derecom

ISSN: 1988-2629. Nº. 31. Nueva Época. Septiembre 2021-Marzo 2022

Cómo citar este texto:

Palacios-Alonso, D., Cousido-González, M.P., Domínguez-Mateos, F., Guillén-García, J., Ortega-delCampo, D., Conde, C. y Cabello, E. (2021). Privacidad por diseño, clave para la buena gobernanza, 31, 215-223, http://www.derecom.com/derecom/

PRIVACIDAD POR DISEÑO,
LA CLAVE PARA LA BUENA GOBERNANZA[1]

PRIVACY BY DESIGN,
THE KEY TO GOOD GOVERNANCE

© Daniel Palacios-Alonso
Universidad Rey Juan Carlos (España)
daniel.palacios@urjc.es
©M.P. Cousido-González
Universidad Complutense de Madrid (España)
cousidop@ucm.es
©Francisco Domínguez-Mateos
Universidad Rey Juan Carlos (España)
©Julio Guillén-García
Universidad Rey Juan Carlos (España)
©David Ortega-delCampo
Universidad Rey Juan Carlos (España)
©Cristina Conde
Universidad Rey Juan Carlos (España)
Enrique Cabello
Universidad Rey Juan Carlos (España)

Resumen

En la actualidad, el mundo gira en torno a las nuevas tecnologías digitales. Sin embargo, este hecho no carece de riesgos. Uno de ellos es la privacidad, que es un concepto claro pero no siempre respetado. Por lo tanto, desde el principio, es obligado el uso de protocolos eficientes o guías. Estas guías asegurarán los derechos de los ciudadanos sin socavar el uso de las nuevas tecnologías. La privacidad por diseño es un enfoque con una antigüedad de más de 20 años que busca proteger la vida privada de los ciudadanos. Para lograr esta ardua tarea, este marco legal define 7 conceptos básicos que aseguran, todo lo posible, consideraciones de privacidad desde el comienzo del diseño y desarrollo de las prácticas mercantiles, de los servicios, productos e infraestructuras. En este texto nos fijamos en el uso de este paradigma para alcanzar un desarrollo económico, social e institucional estable, en otras palabras, una buena gobernanza.

Recibido: 31/05/2021 Revisado: 10/08/2021
Aceptado: 15/08/2021 Publicado:15/09/2021

Summary

Nowadays, the world revolves around new digital technologies. However, this fact is not without risks. One of them is privacy which is a clear concept but not always respected. Therefore, from the beginning, using efficient protocols or guidelines is mandatory. These guidelines will ensure the rights of citizens without undermining the use of new technologies. Privacy by design is an approach with over 20 years that looks to protect citizens' privacy. To carry out this arduous task, this framework defines seven basic concepts which ensure, as far as possible, considerations of privacy concerns from the very beginning of the design and development of business practices, services, products, and infrastructures. In this paper we focus our attention on the use of this paradigm to achieve stable economic, social, and institutional development, in other words, good governance.

Palabras clave: Privacidad por diseño. Buena gobernanza. Inteligencia artificial. RGDP

Keywords: Privacy by design. Good governance. Artificial intelligence. GDPR

1.Introduction

Citizens' personal data are stored in large databases called "data warehouses". These databases contain sensitive information that can be illicitly obtained by criminals. Likewise, different state bodies of any country such as agencies, law enforcement agencies and governments have legal access to our personal data. However, these data are not without risk. On March 9, 2021, the Spanish Public Employment Service was attacked, paralyzing 710 offices that provide face-to-face service, as well as 52 telematic ones.[2] According to the Spanish government the data extraction did not happen, but the true extent of the attack is still unknown. Another international case was the attack on Microsoft exchange accounts, obtaining privileged information of user accounts.[3] For this reason, privacy should be a priority line for any state. It should be noticed that there are tools and frameworks which provide guidelines to prevent and ensure our personal data. As is well known, the General Data Protection Regulation (GDPR), in Article 25, deals with the topic "Data protection by design and by default".[4] Thus, a key point, in this regulation, is to consider privacy from the very beginning as an essential requirement. Thus, privacy will be accomplished for the whole life cycle. Regardless of whether a product, service, or whatever other element related to personal data is created.

