TechSonar

2021-2022 REPORT

EDPS

European Data Protection Supervisor

Project Number: 2021.5702
Title: TechSonar reports
December 2021
Editors: Thomas Zerdick, Stefano Leucci
Authors: Dina Kampouraki, Robert Riemann, Vítor Bernardo, Maria Enescu, Marek Jessen, Kostantina Vemou, Stefano Leucci

PDF/Volume_01 QT-03-21-444-EN-N ISBN 978-92-9242-127-4 doi:10.2804/641632

Technologies worth monitoring

By Wojciech Wiewiórowski

It is undeniable that - amongst a number of difficulties – the COVID-19 pandemic will leave us with many lessons learned. Above all, we have certainly learned that **the world changes and will continue to change, sometimes quite unexpectedly.** We have also learned that there is room for manoeuvre which would allow us to understand the changes, anticipate them, and direct them towards a more sustainable future.

To do this, **we need new tools and new sensibilities.** In particular, the acceleration of technological change that is taking place as a consequence of COVID-19 makes these capabilities even more necessary. Often we do not know the real main uses that these technologies will have until they are applied in specific contexts. Only then will we be able to understand the real value and the real risks that these technologies may have on society.

The General Data Protection Regulation, in recital 4, reminds us that: **"processing of personal data should be designed to serve mankind"**. For this to happen, at such a complex time, I am convinced that it is increasingly important to act in advance.

In other words, **instead of reacting to new emerging technologies when their added value and risks for society are already visible, we should be able to anticipate their developments.** In this way, we can foresee the risks and better support the value-creation process of these technologies. As a result, we might be able to nudge their developers and their development towards respecting fundamental rights and interests of individuals, reducing their risks from the earliest stages of their adoption.

This approach will also help us **focus our energy making Europe more resilient and future-proof**, as already indicated in the latest foresight report of the European Commission.

Based on all this, a big question arose here at the EDPS. **Which technologies are worth monitoring today in order to be prepared for a more sustainable digital future where the protection of personal data is efficiently guaranteed?** To find proper answers to this question, we launched this year, in 2021, our new initiative: **TechSonar.**

TechSonar is a **process** that empowers the EDPS to **continuously analyse the technology arena with the aim of selecting tech trends we foresee for the following year.**

Thanks to an **agile and collaborative approach**, a team of in-house technology experts meets regularly with the aim to provide a basic understanding of the selected technologies and highlight their main positive and negative impacts regarding the protection of personal data. The outputs are published and continuously updated in a dedicated section on the **EDPS website**. With TechSonar, we would like to take our first step in contributing to the wider debate on emerging technologies from a data protection point of view. As the independent supervisory authority for all Union institutions, bodies, offices and agencies, we aim to contribute to the ongoing wider debate on foresight within these institutions. We also hope that TechSonar will serve as a compass for future and more in-depth activities, both by the EDPS itself and other data protection authorities in Europe and around the world.

TechSonar falls within the first pillar of our **Strategy 2020-2024**, Foresight. While our successful TechDispatch continues to provide in-depth analysis on specific emerging technologies, TechSonar is our tool for navigating the surface of the complexity and uncertainty of the tech domain in general.

We are grateful to all the people that helped us with this first exercise. In particular, Professor Roberto Poli, who is professor at the University of Trento and UNESCO Chair in anticipatory systems, who helped us develop our awareness of the culture of foresight.

Think big, start small: how can we train our preparedness muscle?

By Thomas Zerdick and Stefano Leucci

In the international arena, the European Data Protection Supervisor (EDPS) is among the few personal data protection supervisory authorities that has taken active steps in the field of foresight and future studies for improving its way of working. With respect to personal data, the EDPS is responsible for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions, bodies, offices and agencies, in accordance in particular with Regulation (EU) 1725/2018.

Amongst the tasks provided for in this regulation, it emerges in particular that the EDPS must **"monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies"**. In fact, the EDPS has always been a leading institution in the field of technological monitoring, with many initiatives in this area.

