

# SECURITY CHALLENGES FOR CYBER-IDENTITY - OUTLINE OF THE PROBLEM

M.Szyłkowska. PhD.<sup>1</sup>

Faculty of Logistics – Military University of Technology, the Republic of Poland<sup>1</sup>

Monika.szylkowska@wat.edu.pl

**Abstract:** The subject of the considerations contained in the article is the issue of cyber-identity as a subject of protection in the digital area. The considerations concern both the consequences of EU regulations in the field of personal data protection in the context of information placed by the users themselves, as well as the algorithms that are used for analysis.

**Keywords:** CYBER - IDENTITY, DIGITAL SAFETY AND SECURITY, PERSONAL DATA PROTECTION

## 1. Introduction

The identity of every human being is not only the constitutive "I" in the psychological aspect, but above all it is the basis of functioning in legal terms as a citizen, representing rights and duties. The achievements of technology have meant that now every citizen – the user has at least two types of identification: state in the "classic, material form" and in the digital form – the so-called trusted profile and a "private digital form – in the form of a profile of any, even fictitious, name" – regulated only by the regulations of the selected website.

## 2. State identity

On the basis of the Polish law Art. 4. 1. the Act of August 6, 2010 on *identity cards* defines personal ID as a document stating the identity and Polish citizenship of a person on the territory of the Republic of Poland and other European Union Member States, European Economic Area countries not belonging to the European Union and countries that do not constitute parties to the agreement on the European Economic Area [1]. The right to have an ID card is available to every citizen, but after the age of 18 it is obligatory to have it. Evasion of an adult citizen from the obligation to possess or exchange an ID card (if its validity expires) is subject to a penalty of restriction of freedom or a fine. The identity card contains data about the person: a) surname, b) name (names), c) family name, d) names of parents, e) date and place of birth, f) gender, g) face image, h) PESEL number, i) citizenship and data concerning the document itself, i.e.: series and number of the ID, date of issuance, expiration date and designation of the authority issuing the ID card [Art. 12.]. Having an identity document is the basis of the citizen's functioning in the state space – from acquiring and confirming property rights, by concluding agreements, submitting official applications, to protecting the rights and interests of every citizen in the area of public safety and order.

## 3. Trusted profile

The *state trusted profile* is a confirmed set of data that uniquely identifies its holder in the services of public entities on the Internet. Compared to the material form of the ID card, the data set contains only: name (names), surname, date of birth and PESEL number. A person using such a profile, therefore, has the so-called trusted signature for submitting applications and handling official matters of selected public institutions via the Internet. The trusted profile is secured in such a way that nobody – apart from its legitimate owner – can use it, which allows for credibility and authentication of a given person in a given public Internet service (identity confirmation). Thanks to the digital version of the "ID card", the user can, among others, sign an official application, which is

necessary to settle a specific administrative case (e.g. submit an application for an ID card, obtain copies of civil status documents, or submit an appeal against an administrative decision). Apart from purely official matters, a citizen may also use the option of appeal against a social networking decision – in the case of account blocking or deletion of a user's entry, but subject to certain conditions: 1.) submitting a complaint, which has not been considered (or a response has not been provided within 72 hours), 2.) entries were not illegal and the user did not violate the regulations of the website itself, 3.) the applicant is 18 years of age 4.) has an account on a given website and is the author of the removed entry. Currently, this procedure applies only to Facebook [2].

It is worth noting here as well the existence of the official governmental mobile application (dedicated to smartphones) called *mObywatel (mCitizen)*, which allows quick access to the so-called *mDocuments*. Identified as *mIdentity*, it currently has the ability to display its identity on the phone in an electronic version on the phone display, however only in places where it is not required to show an identity card, because it does not replace it (i.e. in the area of services such as loyalty cards, hotel services, etc.). There are also options for two types of *mCard* (school and student). In contrast to the trusted profile, *mIdentity* is only the electronic *quasi identity card* for displaying on the phone's display. In order to check the authenticity of the electronic identity card – the entrepreneur must have an application called *mWeryfikator (mVerifier)*. Regarding the security of the indicated solution, attention should be paid to two aspects: 1.) prerequisites of the application itself, which can be installed on the device in which modifications of the operating system were not made, *in particular modifications consisting in breaking the device manufacturer's security or the manufacturer of the operating system (so-called jailbreaking or rooting)* [3]; 2.) requirements of a given user's behaviour in the form of: securing login data, setting a password, PIN number and optionally (optionally – a fingerprint); 3.) the application itself by: a watermark, hologram, dynamic element (a flag) and update dates. In addition, a user using the application is assigned a cryptographic certificate confirming the authenticity of the downloaded data. With regard to the protection of data stored in a mobile device, the selected service is also encrypted (access is only possible after entering the access password). Other security measures belong to the user himself, e.g. in the form of not installing other applications of unknown origin or downloading files from an unknown source that could expose him/her to the data loss. In this respect, the limitations related to governmental applications are a positive aspect (no data about the place of residence, no possibilities to conclude an agreement, etc.).