On the understanding the cases aforementioned are relevant, it can be noticed that there are different levels of criticality in fraudulent data acquisition. For instance, biometric data have a high level that unequivocally points to a citizen. Hackers could carry out impersonation actions that seriously harm an individual. Some of the most common biometric data are fingerprint, iris, and facial recognition, among others. This kind of technology is mandatory in several critical scenarios such as airports, boundaries, among others. Nonetheless, where is the limit between global security or privacy infringement?

According to the state of emergency due to the global pandemic caused by the COVID-19 virus raises several questions related to the free movement of EU members and their neighbors. To carry out the free movement of EU members, avoiding undesired actions such as terrorism or criminality, it is necessary the sharing information between the agencies, states, and law enforcement agents (Interpol) of the Schengen area, mainly. Therefore, these data must be accessible, fast, reliable, and secure. This is where concepts of Big Data,[5] [6]and Privacy by Design (PbD) [6] [7]come into play.

PbD approach provides a powerful tool to establish answers, a priori, for questions such as what kind of personal data we are going to need/use? How are we going to obtain them? Is it licit to ask for these data? Answering these questions will avoid unexpected events and plausible penalties for the EU or others states.

In the current situation, citizens are considered as just providers of their own biometric data. Sometimes, access to databases is achieved and records without consent or even knowledge of the citizen. This situation is even worse with the huge spread of video surveillance cameras with high resolution to perform face recognition or identification at a distance. In this study case, the recommendation is addressed to obtain the consent of citizens in access to databases. As an example of this situation, an airport border is presented. In this case, it is mandatory to achieve a trade-off between security and privacy. A suggested mechanism to accomplish a balanced situation is based on the acquisition of personal data information only if the owner agrees.

In this paper we present the PbD approach and succinct biometric study case. The paper is organized as follows. The second section is dedicated to PbD. Finally, the last section is addressed to a brief discussion about the use of biometric in ABC gates and airports.

2.Privacy by design

Privacy and design (PbD) is not a novel concept. Indeed, this framework is more than 20 years. Anne Cavoukian (current Ontario's Data Protection Commissioner) developed this idea or concept during the nineties and was presented at the 31st International Conference of Data Protection and Privacy Commissioners in 2009.[8] In 2010, the framework was internationally accepted at the 32nd International Conference of Data Protection and Privacy Commissioners under the term "Resolution on Privacy by Design". This text includes the Foundational Principles of Privacy by Design as defined by Ann Cavoukian. The principles are shown as follows.

2.1.The seven basic principles

1) Proactive not Reactive; Preventative not Remedial. The key point is based on avoiding privacy infringements. For the rest, since prevention is better than cure, it is important to provide adequate responses.

2) Privacy as the Default Setting. The administrator or end-user has not to carry out any special task because privacy is configured from the beginning.

3) Privacy Embedded into Design. It is not an extra that is included at the end. From brainstorming to postmortem document the privacy is present. Privacy does not affect technical aspects, it takes part in the design.

4) Full Functionality: Positive-Sum, not Zero-Sum. It is not a fight between privacy and security.

5) End-to-End Security: Full Life cycle Protection. Before data exist, privacy is considered. Privacy is composed of tasks of gathering, storing, processing and destruction. PbD always will be in our minds, although new requirements are necessary.

6) Visibility and Transparency: Keep it Open. The process will be open access. Indeed, privacy could be audited to ensure accomplished requirements. This task should be carried out by an independent firm or agency.

7) Respect for User Privacy: Keep it User-Centric. Notifications will be user-friendly because the user is who provides data. Likewise, the average user is not an expert. Therefore, the system will be robust by default.

2.2.Criticism of privacy by design

PbD can be considered vague or diffuse, because it keeps many questions open in systems engineering applications. Furthermore, PbD behaves the same with respect to voluntary compliance in the industrial sector, e.g. environment. Therefore, it lacks strong convictions to be effective.