Starting in 2020, the EDPS has decided to use the foresight tools for the main purpose of "closely examining both the potential risks and opportunities offered by technological advances, understand the possibilities of new technologies and, at the same time, encourage the integration of data protection by design and data protection by default in the innovation process". Thus, the first pillar of the EDPS Strategy 2020-2024 is dedicated to foresight. The main goal is to foster an evidence-based dialogue on intrusive, emerging or hypothetical practices and to alert EUIs and the public when digital technology is deployed in a way that does not respect the essence of the fundamental rights of personal data protection.

Thanks to the fundamental value that guides its work – namely, **independence** - the EDPS primarily aims at work in a more anticipatory manner within the data protection playing field in order to participate in the data protection community in a more effective manner, avoiding dispersion of its resources.

To do this, the EDPS decided to develop an inclusive and agile process that leverages on collective intelligence, also aiming to increase the collaboration between internal units.

Thanks to small and measurable actions the main aim of foresight at the EDPS is to acquire capacities and knowledge while evolving the organization organically toward a new way of being prepared to upcoming developments in the technology and data protection field.

1. METHODS

For these purposes, EDPS has developed the TechSonar project with the aim of identify emerging technologies in a short time window of one year. The decision to select such a small time frame is guided by the need to have an immediate return in the technological preparedness of the officers involved in activities occurring on a daily basis.

The **agile and collaborative approach** required the construction of a **team made up of technology**, legal and policy experts, across the various units and with various backgrounds. This team is internally known under the name of the **"EDPS Trend Taskforce"**, coordinated by a **Trend Coordinator.**

The work of the Taskforce applies a tailored methodology called **"Data Protection Technology Sonar"**.

The first step consists in a monitoring activity carried out by the Trend Coordinator, called **"initial scouting"**. With data analysis and observation, a series of weak and strong signals are identified through a qualitative and quantitative approach. A set of emerging technologies with an high-impact in the field of personal data protection and fundamental rights is then identified as output.

During phase two, the Trend Taskforce works in a **collective brainstorming session.**

The group firstly discusses and agreed on plausible future scenarios using a tailored horizon scanning approach aiming at understanding driving forces of change, weak signals and their interactions. According to the results, the group selects the technologies considered most impactful in the year to come. Finally, the group matches them to one individual expert, the **Tech Champion**, in principle one for each technology. Tech Champions are components of the Taskforce that volunteered to follow developments of the assigned technology and produce a dedicated report.

The third phase of **collective review** allows to improve the outcomes and avoid problems and bias that might arise in the process due to the inherent execution speed.

1. METHODS

During the fourth phase, the Trend Coordinator performs a review on the contents, published the outputs on the EDPS website and launched a series of **internal and external promotional and advocacy activities.**

The last phase is called **continuous monitoring.** Here, each Tech Champion continues to monitor the developments of the technology assigned to him in order to notify any relevant updates that will result in the updating of published reports. Moreover, the intended aim is to define a unique reference person for both internal and external stakeholders that looks to gain insight on that specific technology.

The methodology has been deployed for the first time, and the second phase is starting at the moment of the publishing of this paper.

With the occasion of this report, **many of the technologies identified so far have already required several report updates**, a sign that the technologies identified are in particular evolution.

We hope to continue to gain more experience and capacity from the recurrent deployment of our Data Protection Technology Sonar methodology and to be able to help the data protection community to increase its efficiency toward the design of personal data processing that will truly serve mankind.

Selected technologies for 2021-2022

Synthetic data
pag.10

Smart vaccination certificates
pag.7

Central bank digital currency
pag.12

Digital therapeutics
pag.18

Biometric continuous authentication
pag.16

Just walk out technology
pag.14

Smart vaccination certificates

By Dina Kampouraki and Robert Riemann

As COVID-19 vaccination programmes proceed in many countries, governments worldwide are moving towards issuing so-called **smart vaccination certificates (SVCs)** which are interoperable and that document the vaccination status of their bearers. Governments facilitate the re-opening of their economies by easing some restrictions for the free movement and travelling of individuals who have been vaccinated against SARS-CoV-2 and can demonstrate it with a vaccination certificate.