#### 4. User profile

The *user profile* has different meanings and the same functionality – depending on both the type of system and the service. In general, it can be assumed that a digital user profile consists mainly of its user ID necessary for logging in, allowing authorized access to a given system, network, computer or the service itself (e.g. account). The ID can be both in the form of a sequence of numbers and the so-called login (username or e-mail address). Depending on the type of services, the user may be given the option of interchangeably entering the form of the ID, but for the system it will always be a series of digits (assigned automatically). The profile is always associated with a specific service and is usually associated with the user's account (e-mail account, website account, etc.). In the case of social networking sites, the *user profile* is all information contained and shared by him. These include: photos, descriptions, posts and comments. Therefore, it is a digital characteristic, which is shaped by the user himself. The scope of using the websites and services is defined in individual regulations. In the case of electronic banking services, the provisions of the Act in *electronic payment instruments* are applicable in this respect, in particular with regard to the obligation of ensuring the owner with the **security of performing operations**, with due diligence and using appropriate technical solutions [4]. When it comes to statutory obligations on the part of the user – the owner, most of all he **should not disclose information about the operation of an electronic payment instrument** made available under a contract for electronic banking services, the disclosure of which may result in ineffectiveness of mechanisms ensuring the security of outsources transactions [5]. In the case of revealing the indicated information to other persons and performing operations by using the account holder – he is responsible for the operations performed by these persons, which charges the account (individual bank account).

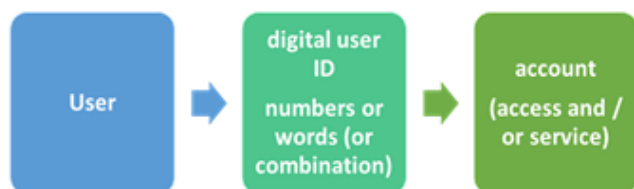


Fig.1. User account creation process

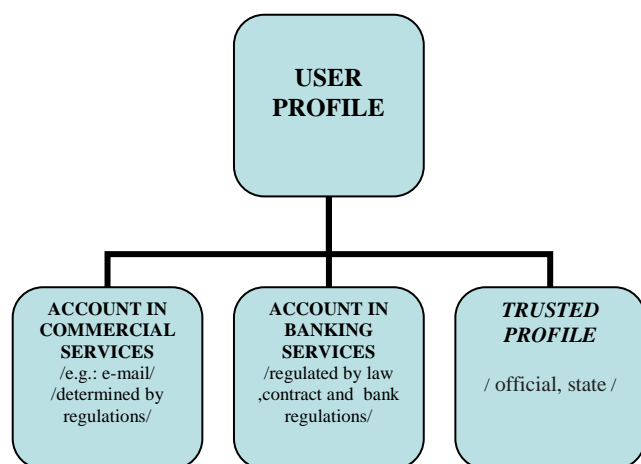


Fig. 2. Types of profiles

#### 5. Threats to profiles and accounts

From the wide range of digital threats, the most dangerous ones for commercial websites users include: gaining access to the account, and then: taking over the profile and account demanding the cyber-ransom for handing it back to the owner, taking over and using the account/profile to commit other crimes (e.g. persuading to violence on social networks, ransom demand, sending offensive content, discrediting).

