastava introduzir um número de identificação pessoal e, quando muito, confirmar a nossa identidade através de um correio eletrónico ou de um SMS. No entanto, em muitos países, este tipo de procedimentos é feito já apoiando simplesmente o dedo num leitor de impressão digital ou deixando que uma máquina digitalize o rosto do interessado.

Segundo os especialistas, a identificação biométrica reduz ao mínimo a possibilidade de fraude, porque os dados que se usam são praticamente impossíveis de burlar no caso da pessoa não estar presente.

E, entre todas as modalidades disponíveis, o reconhecimento facial apresenta-se como a mais eficaz, pois as impressões digitais são mais inexatas e podem variar ligeiramente, por exemplo, no caso de uma pessoa que tenha um trabalho artesanal. Pelo contrário, os programas que realizam a digitalização facial oferecem uma precisão cada vez maior, mesmo se o utente alterar o seu aspeto, por exemplo, com uma barba ou uns óculos.

Além disso, de um ponto de vista prático, para os utentes torna-se muito mais fácil deixar-se fotografar por um scâner ou pressionar um botão para todos os seus procedimentos, do que recordar uma grande quantidade de nomes de utente e senhas.

A Austrália, a Índia e a China são alguns dos governos na vanguarda deste tema.

O governo da Índia possui o maior programa de identificação biométrica do mundo, o Aadhaar. O seu sistema serve tanto para trâmites públicos, como para abrir uma conta no banco ou registar uma linha telefónica. Uma chave semelhante ao “iniciar sessão com o Facebook”, mas com dados mais delicados e capaz de abrir portas oficiais.

No Aadhaar, cada cidadão tem um número de identificação que contém os seus dados pessoais e biométricos (impressão digital, íris…). Embora seja voluntário inscrever-se, a realidade é que se torna praticamente necessário para aceder aos serviços essenciais.

Como pode ser usado para efetuar procedimentos de todo o tipo, a sua base de dados é muito completa e são muitos os que consideram que ameaça a privacidade dos cidadãos, pois o governo pode saber quase instantaneamente o que fazem na sua vida pública e privada.

Atualmente, o sistema armazena os dados de 90 % dos cidadãos indianos, 1110 milhões de pessoas, o que o converte num dos grandes objetivos para os piratas informáticos. Compete em volume com as grandes empresas tecnológicas, cujas bases de dados muito menos são de desprezar: 2000 milhões de utentes no caso do Android e 1000 milhões no da Apple.

Também estas empresas estão a adotar a biometria: há algum tempo que os dispositivos se desbloqueiam com a impressão digital ou com a leitura da íris; e o último iPhone X permite já fazer pagamentos com o seu sistema de reconhecimento facial, Face ID.

Mas as exigências de segurança suscitadas pelas bases de dados biométricos são demasiado grandes e, por isso, ninguém se arrisca a dar passos sem ter tudo sob controlo. De facto, nem a Google nem a Apple instalaram ainda o scâner compatível com o Aadhaar nos seus telefones indianos.

De momento, a Austrália é o país ocidental mais convencido da necessidade de integrar tecnologia biométrica nos sistemas de identificação pública. O Governo Federal já conta com uma base de dados faciais de 85 % dos australianos e, em 2018, tem previsto aprovar uma lei para que também as empresas privadas incluam nas suas bases de dados o reconhecimento facial. Se se concretizar, a Austrália implementaria o sistema FVS (Face Verification Service), através do qual as empresas que obtenham os dados faciais de um cliente poderão enviá-los para o governo de modo a que este os verifique. Algo similar é já utilizado para verificar documentos oficiais (Documents Verification Service), como cartas de condução, passaportes, cartões de imigração...

As razões para o pôr em prática são reduzir a fraude e apoiar o setor financeiro ajudando, além disso, a travar o branqueamento de capitais, o terrorismo, etc. Tal como na Índia, em princípio não será obrigatório aderir ao FVS.

Na futura lei especifica-se que as empresas só poderão guardar esta informação se contarem com a autorização expressa do interessado. Todavia, é bastante provável que os australianos cedam os seus dados com o mesmo escasso conhecimento que tem a maioria dos cidadãos sobre as políticas de privacidade de tudo o que aceitam na Internet.

Além disso, a regulamentação especifica que as empresas que queiram utilizar esse sistema deverão garantir a privacidade da sua base de dados, mas o recente caso de pirataria em massa do Equifax, um dos fornecedores deste serviço aprovados pelo governo australiano para o sistema de verificação de documentos, faz com que a segurança do projeto esteja, de momento, bastante questionada.