The European Union adopted its Regulation on the so called "EU Digital COVID Certificate" to enable free movement during the pandemic. When travelling across EU Member States, the EU Digital COVID Certificate holder should in principle be exempted from free movement restrictions: Member States should refrain from imposing additional travel restrictions on the holders of an EU Digital COVID Certificate, unless they are necessary and proportionate to safeguard public health.

Currently, many European countries such as France, Greece and Italy have already or are adopting SVCs to enter all indoor hospitality venues as cafés, restaurants, workplaces and a range of other venues in order to prove vaccination or immunity. This measure revealed necessary after the spread of new variants across the EU.
SVCs use machine readable images as barcodes with digital signatures and have been considered early on in the pandemic for their higher security against forgery and higher convenience both for the carrier and for the verifier. The WHO tasked in early 2021 a global working group of experts to provide recommendations for secure and interoperable SVCs. These recommendations also looked at situations with no printer, internet or smartphone. In May 2021 the scope and direction of the working group has been updated by WHO and refers in its recommendations now to Digital Documentation of COVID-19 Certificates (DDCC) that like the EU's DGC also encompass certificates on test and recovery status. The EU's use of interoperable SVCs provide for a sunset clause to retire the SVCs, but some experts expect that societies will rely on it also to fight future pandemics.

2.1 REPORTS

Amongst other countries, Israel is issuing COVID-19 certificates to Israeli citizens, and private businesses are already relying on those to grant access to private spaces e.g. restaurants, shopping malls, events. The USA are now also considering federal certificates or passports for travel and other purposes such as authorising to enter specific public and private places.

Positive foreseen impacts on data protection:

- **Easier and more secure access to personal data concerning health**: certificate bearers have easier access to their own health data. Because of the verification of digital signatures, their health data offers a high degree of integrity and is as such more trustworthy. SVCs are convenient, because they may be verified partially or entirely automatically.

- **Improved interoperability based on trust**: the interoperability design scheme of SVCs may enable the bearer to verify its health status with security across borders. For this interoperability between countries, authorities exchange cryptographic country keys as is already the case for the verification of electronic passports. Such a system relies on reciprocal trust amongst countries and the capacity of each country to accurately issue and manage COVID-19 vaccine certificate and the personal data include therein.

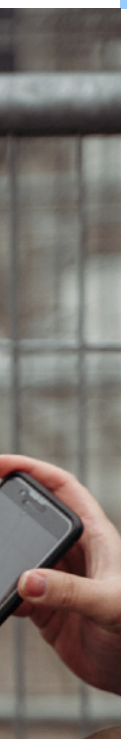
Negative foreseen impacts on data protection:

- **High risk of repurposing bearers' personal data**: SVCs must contain personal data allowing verifiers to link the health data to the carrier. However, this data may be repurposed to use SVCs as identity documents, enabling tracking of bearers. This opens doors to discrimination or infringement of the fundamental rights and freedoms of the bearers. For instance, event organisers or shops could recognise first-time and frequent guests and treat them differently.

- **Several risks from the software solution**: depending on the deployment of the software for bearers to manage and display their certificates, bearers may be nudged to use certain software solution that do not fully comply with data protection rules. If health data is stored on blockchains, risks for individual rights such as the right to correction or deletion may emerge. The potential centralisation of health data in backend IT infrastructure increases incentives of malicious actors to obtain the data.

Further readings:

- The Royal Society, Twelve criteria for the development and use of COVID-19 vaccine passports, February 2021 - **https://royalsociety.org/-/media/policy/projects/set-c/set-c-vaccine-passports.pdf**
- Privacy International, "Anytime and anywhere": Vaccination passports, immunity certificates, and the permanent pandemic, December 2020 - **https://privacyinternational.org/long-read/4350/anytime-and-anywhere-vaccination-passports-immunity-certificates-and-permanent and copy at https://edri.org/our-work/anytime-anywhere-vaccination-immunity-certificates-pandemic/**
- European Union eHealth Network, Interoperability of health certificates
- Trust framework, March 2021 - **https://ec.europa.eu/health/sites/default/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf**
- Ada Lovelace Institute, The socio-technical challenges of designing and building a vaccine passport system, February 2021 - **https://www.adalovelaceinstitute.org/event/socio-technical-challenges-designing-building-vaccine-passport-system/**
- Algorithm Watch, Analysis: Digital vaccine certificates – global patchwork, little transparency, March 2021 - **https://algorithmwatch.org/en/digital-vaccine-certificates-analysis-march-2021/**
- Word Health Organization, Revised scope and direction for the Smart Vaccination Certificate and WHO's role in the Global Health Trust Framework, June 2021 - **https://www.who.int/news/item/04-06-2021-revised-scope-and-direction-for-the-smart-vaccination-certificate-and-who-s-role-in-the-global-health-trust-framework**