Nowadays, to develop a system or a concept, the approach used is an evolutionary one. However, in this case, the privacy by design concept must be maintained for each evolutionary iteration (even if it has not been demonstrated to be compliant). Some business models are built around customer surveillance and data manipulation. Thus, voluntary compliance seems unlikely.

The current definition of PbD does not address the methodological aspect of systems engineering, i.e. it does not detail the systems engineering methods used. These methods must cover all the technical specifications of the system and the data life cycle.

It should be noted that PbD is not focused on the actual data support, but on the design of the system. This role is not known in privacy law, so the concept of PbD is not based in law. This fact, in turn, undermines the trust of stakeholders, i.e. data subjects and policy makers.

3. Using PbD in ABC

The border crossing between EU countries is a matter of national and extraterritorial security. It is worth noting the definition of territory - a portion of the land area belonging to a nation. Therefore, a territory may not always be continuous, e.g. islands, embassies, and overseas territories.

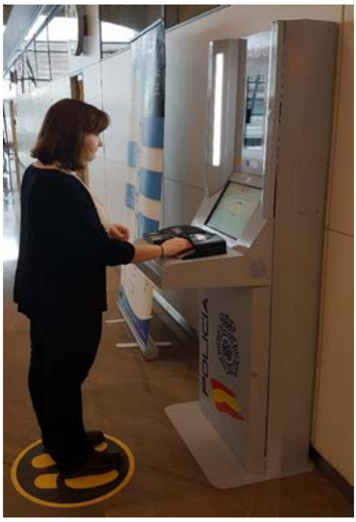

Fig. 1. Example of ABC.

EU airport services must provide high levels of security to prevent criminal situations but without prejudice to the rights and freedoms of passengers. Agencies such as FRONTEX[9] and ICAO[10] are collaborating to achieve a high-quality standard that provides passengers both, security, and freedom of movement. To this end, devices such as Automated Border Control (ABC) and e-Gate have been developed (see Fig. 1).

Currently, Artificial Intelligence (AI) is one of the crucial tools for border control, and more specifically, the use of facial recognition. The authentication process of the ABC consists of taking an image of the passenger and contrasting it with the one provided in the electronic machine readable travel document (eMRTD). There is even a high-end device known as a biometric corridor that performs taking and validation process of the image in real time (see Fig. 2).

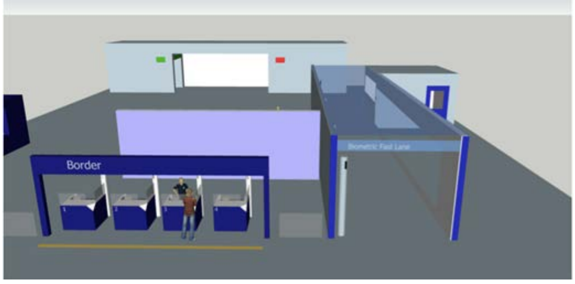

Fig. 2. 3D example of an eGate.

The ABC systems are exposed to multiple attacks or threats, for example, identity theft or fraud, which also is called spoofing. For this reason, many current research works focus their attention on anti-spoofing techniques,[11] [12].[13]

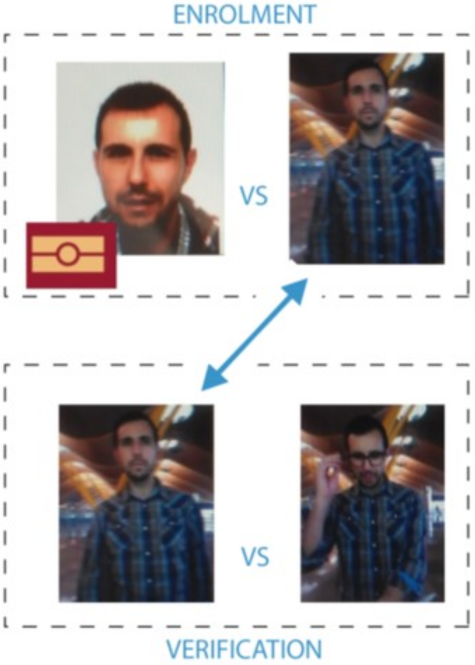

Fig. 3. Example of two stages belongs to ABC system.