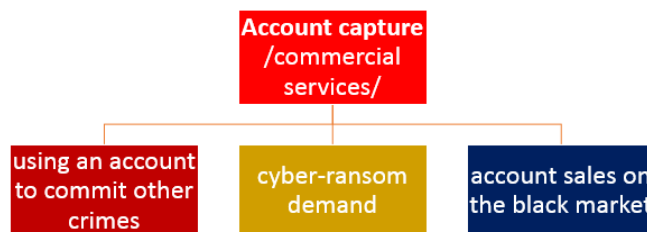


Fig. 3. Account capture effects

In turn, the Internet banking accounts' users will also include – in addition to the risk of data interception and ransom demand – also the option of making purchases at the expense of the user of the intercepted account. For a trusted profile, these will be, in addition: the possibility of submitting official applications (e.g. issuing a duplicate ID card to a different address than the address of the rightful owner).

#### 6. Personal data

The user account and his profile will not always fully meet the definition of personal data within the meaning of the regulations in force in the European Union, because pursuant to Art. 4 (point 1) of the Regulation of the European Parliament and the Council (EU) 2016/679 of April 27, 2016 *on the protection of individuals with regard to the processing of personal data and on the free flow of such data and the repeal of the 95/46/EC directive* (general data protection regulation) Official Journal of the European Union L 119/1 – “personal data” means information on the identification or identifiable individual, (...) to whom the data relates”. An identifiable person is a person who can be directly or indirectly identified (...) based on information that will identify it, in particular on the basis of an ID, such as the name and surname, ID number, location data, Internet ID or one or several specific IDs determining the physical, physiological, genetic, mental, economic, cultural or social identity of an individual” [6]. Considering the possibilities of commercial services in the scope of having an account, which does not have to be marked with real user data, indicated, indirect markers (e.g. location) may be of key importance. The ability to use an account with fictitious data created an exception: identifying a specific individual in this case will be misleading – unless other factors indicate it. It is worth considering a situation in which the user, wanting to deliberately obscure the real identity – uses fictitious data, which, however, identify a specific individual by, e.g., making purchases using a payment card or an electronic wallet. In accordance with the aforementioned regulation and Polish regulations regarding the protection of personal data: *Information is not considered to enable identifying a person if it would require excessive costs, time or actions* [7]. Such a provision allows for a fairly wide interpretation depending on “the justified probability, but ignorance of the algorithms used to filter user information should not prejudice the lack of qualifications for protection.

## 7. Profiling users

The so-called user profiling by algorithms created for this purpose differs from the previously indicated profile creation by users themselves. They are most often used to create contextual ads, prepared for specific user preferences.

The CM/Rec (2010) recommendation 13 of the Committee of Ministers of the Member States on the protection of persons *in relation with automatic processing of personal data during the creation of profiles* in chapter 1 defines: "Profile" – as a data set characterizing the category of persons to be applied to a given person. In turn: "Creating profiles" means automatic data processing technique consisting in assigning a given person a "profile" in order to make decisions about it or analyse or predict its preferences, behaviours and attitudes [8]. Algorithms of most digital services companies (including entertainment) are based on many, seemingly independent indicators, collecting "bits of digital traces" from the actions of each user individually. These include both "likes" of specific content and models based on analysing text information (content). The fact of performing analyses based on face photography should also not be surprising. The Convention no. 108 itself of the Council of Europe *on the protection of individuals with regard to the automatic processing of personal data* [9] does not contain the definitions set out above. It also deals with general issues, such as: collecting personal data for specific and justified purposes, prohibiting the use of such data in a manner inconsistent with these goals, and: appropriate, factual, not exceeding the needs arising from the purposes for which they are collected [10]. However, it would be reasonable to conduct a thorough analysis, or "Advanced analytics" as part of *cookies* used to analyse and identify the behaviour of website users, among others, monitoring the IP address of the device used by the user to be able to identify it, and then combining such data with personal data provided earlier – do not go far beyond the "specified purpose", if the main one is, e.g., to transmit information in the form of newspaper articles. Is it equally legitimate to allow websites to place third-party *cookies* – of advertising partners that are most often used strictly to build interest profiles in order to match advertising types on other websites (sic!) Although they theoretically do not contain personal data, they identify the user's browser and the device itself. Thus, the user's influence and capabilities are limited only to the acceptance of being notified about the use of *cookies* by a given website and possible changes made to the advanced settings that require additional action on the part of the user. Creating such legal "gates" should not take place due to the type and amount of data that is transferred, and then they are used primarily for specific profits for third parties, unrelated to the purpose or content of the website visited by the user.