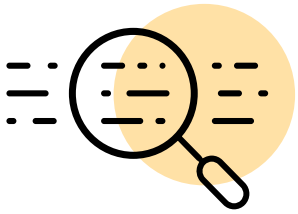
Synthetic data

By Vítor Bernardo

The concept of synthetic data generation is to take an **original data source (dataset)** and create new, artificial data, with similar statistical properties from it. Keeping the statistical properties means that anyone analysing the synthetic data, a data analyst for example, should be able to draw the same statistical conclusions from the analysis of a given dataset of synthetic data as he/she would if given the real (original) data. The process to create synthetic data, called synthesis, involves the use of generative models.

The way a generative model work is explained by Foster D., in the following way:

> **Suppose we have a dataset containing images of horses. We may wish to build a model that can generate a new image of a horse that has never existed but still looks real because the model has learned the general rules that govern the appearance of a horse. First, we require a dataset consisting of many examples of the entity we are trying to generate. This is known as the training data, and one such data point is called an observation. It is our goal to build a model that can generate new sets of features that look as if they have been created using the same rules as the original data.**



The use of synthetic data is growing in many fields: from training of artificial intelligence models within the health sector to computer vision, image recognition and robotics fields.

Positive foreseen impacts on data protection:

- **Less privacy-intrusive training of artificial intelligence models:** synthetic data allows for the training of artificial intelligence models, in a manner that is less privacy-intrusive for the individuals because the data used in the training process does not directly refers to an identified or identifiable person.

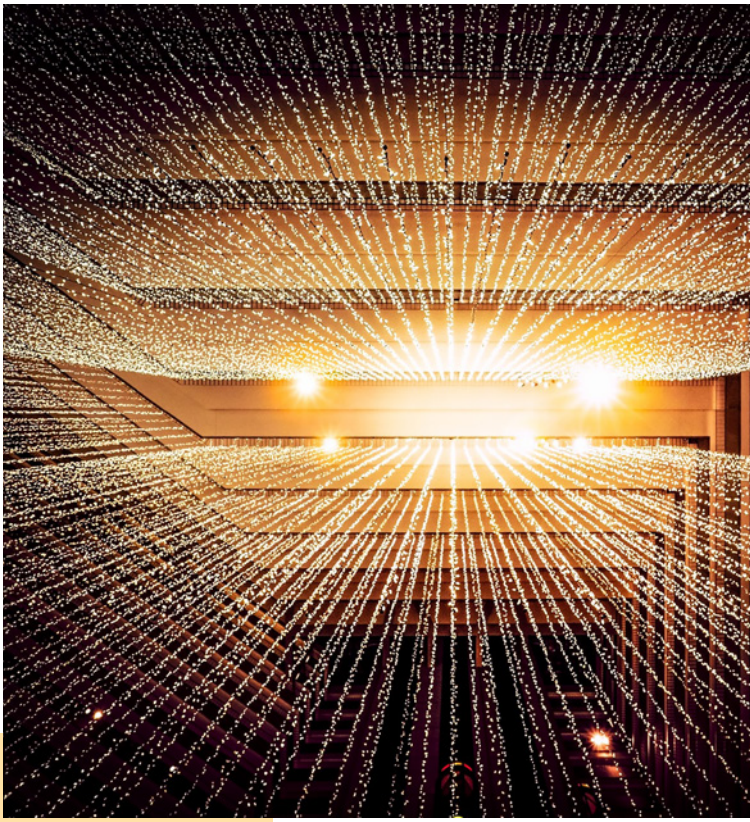
- **Enhanced privacy in data transfers:** synthetic data can be considered as a Privacy Enhancing Technology (PET) and, in that sense, it might be used as a supplementary measure for data transfers outside the European Union or within organizations that do not need to identify a specific person.