Os especialistas alertam já contra a falta de supervisão do FVS e interrogam-se sobre quem será o responsável por armazenar esses dados e com quem será legal partilhá-los. Adicionalmente, os seus detratores queixam-se da pouca transparência que existe nas negociações do governo com estas empresas.

Na China, o setor financeiro do gigante asiático é pioneiro na utilização de tecnologia biométrica e milhões de chineses utilizam já diferentes sistemas de identificação facial para autorizar pagamentos. Mas não só isso. O caso da China levanta o maior problema das bases de dados em massa, que vai além do risco de pirataria: o uso dessa informação para controlar os cidadãos.

Desde há alguns anos, o governo de Xi Jinping espia os seus cidadãos com um projeto que foi qualificado em múltiplas ocasiões de "orwelliano", fazendo referência ao cenário descrito no romance "1984". O sistema apoia-se, sobretudo, no reconhecimento facial e na inteligência artificial para vigiar e prever o comportamento das pessoas.

Para controlar os seus 1300 milhões de habitantes, o Estado chinês conta com 170 milhões de câmaras inteligentes que podem reconhecer um rosto, ou decifrar a idade ou a etnia de uma pessoa e registar todos os seus movimentos: que automóvel possui, para onde vai, com quem contacta habitualmente… Nos próximos três anos, vão ser instalados mais 400 milhões de câmaras.

O governo tem uma base de dados com 700 milhões de rostos e utiliza-a para coisas tão surrealistas como evitar que nas casas de banho públicas as pessoas utilizem mais de 60 centímetros de papel higiénico num período de nove minutos, como explicava recentemente a "The Economist".

Com todos esses dados, o Estado criou, em 2012, o chamado "Sistema de Crédito Social": uma lista negra do Supremo Tribunal da China com nomes de pessoas que considera "pouco confiáveis". O objetivo é que estas tenham dificuldades, mais ou menos sérias, no momento de aceder aos serviços públicos e privados – desde comprar *online*, até conseguir um emprego ou escola para os seus filhos –, de forma a que uma pessoa que comete fraude num lugar não possa voltar a fazê-lo noutro.

Alguns governos locais colocam as fotografias, nomes completos e endereços dos incluídos no sistema em painéis publicitários, mas o normal é que as autoridades não avisem ninguém se a pessoa está incluida nem porquê; as pessoas apercebem-se, por exemplo, quando não podem comprar um bilhete de avião. Os "não confiáveis" deixam de sê-lo quando se retratam naquilo por que foram inscritos na lista; ora, para isso, primeiro têm de conseguir averiguá-lo.

Contava o "The Wall Street Journal" que, somente em 2017, sete milhões de chineses passaram pelo Sistema de Crédito Social. Um deles, por exemplo, foi incluído por declarar num tribunal como testemunha, tendo o seu testemunho sido

considerado por esse tribunal como "não sincero". Até ter feito uma retratação pública a pedir perdão, o seu nome não foi retirado. Noutro caso, um jornalista acabou na "lista negra" depois de publicar uma informação sobre um suposto extorsionário e não poder demonstrar a veracidade do seu artigo.

Logicamente, trata-se de um sistema que dá lugar a múltiplos abusos, a começar no facto dos afetados não terem direito a defender-se nem a um julgamento justo. Mas, além disso, com este projeto, o governo pretende não só evitar o crime, também prevê-lo.

A comunidade internacional criticou muitas vezes as empresas privadas que se submetem a servir de cúmplices do regime de Pequim. Recentemente, foram especialmente sonantes os protestos contra a Apple, que tem na China o seu terceiro mercado mais importante. A empresa retirou 674 aplicações da sua *appstore* nesse país, a pedido do governo, porque permitem aos utentes ultrapassar o chamado "grande *firewall* chinês". Tim Cook, CEO da Apple, declarou em sua defesa que, embora ele como norte-americano não esteja de acordo, "cada país tem direito a criar as suas próprias leis".

Também as empresas chinesas colaboram de maneira ativa no grande sistema de vigilância, em muitos casos, cedendo os seus dados ao serviço do governo. É o caso do Sesame Credit, um programa piloto da área financeira da Alibaba (a Amazon chinesa, que já é a maior plataforma de compra *online* do mundo), seguido muito de perto pelo Estado.

Com este sistema, a Alibaba classifica o risco das operações financeiras em função das compras de cada pessoa: "Alguém que joga videojogos durante dez horas por dia, por exemplo, seria considerado uma pessoa ociosa, e alguém que frequentemente compra fraldas provavelmente será pai e, portanto, considerado como alguém com sentido da responsabilidade", explicava Li Yingyun, diretor de tecnologia do Sesame, à revista chinesa "Caixin", em 2015.