### Profiling vs sharing information by users

Considering the indicated issues, it is impossible not to pay particular attention to the issue of the amount of information placed by the users themselves – in every form. In 2012, it was estimated that each user generated about 500 MB of data a day (sic!), and in 2015 this figure is expected to oscillate around 65 GB. However, most often users do not pay attention to security or privacy – at least when posting their photos.

### Algorithms in the security service

The indicated mechanisms do not only serve to predict preferences in the marketing area. They have been used for a long time in areas of public safety and order. The so-called safety gates at airports can

serve as an example, which, taking pictures of all passengers, are able to signal an employee that a particular person is showing nervousness or tension beyond the accepted standard or defined range.

## 8. Conclusion

There is no doubt that currently the majority of citizens – users operate in two realities: *real* and *virtual* – and in each of them they have their own identity. In the case of official services – both commercial and strictly state-related – these identities constitute *one* [homogenous] in two dimensions and their corresponding forms ("material" proof and digital ID). In the case of strictly private sphere and commercial services, the user can adopt a fictitious, virtual quasi-identity, which he will use, for example, in his activity on forums or social websites – remaining relatively *anonymous* until he goes beyond the limits of the law with his behaviour, which could result in the identification by the law enforcement agencies (IP address, device address, etc.), and then responsibility under the *correct [real]* identity. Undoubtedly, EU regulations in the field of personal data protection constitute a significant step in this area – in particular security principles and procedures, but the remaining issue is the broad meaning of cyber-identity that is owned by every "virtual" user – even if, theoretically, it is anonymous (in the sense: not defined by name and surname). It would be appropriate to prohibit the collection of information in the form of *cookies* and user profiling using mechanisms that categorize their interest, including the selection of information about the location and devices used (including the type of operating systems). Only then would there be a complete regulation regarding the protection of user identification data. Data that is private in the most basic and important issue for everyone. However, it is worth bearing in mind that users themselves are often not aware of the threats and algorithms by which they are analysed and evaluated. Therefore, if legislators want to protect their citizens seriously and comprehensively, the proposed provision should be complementary to the existing gap. Otherwise, the American saying will be binding and unchangeable: "if you do not pay for the service (digital – assumed by the author), it means that you are a product".

Taking into account the current possibilities of algorithms – it is also possible that in the very near future it will be possible to "design" and "code" specific user behaviour, where the strictly *purchasing preferences* will be at the end of the list. From the above-indicated reasons for the protection of cyber-identity, its owner is and will be the most important and critical element.

## 8. References

- [1] Source: <http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20101671131/U/D20101131Lj.pdf>
  - [2] Source: <https://obywatel.gov.pl>
  - [3] Source: <http://mc.bip.gov.pl/publiczna-aplikacja-mobilna/informacje-o-publicznej-aplikacji-mobilnej.html>
  - [4,5] Act of September 12, 2002 *on electronic payment instruments* (Journal of Laws of 2002, No. 169, item 1385, as amended).
  - [6] Regulation of the European Parliament and the Council (EU) 2016/679 of April 27, 2018 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the 95/46/EC Directive* (general regulation on data protection) Official Journal of the European Union L 119/1.
- Source: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32016R0679>

[7] Act of May 10, 2018 *on the protection of personal data* [Journal of Laws of 2018, item 1000, 1669].

Source:<http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf>

[8] Recommendation CM/Rec (2010) 13 of the Committee of Ministers of the Member States *on the protection of persons in relation to the automatic processing of personal data when creating profiles*/ Source: <https://uodo.gov.pl/pl/file/1425>

[9-10] Convention No. 108 of the Council of Europe on the protection of persons with regard to the automatic processing of personal data, prepared in Strasbourg on January 28, 1981 [Journal of Laws of 2003, no. 3, item 25. Source: <http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20030030025>

[11] European Commission Justice and Consumers, <https://ec.europa.eu/newsroom/article29/news-overview.cfm>

[12] European Data Protection Supervisor *2017 Annual Report - Data Protection and Privacy in 2018: going beyond the GDPR* [https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2017-annual-report-data-protection-and-privacy\\_en](https://edps.europa.eu/data-protection/our-work/publications/annual-reports/2017-annual-report-data-protection-and-privacy_en)