Negative foreseen impacts on data protection:

- **Risk of reidentification:** synthetic data generation implies a compromise between privacy and utility. The more a synthetic dataset mimics the real data, the more utility it will have for analysts but, at the same time, the more it may reveal about real people, with risks to privacy and other human rights.

- **Lack of clarity on other risks:** it is unclear at this stage if the data transference of generative models, which would allow other parties to generate synthetic data on their own, might bring further risks to privacy.

- **Risk of membership inference attacks seems possible:** synthetic data seems to share the same caveats of other forms anonymisation regarding the risk of membership inference attacks (i.e., the possibility for an attacker to infer whether the data sample is in the target classifier training dataset), especially when it comes to outlier records (i.e., data with characteristics that stand out among other records).



Further readings:

- Synthesis Tutorials, Replica Analytics - **https://replica-analytics.com/synthesis-tutorials**
- D. Foster, Generative deep learning: teaching machines to paint, write, compose, and play. O'Reilly Media, 2019
- T. Stadler, B. Oprisanu, C. Troncoso, Synthetic Data - A Privacy Mirage. arXiv preprint, 2020 - arXiv:2011.07018

Central bank digital currency

By Stefano Leucci and Robert Riemann

Central bank digital currency (CBDC) is a new form of money that exists only in digital form. Instead of printing money, the central bank issues **digital coins**. It mainly aims at facilitating digital transactions and transfers through a new type of widely accessible, digitally issued money.

Efforts on making CBDC is growing all over the world for many reasons. First, the COVID-19 crisis induced a shift in payment habits towards contactless payments and e-commerce due to fear of banknotes as a way for transmitting infection, accelerating the decline of cash use. Second, cryptocurrencies developed by private companies (e.g. Novi by Facebook) or informal communities (e.g. Bitcoin) have seen significant developments and value gain. As a response, 81 countries (representing over 90 percent of global GDP) are now exploring central bank digital currencies.

The European Central Bank, after exploring possible design scenarios for launching a Digital Euro, consulted some stakeholders. Results shown that privacy is considered the most important feature of a digital euro by both citizens and professionals. An investigation phase will start on October 2021, with the aim of investigate what a **digital euro** might look like.

CBDC could be developed in a number of ways. In a centralised approach, transactions are in ledgers managed by central banks that also provides user-facing services. In a decentralised approach, a central bank sets rules and requirements for the settlement of CBDC transactions that are then recorded by users and/or supervised intermediaries.

According to design choices, CBDC could have diverse impacts. First, worth noting that actual money requires many intermediaries in the payment process, resulting in less efficient and secure payment experience. CBDC could find solutions to these issues, developing a more efficient, fast and secure payment process. Then, CBDC can pose a risk of disruption to commercial banks and the financial ecosystem, depending on the new role that they will have or maintain.

Positive foreseen impacts on data protection:

- **Difficulties in demonstrating positive impacts:** since CBDC are at their very early stage, direct positive impacts cannot be demonstrated with concrete figures.

- **More control over personal data and security:** assuming that the development of CBDC will follow a strict data-protection-by-design and by-default approach, a CBDC could increase data protection and security in digital payments and provide payers more control over their personal data.

- **Enhanced anonymity in the payment process:** privacy-enhancing technologies could be used for enhancing anonymity within the entire payment process while permitting auditability only in pre-determined lawful cases, as for preventing money laundering, counter terrorism financing and tax evasion.

Negative foreseen impacts on data protection:

- **New players might increase the amount of data collected:** direct access to central bank accounts of a CBDC could lead to a flourishing of a number of new players that offer payment services and digital wallets. When this market development is linked to the increased efficiency of payments and transfers, many users might prefer a payment service based on CBDC, increasing the amount of personal data collected by such intermediaries.

- **Wrong design choices might worsen data protection issues:** payment data already reveals very sensitive aspects of a person. Wrong design choices in the underlying technological infrastructure might exacerbate the privacy and data protection issues that already exists in the digital payment landscape. For example, transactional data could be unlawfully used for credit evaluation and cross selling initiatives.