Os utentes podem conhecer a pontuação que a Alibaba lhes concede. De momento não penaliza, mas premeia sim as pontuações elevadas com descontos ou acesso a certos serviços financeiros.

Na China, não existe nenhum tribunal que proteja a privacidade e, portanto, os cidadãos não têm possibilidade de denunciar ninguém. No entanto, a sua situação atual é encarada à lupa pelo Ocidente, como um modelo ao qual nunca deveríamos chegar.

C. G. H.

Como e porquê "nos espiam" os governos no Ocidente

Desde que as revelações de Edward Snowden foram contadas pela primeira vez no "The Guardian" e no "The Washington Post", em junho de 2013, o conceito de "espionagem em massa" passou a ser um tema habitual nos meios de comunicação. À voz do ativista foram-se juntando as de muitos outros que também reclaman e alertam os cidadãos contra os seus próprios governos.

Até agora, parecia algo que só era motivo de preocupação para os ativistas ou para as pessoas especialmente sensíveis à privacidade na Internet. Enquanto a espionagem do governo é já uma realidade não oculta na China, no Ocidente os governos foram aprovando recentemente leis favoráveis à vigilância eletrónica que passaram praticamente despercebidas aos cidadãos, no contexto existente do complexo panorama político.

Em 1993, a Comissão dos Direitos Humanos da ONU decidiu designar um Relator Especial em matéria de liberdade de expressão e opinião, devido às crescentes ameaças contra este direito. Em março de 2017, Joseph Cannataci, o relator desta matéria, publicou um relatório que condena a legislação atual sobre vigilância, alertando especialmente contra as leis recentemente aprovadas no Reino Unido, França e Alemanha. "Mal existem provas, se é que há alguma, que me convençam da eficácia ou da proporcionalidade de algumas das medidas extremamente invasivas que foram introduzidas com as novas leis de vigilância".

Há algum tempo que as pessoas com maior sensibilidade para com a possível "espionagem" – jornalistas de investigação, defensores dos direitos humanos…– utilizam sistemas de correio criptografado e de navegação escondido. Mas, os outros, devem estar preocupados?

A 1 de dezembro de 2016, a Grã-Bretanha aprovou a Lei de Poderes de Investigação, que alguns, como Edward Snowden, qualificaram como "uma das mais extremas" numa democracia.

A legislação permite aos organismos de segurança *hackear* computadores e telemóveis de cidadãos que não são suspeitos de nenhum comportamento criminoso, e armazenar os dados que extraiam. Além disso, obriga as empresas de comunicação privadas a guardar, durante um ano, todo o historial que tenham dos seus utentes, à disposição das autoridades.

Na altura, foram poucas as vozes internas que se opuseram ao projeto. Uma delas foi a do deputado David Davis, que chegou a dizer que "o Governo britânico está a tratar o país inteiro como um suspeito", mas pouco depois foi nomeado ministro do Brexit e abandonou o assunto. Pelo seu lado, a Amnistia Internacional e outras onze organizações de direitos

humanos e jornalismo apresentaram uma reclamação ao Tribunal Europeu dos Direitos Humanos para tentar travar a Lei.

Uma das denúncias feitas por Edward Snowden, em 2013, era que, desde os anos 90, a agência de informações do Reino Unido intercetava e processava, indiscriminadamente e em segredo, milhões de comunicações privadas de cidadãos e partilhava esses dados com as agências de informações de outros países. O caso é especialmente grave, porque pelas ilhas britânicas passam os principais cabos de Internet do mundo.

Como declarava Martha Spurrier, directora da Liberty, uma das entidades denunciantes: "Perder a nossa privacidade é a porta de entrada para perder tudo o que nos mantém livres: o direito de protestar, o de ter um julgamento justo, o de praticar a nossa religião, o de pensar e de falar livremente. Nenhum país que implementa vigilância estatal à escala industrial permaneceu alguma vez como uma democracia respeitadora dos direitos humanos. Agora esperamos que o tribunal defenda os nossos direitos, pois o nosso Governo não o fez".

Emmanuel Macron chegou à presidência de França num momento em que a ferida do terrorismo estava demasiado aberta para não fazer nada. Por isso, ao fim de alguns meses de governo, não lhe foi difícil aprovar uma série de medidas que preocupam, e muito, os especialistas em privacidade.

Em junho último, o presidente francês criou um Centro Nacional de Contraterrorismo (CNCT – Centre National de Contre-Terrorisme) para melhorar a coordenação dos serviços de informações. Poucos meses depois, a França aprovava uma Lei de Exceção Antiterrorista, que não é exatamente um estado de exceção permanente, mas que aumenta a facilidade dos corpos de segurança para vigiar possíveis suspeitos (movimentos, registos, atividade na Internet…), mesmo que nunca tenham cometido qualquer delito.

O advogado francês François Sureau, especialista em privacidade, declarou ao "Le Monde" que "a ideia de, por ter havido três atentados, há que considerar as garantias liberais como um luxo, é surpreendente". E a verdade é que a legislação francesa diminui a intervenção do poder judicial em benefício da autoridade administrativa, o que para os críticos é, em última análise, enfraquecer o Estado de Direito; algo que não faz mais do que alimentar a ideia de que existe uma dicotomia entre liberdade e segurança.

Um mês depois da concretização da polémica aprovação, o governo francês anunciava ter sido criada uma unidade de segurança especializada na qual os investigadores poderão usar *spyware*: ferramentas tecnológicas para extrair dados (isto é, *hackear*) dos dispositivos informáticos de uma pessoa envolvida numa investigação judicial. Irá ser um serviço ultrassensível cujas atividades serão consideradas classificadas.

Em pouco mais de seis meses, Emmanuel Macron demonstrou a preocupação do governo francês pela segurança, mas haverá que esperar um pouco mais para avaliar a legitimidade dos seus modos.

C. G. H.

"Falso testimonio"

"Bearing False Witness"

Autor: Rodney Stark
Sal Terrae
Santander (2017)
302 págs.
Tradução (Castelhano):
Isidro Arias Pérez.

"Não sou católico romano", diz Rodney Stark, " e não escrevi este livro em defesa da Igreja. Escrevi-o em defesa da História". A origem deste ensaio é o mal-estar intelectual de um sociólogo da religião que, ao investigar anteriormente o cristianismo primitivo e medieval, foi-se dando conta de importantes distorções que deformam o julgamento sobre a ação da Igreja católica.

Stark, codirector do Instituto para os Estudos da Religião na Universidade de Baylor (Texas), havia estudado a rápida expansão do cristianismo nos três primeiros séculos ("The Rise of Christianity" em "Aceprensa", 28.5.1998) e o substrato cultural cristão que tornou possível o progresso da civilização ocidental ("How the West Won" em "Aceprensa", 3.3.2015).

Nesta nova obra seleciona uma série de temas bastante habituais na polémica anticatólica – antissemitismo, obscurantismo medieval, Inquisição, rejeição da ciência…– e vai-os pondo à prova. No começo de cada capítulo expõe a visão convencional e arraigada sobre o assunto, para depois a confrontar com os resultados de investigações modernas e não tendenciosas. Stark não pretende ser um especialista em cada um desses temas; por isso, dá conta em cada capítulo dos estudos especializados sobre os quais se baseia e cujos resultados divulga.

A sua condição de sociólogo nota-se na sua atenção aos números, sempre que é possível. Por exemplo, a ideia de que a partir de Constantino a Igreja aproveitou a sua nova condição para extirpar rapidamente o paganismo, fica em questão ao observar a filiação religiosa dos indivíduos nomeados cônsules e perfeitos até meados do século V, lista em que

os pagãos são uma grande parte. Também chama a atenção que, durante o período compreendido entre 1540 e 1700, nos tribunais da Inquisição espanhola, de 44 674 processados, somente 826 foram executados, e deve ter-se em conta que estes tribunais não se pronunciavam somente sobre acusações de heresia, como também sobre outros delitos: violações, perjúrio ou abuso de menores.

Ou quando, contra o lugar-comum de que a ciência arranca na era do Iluminismo graças à sua rutura com a fé cristã, Stark fixa-se na filiação religiosa de 52 cientistas de topo da época, e verifica que um quarto deles são clérigos, existem tantos católicos como protestantes e, no conjunto, 60 % são crentes convictos e apenas 1 %, céticos.

Não é que Stark pretenda apresentar uma folha de serviços da Igreja católica sem mácula. Em cada tema tratado reconhece também falhas e limitações. Mas coloca-as no contexto da época, o que em muitos casos mostra que a Igreja fez melhor do que outros, cuja atitude não costuma ser recordada. Como também tendem a ser silenciadas perseguições implacáveis contra a Igreja, por parte dos revolucionários franceses ou pelos regimes comunistas, fanatizados pelo empenho de erradicar a fé.

O livro de Stark é uma alegação eficaz para sacudir intelectualmente preconceitos que, por preguiça mental ou deturpação intencional, transmitem uma visão negativa do catolicismo.

I. A.