ABC systems are composed of two stages, enrollment and verification processes (see Fig. 3). In first stage, the passenger stands in front of the ABC. The individual inserts the hand and the eMRTD. A snapshot of the passenger is then taken. The second stage, verification, is based on the comparison of the image previously taken in the enrollment phase versus the sample *in situ* (see Fig. 3).

In this balance between security and usability, there exists the risk of avoiding or devoting light interest to the passengers' privacy. To improve this aspect, the authors propose the use of pseudo-identity approach. This approach is a novel and plausible process and is widely proposed in the literature to preserve the privacy at biometric processes.

4. Pseudo-identity approach

A pseudo-identity (PI) does not reveal any information that would allow the recovery of the original biometric data. It is also an irreversible process with no connection with the original data. This approach is reusable and renewable, i.e. a very large number of pseudo-identities are independent and they can be generated from the same biometric measurement. This PI can be also revoked at any time.

The pseudo-identity is generated in the enrollment process. The biometric samples are processed by a feature extractor that generates a set of them. It should be noted that those features have discriminative properties.

This part is essentially the same as a conventional biometric enrollment process. Subsequently, a pseudo-identity encoder (PIE) generates the renewable biometric reference comprising a PI and auxiliary data (AD). The biometric sample and the features extracted from them can be discarded as soon as the PI and AD elements are created (see Fig. 4).

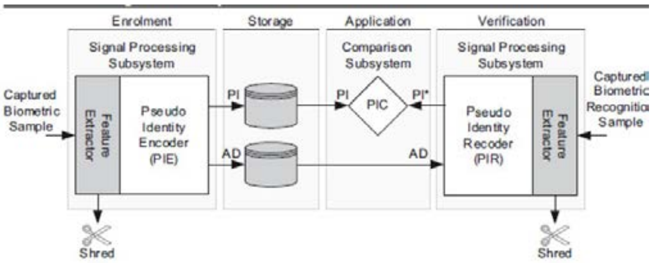
Enrolment
Storage
Application
Verification
Signal Processing Subsystem
Comparison Subsystem
Signal Processing Subsystem
Captured Biometric Sample
Feature Extractor
Pseudo Identity Encoder (PIE)
PI
AD
PI
PIC
PI*
AD
Pseudo Identity Recoder (PIR)
Feature Extractor
Captured Biometric Recognition Sample
Shred
Shred

Fig. 4. Scheme of pseudo-identity.

PI and AD elements are stored for later use (can be done independently). The storage can be implemented in a central database or in an element that can be carried by the user, e.g. card, NFC, etc. The advantage of data separation is that both, the subject (who carries the token containing AD) and the service provider (who has access to the PI), must cooperate.

During the verification process, the passenger provides a new biometric sample to a system which consists of a feature extractor and a PI re-encoder (PIR). The PIR generates a new PI* (see Fig. 4) based on the extracted features and the AD. Only if the correct AD is presented and the biometric feature is legitimate, the reconstructed PI* will match the PI. In all other cases, authentication will fail. The use of PI provides a set of features that are explained below:

1) Match-on-card. In some systems, the PI* can be combined with the pseudo-identity comparator (PIC) in a logical or physical component called a pseudo-identity verifier (PIV), which directly outputs a binary verification result.

2) Identity privacy. The storage of biometric data is one of the most serious risks of privacy loss. The union between biometric identity data and other data (bank account, credit card) may allow sensitive information to be linked.

3) Irreversibility. It is important to note that biometric data should only be used for its original purpose. Likewise, biometric data should be transformed, avoiding that the biometric information cannot be recovered. However, the biometric verification performance should not be worsened. Irreversibility must be maintained even when the biometric data are accessible from different applications, services or databases.