- **Lack of security might turn into lack of trust of users:** security concerns in payments can be worsened, leading to lack of privacy in payers and turning into lack of trust on the CBDC, that is among the core requirements for a monetary instrument to be exchanged.

Further readings:

- CBDC Tracker - **https://cbdctracker.org/**
- Atlantic Council, The Rise of Central Bank Digital Currencies, 20 April 2021 - **https://www.atlanticcouncil.org/cbdctracker/**
- European Central Bank, A digital euro – 2021 - **https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html**
- European Central Bank – Bank of Japan, Balancing confidentiality and auditability in a distributed ledger environment, February 2020 - **https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf**
- Institute and Faculty of Actuaries, Understanding Central Bank Digital Currencies (CBDC), March 2019 - **https://www.actuaries.org.uk/system/files/field/document/Understanding%20CBDCs%20Final%20-%20disc.pdf**

Just walk out technology

By Maria Enescu and Marek Jessen

Just walk out technology (JWO) enables shoppers to simply enter a store, take what they want, and just leave, enabling a seamless shopping experience. JWO is based on artificial intelligence, image recognition and sensors. These specific sensors are usually placed on the aisles/shelves of the shop to know Maria Enescu, Marek Hansen hat the shopper picks and wherever the product is being moved or placed somewhere else. Additionally, cameras are placed all around the shop in all aisles, racks, store walls, etc. The shopper, before entering the store, is required to have a specific mobile application that processes the necessary information regarding his personal profile and preferred payment method.

This **new way of shopping** can be summarised in four simple steps:

1. The customers scan a code on their phone when they enter the store;
2. When they pick something off the shelf, it is automatically added to their virtual cart;
3. If they put something back on the shelf, it is automatically removed from their virtual cart; and
4. Once they have what they need, they just leave the store and their credit card will be automatically charged for the items they purchased.

If shoppers need a receipt, they can visit a kiosk inside the store and enter their email address. The receipt will then be emailed to them for that shopping trip and for any subsequent ones for which they will use the same credit card. While Amazon and Alibaba - that respectively launched Amazon Go and Hema - were the only two players developing JWO, many new players are entering the market all over the world, also with few European retailers. Additionally, Amazon is pursuing a different strategy and has started to offer JWO technology to other retailers, which will help spread this concept further.

Positive foreseen impacts on data protection:

- **No positive impacts on data protection have been identified for the moment:** taking into consideration the early deployment of the technology in the market, there are no specific positive outcomes toward data protection. The situation may change in the case of a different design and configuration of the technology embedding privacy enhancing features.

Negative foreseen impacts on data protection:

- **Constant surveillance becoming the norm:** shoppers are closely tracked and monitored while moving around the store by facial recognition solutions and sensors. This implies a massive collection of personal data and might generate a feeling of being on constant surveillance. This can be linked to surveillance becoming the norm. In fact, people might get used to this technology and easily accept it for other purposes as well.

- **Repurposing of the shoppers' profile:** the constant profiling of the shoppers could be subsequently abused for other purposes such as targeted advertising and direct marketing.

- **Lack of transparency:** even if major technology providers declare that data collected in-stores will be associated with the customer's account for 30 days, it is unclear how this data will be used during and subsequent to this period of time.

- **Lack of safeguards for vulnerable subjects:** processing personal data of vulnerable subjects without any additional safeguards might exacerbate other data protection issues. For example, children might be exposed to facial recognition technologies when visiting the stores with their family.

Further readings:

- Amazon, Just Walk Out technology, 2020 - **https://justwalkout.com/**
- Lexology, Just Walk Out: Is this the future of shopping?, 2021 - **https://www.lexology.com/library/detail.aspx?g=792234aa-89cc-426a-89b6-bd1804884cc3**
- K. Wankhede, B. Wukkadada, V. Nada, Just Walk-Out technology and its challenges: a case of Amazon Go, 2018 - **https://ieeexplore.ieee.org/document/8597403**
- UPI, Amazon planning smart app-based 'Go' stores in U.S. next year, 2016 - **https://www.upi.com/Business_News/2016/12/05/Amazon-planning-smart-app-based-Go-stores-in-US-next-year/6781480980680/?ur3=1**

Biometric continuous authentication

By Konstantina Vemou

Authentication usually relies on statical processes like the use of passwords, cards, or any biometric trait of the person. The main aim is to verify the identity of users at the beginning of the delivery of a service or at the entrance of a specific area. Contrasting with this approach, continuous authentication aims at repeating this verification throughout a specific time frame during the delivery of an electronic service or during the presence of a person in a certain area.

