Commentary

BIG DATA & SOCIETY

Big Data & Society
January–June 2019: 1–6
© The Author(s) 2019
DOI: 10.1177/2053951719855091
journals.sagepub.com/home/bds
SAGE

Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights

Ana Beduschi

Abstract

The World Bank estimates that over one billion people currently lack official identity documents. To tackle this crucial issue, the United Nations included the aim to provide legal identity for all by 2030 among the Sustainable Development Goals. Technology can be a powerful tool to reach this target. In the digital age, new technologies increasingly mediate identity verification and identification of individuals. Currently, State-led and public–private initiatives use technology to provide official identification, to control and secure external borders, and to distribute humanitarian aid to populations in need. All of these initiatives have profound implications for the protection of human rights of those affected by them. Digital identity technologies may render individuals without legal documentation more visible and therefore less vulnerable to abuse and exploitation. However, they also present risks for the protection of individuals' human rights. As they build on personal data for identification and identity verification, data protection and privacy rights are most clearly affected. The prohibition of discrimination in the digital space is also of concern as these technological advances' societal impact is not yet fully understood. Accordingly, the article argues that emerging digital identity platforms will only contribute to the protection of human rights if the providers adequately mitigate any risks of potential discrimination and promote high standards of privacy and data protection.

Keywords

Biometric data, blockchain, data protection, digital identity, non-discrimination, privacy

Introduction

A valid proof of legal identity is often a prerequisite for accessing many basic services including healthcare, social protection, banking or education (World Bank, 2018a). Presently, over one billion people still lack ways of proving legal identity (World Bank, 2017a). Such a situation is primarily due to the absence of birth registration in less developed countries, statelessness, or the loss of documentary evidence. Technology can help address this problem, by providing digital tools for identity verification and identification.

This article evaluates the implications that such digital identity technologies can have for the protection of human rights. It places the analysis within the framework of international human rights law (IHRL) and data protection instruments such as the General Data Protection Regulation (GDPR). The article argues that albeit worthwhile, digital identity platforms will only contribute to the protection of human rights if the providers adequately mitigate any risks of potential discrimination and promote high standards of privacy and data protection.

Prioritising legal identity for all

In law, everyone has the right to be recognised as a person (Article 6, UDHR; Article 16, ICCPR; Article 24, ACHR; Article 3, ACHPR) and to be treated equally before the law without any form of discrimination (Articles 1, 2 and 7, UDHR; Article 26, ICCPR;

Law School, University of Exeter, Exeter, UK

Corresponding author:
Ana Beduschi, Law School, University of Exeter, Exeter, UK.
Email: a.beduschi@exeter.ac.uk

Article 14, ECHR; Article 1, ACHR; Article 2, ACHPR). Similarly, every child has the right to be registered at birth (Article 24, ICCPR; Article 7, CRC).

In practice, however, substantive equality (Fredman, 2016) is compromised when individuals who are formally entitled to equal treatment are materially unable to access their rights due to the lack of proof of identity. Without a birth certificate, children face additional difficulties in access to education. Similarly, asylum-seekers without documentary evidence of their identity and age may incur significant problems in acquiring legal status in a host country.

Therefore, verifying legal identity is not an easy task for those who have not been registered at birth or for those who lack legal documentation. Those individuals tend to concentrate in Sub-Saharan Africa and South Asia (Asian Development Bank, 2016; World Bank, 2017b). To tackle this major challenge, the United Nations included the aim to provide legal identity for all by 2030 among the Sustainable Development Goals (UN SDGs) in Target 16.9. Technology can be a powerful tool to reach this target.

Bridging the identity gap with digital technologies

In the digital age, new technologies increasingly mediate identity verification and identification of individuals (Sullivan, 2016, 2018). Life factors including date and place of birth, origins, ethnicity, nationality and biological features such as eye and hair colour are still commonly used. However, biometric data such as fingerprints and iris scans have a prominent place in identity verification and identification. For example, biometric passports have become a standard tool for a variety of states (Torpey, 2018). Another example is India's Aadhaar programme, which uses biometric technology to record fingerprints and iris scans in addition to personal information such as name, date of birth and domicile (Abraham, 2018). Biometric technology is also used for border control and migration management in the European Union (Eurodac Regulation).