4) Impossibility of linkage. It is logical to think that it should not be possible to track and trace subjects. Therefore, biometric data should be impossible to link (unlinkable) between the various applications.

5) Confidentiality. This concept ensures that information is only disclosed to authorized entities. Indeed, data storage and transmission must be protected against eavesdropping, unauthorized disclosure or modification of data. Obviously, this requires cryptographic techniques such as symmetric or asymmetric encryption.

6) Data protection is not privacy by design. Data protection is the first step, but there are more. Thus, informed consent is not a magic solution. The objective must be well defined and the data to be used must be the minimum necessary. Furthermore, a criterion of

proportionality and reasonableness must be maintained. Another important point is data anonymization, which is not a trivial task.

5. Discussion

This short research work deals with two remarkable concepts in biometric area: privacy by design and pseudo-identity. Both techniques are interconnected. However, a question arises: Who watches the watchman?

Perhaps, an administrator could view a personal log and leave no trace. Likewise, it is mandatory that these logs must be secure. Elsewhere, to improve these aspects, the authors propose the use of personal data, including biometric information only with passengers' consent or, at least, providing information to passengers. The benefits aimed with these processes will increase passengers' confidence in the system. Indeed, the process will be divided into two parts. The first part consists of obtaining access to biometric data stored in the passport (with passenger consent, previously). The second part is about the information process. This process could be carried out by sending a push notification to the passenger's mobile phone.

Finally, this process suggests several questions about privacy:

1) Security or privacy infringement?
2) Who controls the rights and freedoms of individuals?
3) Is there any rule that dictates or regulates how long these images are guarded by a country?
4) Who controls the agencies or entities charged of these tasks?

[1] This work was supported by the Universidad Rey Juan Carlos, under Grants Ref.2021/00009/003 and Ref.2021/00168/001.

[2] Ehackernews, E. Hacking News. «Ryuk Ransomware Hits Spain's Employment Agency ». E Hacking News - Latest Hacker News and IT Security News (blog). https://www.ehackingnews.com/2021/03/ryuk-ransomware-hits-spainsemployment.html (Last access May 10, 2021.)

[3]«European Banking Authority Hit by Microsoft Exchange Hack». BBC News, March 8, 2021, sec. Technology. https://www.bbc.com/news/technology-56321567.

[4] Radley-Gardner, O., Beale, H., & Zimmermann, R. (Eds.). (2016). Fundamental Texts On European Private Law. Oxford: Hart Publishing. http://dx.doi.org/10.5040/9781782258674 (Last access May 6, 2021

[5] Craig, T., & Ludloff, M. E. (2011). Privacy and big data: the players, regulators, and stakeholders. " O'Reilly Media, Inc.".

[6] Cuzzocrea, A., Jiang, H., Li, K.-C., & Yang, L.T. (Eds.). (2015). Big Data: Algorithms, Analytics, and Applications (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/b18050

[7] Bowman, C., Gesher, A., Grant, J. K., Slate, D., & Lerner, E. (2015). The architecture of privacy: On engineering technologies that can deliver trustworthy safeguards. " O'Reilly Media, Inc.".

[8] Cavoukian, A. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. IDIS 3, 247–251 (2010).
https://doi.org/10.1007/s12394-010-0062-y

[9] Frontex. (2015). Best practice technical guidelines for Automated Border Control (ABC) systems.

[10] ICAO-Innovation Communication Automation Digitalization Operation, 2018, [online] Available: https://www.icao.int.

[11] Ortega-Delcampo, David, et al. "Border control morphing attack detection with a convolutional neural network de-morphing approach." IEEE Access 8 (2020): 92301-92313.

[12] Scherhag, Ulrich, et al. "Deep face representations for differential morphing attack detection." IEEE Transactions on Information Forensics and Security 15 (2020): 3625-3639.

[13] Ferrara, Matteo, Raffaele Cappelli, and Davide Maltoni. "On the feasibility of creating double-identity fingerprints." IEEE Transactions on Information Forensics and Security 12.4 (2016): 892-900.