Biometric continuous authentication is a type of continuous authentication that verifies a user identity by using biometric traits or behaviours. Examples include facial images, typing, screen tapping, walking patterns or voice. Applications of biometric continuous authentication can be seen in banking services, identification of stolen mobile devices or authentication on smart home devices.

Positive foreseen impacts on data protection:

- **Improved security:** in case of particular high risk within a process operation, this solution can improve the certainty that a subject is duly authorized to access specific data.
- **Improved user experience:** authentication is done in a seamless way, without stopping the users' experience with the service.

Negative foreseen impacts on data protection:

- **Risk of repurposing of the users' biometric data:** controllers could use stored biometric data for different purposes, such as unlawful tracking of employees, for disciplinary purposes or creation of profiles.
- **Excessive data collection:** depending on the purpose, the amount of data collected (even if not stored) could be excessive, contradicting the principle of data minimization.
- **Risk of chilling effect:** users might fear being tracked and profiled while using a system that continuously rely on their biometric feature for continuing the fruition of a service.

- **Lack of transparency and valid legal ground:** organisations might not properly inform data subjects on the fact that the captured biometric traits are used for training artificial intelligence algorithms without properly informing the data subjects and without choosing valid legal grounds.

- **Low data accuracy:** the adaptability of algorithms to changes of user behaviour - as result of users realising, they are continuously monitored - could lead to accept irregular patterns of behaviour and trigger false positive results in user authentication. Moreover, low accuracy of the involved algorithm could lead to depriving users from accessing a service.

- **Low control of data and high impact of data breaches:** users are not able to control when this technology is applied, while a data breach on the stored biometric data can have an important impact, as they are not in the position to change their biometric data.

Further readings:

- A. Krašovec, D. Pellarini, D. Geneiatakis, G. Baldini, V. Pejović, Not quite yourself today: behaviour-based continuous authentication in IoT Environments, Proc. ACM Interact. Mob. Wearable Ubiquitous Technol, 4, 2020 - **https://doi.org/10.1145/3432206**
- N. Memon, How biometric authentication poses new challenges to our security and privacy, IEEE Signal Processing Magazine, 2017 - **https://ieeexplore.ieee.org/document/7974880**
- A. E. Ahmed, Continuous Authentication Using Biometrics: Data, Models, and Metrics, IGI Global, 2012
- K. Niinuma, P. Unsang, A. K. Jain, Soft biometric traits for continuous user authentication, IEEE Transactions on information forensics and security 5, no. 4, 2010 - **https://ieeexplore.ieee.org/document/5570993**