More recently, we saw the emergence of solutions combining biometrics and blockchain technologies for digital identification. Blockchain uses decentralised distributed ledger technology (Swan, 2015) which can be an advantage for digital identity providers as data is not stored in a single central database (Tapscott, 2017). Instead, the data is encrypted and recorded in the different blocks of the chain, making it challenging to delete or tamper with the information stored in it (Finck, 2018). However, this also means that any personal information directly stored in the chain cannot be easily removed (Zyskind, 2015), creating challenges for data protection. Similarly, blockchain is not exempt from security concerns, as for example, private keys may be stolen by hackers or lost (Iuon-Chang and Tzu-Chun, 2017; Swan, 2015). Still, blockchain enthusiasts maintain that this technology could contribute to building a self-sovereign identity, or in other words, a digital identity owned and controlled by the user – who can then decide with whom and when to share information contained in their 'digital wallet' (Tobin and Reed, 2017).

International organisations, including the World Bank, play an important role in promoting and assisting states with the implementation of digital identity solutions encompassing domestic as well as refugee populations (World Bank, 2018c). The United Nations High Commissioner for Refugees (UNHCR) provides refugee registration using biometric data to verify identity (UNHCR, 2018). The World Food Programme uses blockchain technology to distribute aid (2018) while the World Economic Forum supports financial inclusion through technology (2018). The ID2020 Alliance, a public–private initiative, also funds digital identity solutions based on blockchain and biometric technologies in less developed states (2019).

Presently, several states have implemented or are considering digital identity solutions using these technologies. Besides India, Estonia has implemented a digital citizenship model (e-Estonia, 2019). Australia and Canada are currently exploring ways to adopt digital identity solutions (DIACC, 2019; DTA, 2019). Guinea and Ivory Coast are leading the West Africa Unique Identification for Regional Integration and Inclusion programme on digital identity (World Bank, 2018b).

Digital identity campaigns embraced by states can operationalise their obligations under IHRL, giving full effectiveness to everyone's right to be recognised as a person and to be treated equally before the law. Such initiatives can work as equalisers of societal disparity, providing excluded individuals with the means to prove their identity and to access services. In doing so, they function as enablers of opportunities (Haenssgen and Ariana, 2018; Sen, 1992: 48) for those individuals without proof of legal identity. These individuals have a limited set of opportunities when compared to the rest of the world's population. In this regard, they are not free to do or to be whatever they choose (Sen, 2005: 153). They do not have the opportunity to do what others take for granted, such as opening a bank account or registering to attend school. Digital identity technologies can facilitate access to opportunities – and thus give choices to those individuals. Besides, they may render those individuals without legal documentation more visible and therefore less vulnerable to abuse and exploitation.

Complying with human rights and non-discrimination law

Technology alone cannot protect human rights or prevent discrimination. Depending on how digital identity technologies are designed and used, they may also hinder the rights of those that they intend to benefit. These technologies can simultaneously include and exclude individuals from protection. For example, using blockchain technology to identify highly persecuted groups of people such as the Rohingya minority in Myanmar may allow them to access services in a host country such as Bangladesh (Rohingya Project, 2018). However, it may also allow for more efficient ways to discriminate these populations since identification makes them more visible. That could be for instance the case with the marginalisation of ethnic minorities such as the Uyghurs in China (Byler, 2019). Moreover, the digitisation of identity is understandably not exempt from cybersecurity threats (Singer and Friedman, 2014: 34). Therefore, it may also present a risk for their safety. If the information falls into the wrong hands, it may facilitate persecution by authorities targeting individuals based on their ethnicity.

Digital identity may thus be used to promote equal treatment, but it can also contribute to discriminatory practices, even if indirectly. IHRL prohibits any discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status (Article 26, ICCPR; Article 14, ECHR; Article 1, ACHR). Indirect forms of discrimination occur when a rule that is neutral in appearance leads to less favourable treatment of an individual or a group of individuals on one or more of these protected grounds. In the digital identity context, it has been shown that biometric data collected from older individuals are often of less good quality (Rebera and Guihen, 2012). This is because ageing and manual labour can both cause changes in an individual's biometric information. Solely relying on biometric technology for identification and verification can, therefore, affect older individuals more severely, as their fingerprints and iris scans may not guarantee that identity verification and identification will always be possible (Abraham, 2018). As a result, they may experience obstacles in joining and using digital identity programmes. If access to services requires digital proof of identity, they may also be excluded from these benefits.

Moreover, digital identity initiatives must be kept to what is necessary for the fulfilment of their aim and not go beyond what is proportionate to their objective. States should not use the information collected for digital identification for any other purposes outside of what individuals were informed of and had agreed to. In particular, states should not transform digital identity platforms into tools for digital surveillance (Hu, 2017). As the ECtHR has noted 'any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance [between the State's and the individuals' interests]' (*S. and Marper v United Kingdom*, para. 112). All the more, states should be particularly careful when individuals affected by these technologies are amongst the most vulnerable populations, such as refugees.

Digital identity solutions must be implemented within systems design to comply with IHRL. Ideally, non-discrimination considerations should be integrated into the design of digital identity platforms from the outset, leading to what could be described as 'non-discrimination by design platforms.' Technical solutions may take inspiration in the existing privacy and data protection by design protocols (Rachovitsa, 2016). Furthermore, teaching the basics of human rights law to software engineers responsible for innovation in the digital identity sphere could contribute to better compliance with the legal requirements (Beduschi, 2018). Scenario-based learning techniques could be used to disseminate a better understanding of non-discrimination requirements and thus enhance software engineers' preparedness to design technological solutions responsibly.

Meeting data protection and privacy imperatives

Finally, digital identity technology must also comply with the legal requirements of data protection and privacy. All states parties to international treaties on human rights must respect, protect and fulfil the rights to private life, home and correspondence (Article 12, UDHR; Article 17, ICCPR; Article 8, ECHR; Article 11, ACHR) of all individuals within their jurisdiction. One's right to private life encompasses one's 'personal identity,' 'aspects of physical and social identity,' (*Pretty v United Kingdom*, para. 61; *Mikulić v Croatia*, para. 53; *Atala Riffo v Chile*, para. 135), a person's right to their image (*Axel Springer AG v Germany*, para. 83) and their personal data, including biometric, genetic and electronic data (*S. and Marper v United Kingdom*, para. 68). State interferences with this right can only be justified if they have a legal basis in domestic law, pursue a legitimate aim and are necessary and proportionate to that aim (*Big Brother Watch v United Kingdom*, para. 304; *Escher v Brazil*, para. 116).

Accordingly, domestic laws establishing digital identity programmes must determine with enough clarity their scope of application, the safeguards they put in place on data storage, duration, usage, destruction and access of third parties, as well as the guarantees against

arbitrariness and abuse. To illustrate, the Supreme Court of India recently confirmed that these requirements applied to India's Aadhaar programme, which had been criticised for lacking a comprehensive privacy safeguard mechanism (*Justice K. S. Puttaswamy (Retd.) and Anr. v Union of India*, para. 153). The same considerations apply to blockchain technology, which presents significant risks unless the necessary safeguards are implemented (Finck, 2018). Domestic laws should require that technology developers implement such safeguards as a matter of design.

Public–private initiatives led by non-state actors including private companies should align their practices to the existing standards on privacy and data protection. In this regard, data protection rules provided by the GDPR can be of assistance. These rules apply to state and non-state actors alike, even though formally their extraterritorial reach is limited to processing or controlling of EU data subjects' personal data (Article 3, GDPR).

Two main aspects are particularly relevant to digital identity providers. Firstly, the GDPR's definition of personal data encompasses 'any information relating to an identified or identifiable natural person' (Article 4-1, GDPR). This definition is broader than, for instance, the concept of personally identifiable information used in the United States (Schwartz and Solove, 2011). Opting for the most comprehensive definition – the one proposed by the GDPR, even when operating outside of its remit – can provide a clear benchmark for anyone deploying digital identity solutions. Secondly, the GDPR puts forward a list of key requirements, which include the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, data integrity and confidentiality (Article 5, GDPR). Digital identity providers should consider these requirements as part of the design of technical and organisational measures (Article 25, GDPR). Privacy by design and data protection by design (Article 25-1, GDPR) can be instrumental in avoiding common privacy and data breaches (Omidyar Network, 2017; Rachovitsa, 2016; Schartum, 2016). In doing so, digital identity providers can contribute to the implementation of best practices in matters of data protection wherever they operate.

Conclusion

New technologies have the potential to revolutionise how individuals are identified and how their identity is verified online. Such technologies may be a useful tool to provide legal identification for those without proof of identity, thus meeting the UN SDG Target 16.9. However, emerging digital identity platforms will only effectively contribute to the protection of human rights if they comply with IHRL, adequately mitigate the risks of potential discrimination, and promote high standards of privacy and data protection. Such considerations should be integrated into digital identity platforms' design from the outset. If innovators and technology developers do so, they can promote best practices and contribute to the implementation of better levels of protection of human rights around the world. Their actions in this field would thus ensure that human rights remain relevant amid the rapid technological advances that have come to define our current digital age.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Ana Beduschi https://orcid.org/0000-0002-8037-5384

References

Abraham R (2018) State of Aadhaar Report 2017–18, s.l.: s.n.

Asian Development Bank (2016) Identity for development in Asia and the Pacific, s.l.: s.n.

Beduschi A (2018) Technology dominates our lives – That's why we should teach human rights law to software engineers. Available at: https://theconversation.com/technology-dominates-our-lives-thats-why-we-should-teach-human-rights-law-to-software-engineers-102530 (accessed accessed 30 May 2019).

Byler D (2019) China's hi-tech war on its Muslim minority. *The Gardian,* 11 April.

DIACC (2019) DIACC. Available at: https://diacc.ca//

DTA (2019) Digital identity programme. Available at: https://www.dta.gov.au/what-we-do/policies-and-programs/identity/ (accessed accessed 30 May 2019).

e-Estonia (2019) e-identity. Available at: https://e-estonia.com/solutions/e-identity/id-card/ (accessed accessed 30 May 2019).

Finck M (2018) Blockchains and data protection in the European Union. *European Data Protection Law Review* 4(1): 17–35.

Fredman S (2016) Substantive equality revisited. *International Journal of Constitutional Law* 14: 712.

Haenssgen MJ and Ariana P (2018) The place of technology in the capability approach. *Oxford Development Studies* 46: 98.

Hu M (2017) Biometric surveillance and big data governance. In: Gray D and Henderson SE (eds) *The Cambridge*

Handbook of Surveillance Law. Cambridge: Cambridge University Press, p. 121.
ID2020 (2019) Available at: https://id2020.org/ (accessed accessed 30 May 2019).
Iuon-Chang L and Tzu-Chun L (2017) A survey of blockchain security issues and challenges. *International Journal of Network Security* 19(5): 653–659.
Omidyar Network (2017) Digital identity and privacy, s.l.: s.n.
Rachovitsa A (2016) Engineering and lawyering privacy by design: Understanding online privacy both as a technical and an international human rights issue. *International Journal of Law and Information Technology* 24: 374.
Rebera AP and Guihen B (2012) Biometrics for an ageing society. Societal and ethical factors in biometrics and ageing. In: *Proceeding international conference of the biometrics special interest group*, Darmstadt, Germany, 6-7 September 2012.
Rohingya Project (2018) A Rohingya initiative. Available at: http://rohingyaproject.com/ (accessed accessed 30 May 2019).
Schartum DW (2016) Making privacy by design operative. *International Journal of Law and Information Technology* 24: 151.
Schwartz PM and Solove DJ (2011) The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review* 86: 1814.
Sen A (1992) *Inequality Re-examined*. Oxford: Oxford University Press.
Sen A (2005) Human rights and capabilities. *Journal of Human Development* 6: 151.
Singer PW and Friedman A (2014) *Cybersecurity: What Everyone Needs to Know*. Oxford: Oxford University Press.
Sullivan C (2016) Digital citizenship and the right to digital identity under international law. *Computer Law & Security Review* 32: 474.
Sullivan C (2018) Digital identity. From emergent legal concept to new reality. *Computer Law & Security Review* 34: 723.
Swan M (2015) Blockchain: Blueprint for a new economy, s.l.:O'Reilly Media.
Tapscott D (2017) Blockchain: The ledger that will record everything of value to humankind, s.l.: s.n.
Tobin A and Reed D (2017) The inevitable rise of self-sovereign identity, s.l.: Sovrin Foundation White Paper.
Torpey J (2018) *The Invention of the Passport. Surveillance, Citizenship, and the State*. Cambridge: Cambridge University Press.
United Nations High Commissioner for Refugees (UNHCR) (2018) *Biometric identity management system*. Available at: http://www.unhcr.org/550c304c9.html (accessed accessed 30 May 2019).
World Bank (2017a) 1.1 Billion ''invisible'' people without ID are priority for new High-Level Advisory Council on Identification for Development. Available at: http://www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-wi (accessed accessed 30 May 2019).
World Bank (2017b) The State of Identification Systems in Africa, s.l.: s.n.
World Bank (2018a) Principles on identification for sustainable development: Towards the digital age. Available at: http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age (accessed accessed 30 May 2019).
World Bank (2018b) Cote d'Ivoire and Guinea to kick-start West Africa Regional Identification Program. Available at: https://www.worldbank.org/en/news/press-release/2018/06/05/cote-divoire-and-guinea-to-kick-start-west-africa-regional-identification-program (accessed accessed 30 May 2019).
World Bank (2018c) Technology Landscape for Digital Identification, s.l.: s.n.
World Economic Forum (2018) Digital identity. On the threshold of a digital identity revolution, s.l.: s.n.
World Food Programme (2018) Blockchain for zero hunger. Available at: https://innovation.wfp.org/project/building-blocks (accessed accessed 30 May 2019).
Zyskind G et al., (2015) Decentralizing privacy: Using blockchain to protect personal data. In: *Proceedings of the IEEE security and privacy workshops*, San Jose, CA, USA, 21-22 May 2015, pp. 180–184.

Appendix 1

Legal documents and case law

International treaties

African Charter on Human and Peoples' Rights (ACHPR) 27 June 1981 (1982) 21 ILM 58.

American Convention on Human Rights (ACHR) 22 November 1969 1144 UNTS 123.

European Convention on Human Rights (ECHR) 4 November 1950 ETS 5.

International Covenant on Civil and Political Rights (ICCPR) 16 December 1966 999 UNTS 171.

Universal Declaration of Human Rights (UDHR) 10 December 1948 UNGA Res 217 A (III).

European Union

Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection

lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Eurodac Regulation) OJ L 180.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) OJ L 119.

Case law

European Court of Human Rights

Axel Springer AG v Germany, App no 39954/08 (ECtHR, 7 February 2012).

Big Brother Watch v United Kingdom, App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018).

Mikulić v Croatia, App no 53176/99 (ECtHR, 7 February 2002).

Pretty v United Kingdom, App no 2346/02 (ECtHR, 29 April 2002).

S. and Marper v United Kingdom, App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008).

Inter-American Court of Human Rights

Atala Riffo v Chile (Merits, Reparations and Costs) Inter-American Court of Human Rights Series C No 254 (24 February 2012).

Escher v Brazil (Preliminary Objections, Merits, Reparations and Costs) Inter-American Court of Human Rights Series C No. 200 (6 July 2009).

Supreme Court of India

Justice K. S. Puttaswamy (Retd.) and Anr. v Union of India and Ors (Supreme Court of India, 26 September 2018) Writ Petition (Civil) No 494 of 2012.