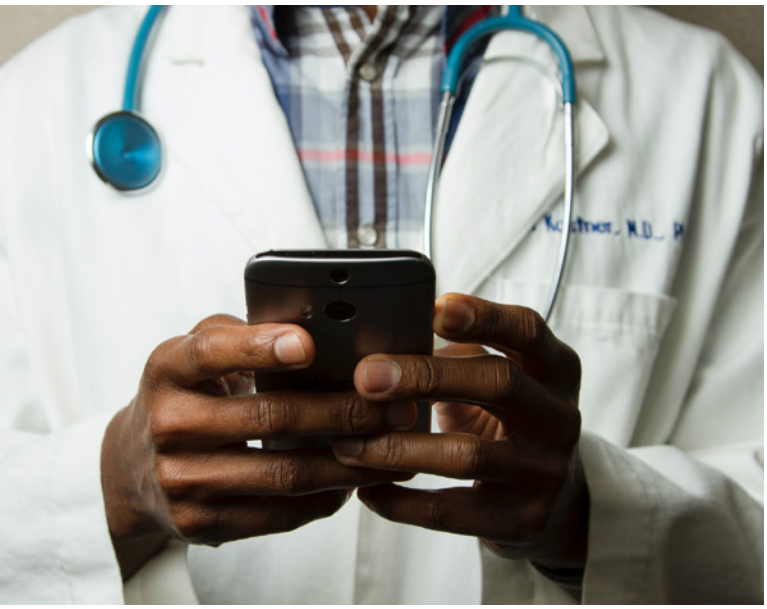
Digital therapeutics

By Dina Kampouraki

Digital therapeutics (DTx) are evidence-based therapeutic interventions driven by software to prevent, manage, or treat a medical disorder or disease. In other words, DTx are patient-facing software applications that help patients treat, prevent, or manage a disease and that have a proven clinical benefit. For example, Digital Therapeutics can support patients in self-managing symptoms and thereby improve their quality of life and other clinical endpoints. DTx uses digital implements like mobile devices, apps, sensors, virtual reality, the Internet of Things, and other tools to spur behavioural changes in patients. DTx development can have a positive impact on providing well customised health services as their design is tailored to fit patient's needs. Considered one of the most innovative areas within digital health, DTx ecosystem has experienced an accelerated period of progress over the past two years.

DTx can be used as a standalone therapy or in conjunction with more conventional treatments like pharmacological or in-person therapy or also with certain hardware or other sensory or mechanic devices. The treatment depends on the collection and processing of digital measurements. Because of the digital nature of the methodology, data can be collected and analysed as both a progress report and a preventative measure. Currently, treatments are being developed for the prevention and management of a wide variety of diseases and conditions, such as type II diabetes, congestive heart failure, Alzheimer's disease, anxiety, depression, and several others.

At the European level, the Regulation (EU) 2017/745 is a regulation of the European Union on the clinical investigation and sale of medical devices for human use. No specific legal regulation exists on DTx while the European Medicines Agency and the European Commission are starting exploring these solutions. On national level, the new German Digital Healthcare Act (DiGA) regulates specific requirements for the use of DTx. A list of requirements defines which features any DTx application must have. Important factors such as quality, security and data protection must be proven with scientific evaluation. France is moving forward to implement a similar legal act like Germany. In the USA, the Food and Drug Administration has an active pre-certification program in place since 2017 on DTx.



Positive foreseen impacts on data protection:

• No positive impacts upon data protection have been identified for the moment: taking into consideration the current design of this technology developed in the market, there are no specific positive outcomes toward data protection. The situation may change in the case of a different design and configuration of the technology embedding privacy enhancing features.

Negative foreseen impacts on data protection:

• Constant observation and profiling of the patient: a vast amount of personal data is collected directly from the patient and processed in a complex digital ecosystem. In most cases, accurate health and/or behavioural profile of the person are created for the functioning of the solution. This practice might entail risks of being constantly observed or the possibility of repurposing patients' profiles.

• High impact of personal data breaches: as the particular sensitivity and amount of personal data processed within DTx applications, a potential data breach can be a major threat against for the person concerned.

• Complexity might generate security flaws: the fact that the processing is done via numerous OSs and application providers might create risks on unlawful access across devices and providers due to possible security flaws.

Further readings:

- German Federal Institute for Drugs and Medical Devices - DiGA **https://www.bfarm.de/EN/Medical-devices/Tasks/Digital-Health-Applications/_node.html**
- Evidera, Digital Therapeutics: Past Trends and Future Prospects, 2020 - **https://www.evidera.com/digital-therapeutics-past-trends-and-future-prospects/#:~:text=Digital%20therapeutics%20(DTx)%20are%20a,1%20DTx%20are%20distinct%20from**
- Healthcare Global, Top 10 digital therapeutics, 2021 - **https://healthcareglobal.com/top10/top-10-digital-therapeutics**
- Digital Health London, Digital Therapeutics in the NHS: Report from the Digital Health. London Summit, 2018 - **https://digitalhealth.london/digital-therapeutics-in-the-nhs-report-from-the-digital-health-london-summit-24-april-2018**
- Digital Therapeutics Alliance website - **https://dtxalliance.org/**

edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor