Data Protection, Digital Forensics and Encryption in Mobile Devices in European Union

DATA PROTECTION, DIGITAL FORENSICS AND ENCRYPTION IN MOBILE DEVICES IN EUROPEAN UNION

Federico Costantini / Marco Alvise De Stefani

Researcher, University of Udine, Department of Law
Via Treppo 18, 33100, Udine, IT
federico.costantini@uniud.it; https://people.uniud.it/page/federico.costantini

CEO, Synaptic Srls
Via Gemona 52, 33100 Udine, IT
destefani@synaptic.it; www.synaptic.it

Keywords: ***Digital Forensics, Encryption, Fingerprints, Data protection, Mobile devices, GDPR, Human rights, Privacy***

Abstract: *Nowadays cryptography has been used to increase trust in confidentiality of many sources of information. Indeed, such technologies are helpful in protecting data from illegal accesses, yet drawbacks arise if they have to be enforced by investigative authorities to collect evidence. Balancing investigative powers and fundamental rights – most importantly, privacy – is difficult, especially when decryption keys are provided by human fingerprints or other biological traits. In this paper we focus on Digital forensics of encrypted mobile devices in the EU legal framework.*

1. Introduction

«*The genie of guerrilla cryptography is out of the bottle. No one, not even its maker, can stuff it back in or keep it within what America laughably calls its borders. The genie is all over the Net. It's in your hands as you hold this book. Summon it with a conscience. But be prepared to summon it if you must*».[1] This quote from a comment by John Perry Barlow to the «Crypto-Wars» – the unofficial name originally given to the dispute between Phil Zimmermann and the U.S. federal government concerning the export of the PGP (Pretty Good Privacy) encryption software[2] – is more than twenty years old, and still affects our future as a technological prophecy.

In history of human communication, as far as we know, cryptography has always been crucial in maintaining confidentiality on certain public or private matters.[3] Recently, the development of computer science has enabled more complex methods – cryptographic systems – requiring the use of increasingly sophisticated devices (mechanical, electrical, electronic, quantum-theory based) to communicate hidden messages. Currently cryptographic technologies are used in several fields and with different purposes: to protect confidentiality

1 Barlow 1995, (p. xiii).

2 https://en.wikipedia.org/wiki/Crypto_Wars (all websites last visited in January 2018). In 1976 the U.S. government issued the AECA (Arms Export Control Act) – in Title II of Pub. L. 94-329, 90 Stat. 729, enacted June 30, 1976, now in Title 22 USC § 2778 and § 2794 (7) – which provides a very strict regime for arms exports contained in the ITAR (International Traffic in Arms Regulations), in Title 22 CFR, Title 22, Chapter I, Subchapter M, Parts 120–130. Within ITAR the USML (United States Munitions List) – Title 22 CFR, Title 22, Chapter I, Subchapter M, Part 121.1 – contains a very detailed list of goods whose export required permission from the Department of State. The AECA included cryptographic systems in the USML, thereby establishing that the export of cryptographic systems would be severely punished as «contraband of war». Indeed, Phil Zimmermann was indicted of such federal crime.

3 Ancient Greeks used the scytale and Romans the «Cesar Code», cfr. https://en.wikipedia.org/wiki/Scytale, https://en.wikipedia.org/wiki/Caesar_cipher.

of data stored in hard drives (i.e. encrypted volumes) or available through online services (i.e. cloud computing), to secure transmissions from tampering and eavesdropping (i.e. SSL) to defend data streams in open networks (i.e. copyrighted broadcast) to authenticate the owner of given resources and thus to assign responsibility for their content (i.e. digital signatures), to allow anonymity in trusted transactions (i.e. blockchain cryptocurrencies).[4]

Today cryptography is commonly combined with biometric technologies. Since mobile devices equipped with such functionalities – once laptops, then tablets and now smartphones – have been spreading worldwide in the last few years, the massive storage of fingerprints – and other biometrical features – of millions users has arisen great concerns for the protection of their personal data.

As recently shown in the «FBI-Apple case»,[5] the scene is overcrowded by several actors, each pretending to be the main character: investigative authorities require backdoors to access data transmissions, clouds and personal devices on the grounds of the public security; private and business users demand protection in their privacy as a safeguard for freedom of expression; companies – hardware manufacturers and internet providers – raise «plausible deniability»[6] as a marketing leverage while claiming openness of technical standards and protocols against competitors.

In European Union the ongoing discussion is currently evaluating different options and the debate is more difficult since the legal framework is rapidly changing. On one hand, the «Budapest Convention» of 2001[7] has gathered consensus among EU member States, nurturing the growth of a «digital forensics» community where standards and best practices in «electronic evidence» are being constantly deployed and implemented.[8] Furthermore, the «European Investigation Order» – provided by the Directive 2014/41/EU entered into force on 22th of May 2017[9] – created a common instrument for obtaining evidence and thus sharing «criminal intelligence» from agencies of all Member States. On the other, encryption is encouraged by the EU General Data Protection Regulation (GDPR)[10] – specifically, in whereas 83 – and considered among the appropriate measures of data security by Article 6 Par. 4 (e) and Article 32 Par. 1 (a).[11]

In this paper we intend to provide an overview – from an interdisciplinary perspective – of the theoretical and practical issue raising within European Union legal framework in enforcing access in a encrypted mobile devices protected by biometric cryptographic keys. Our contribution is divided into sections as follows: (1) we draw a brief premise on cryptography in order to enlighten the relevance of the topic; (2) we provide some observations on the legal framework in the European Union and the most relevant decisions of the

4 Precisely, a message can be entrusted by encryption under different aspects: confidentiality, authentication, non-repudiation, time-date stamping.

5 On 2 December 2015 Syed Rizwan Farook and Tashfeen Malik killed 14 people and injured 22 others in a suicidal attack to the Inland Regional Center in San Bernardino, California. Investigators, trying to access in Farook's iPhone 5C, subpoenaed Apple to provide the keys to unlock the device. to overcome the refusal of the manufacturer, FBI obtained the access hiring an israeli software company – paying an estimated amount of 1,2 million dollars – and then withdrew the action against Apple.

6 «Deniable Encryption» is properly named the attempt to hide the encryption in itself in order to protect the resources contained in the device. Different schemes have been classified depending by the subject protected (sender-deniable or receiver-deniable) or the assumption of a prior communication of the keys (shared-key or public-key) cfr. Canetti/Dwork/Naor/Ostrovsky 1997, p. 90–104, (p. 92).

7 Council of Europe Convention on Cybercrime (ETS No.185) of 23 November 2001.

8 www.evidenceproject.eu/.

9 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, in OJ L 130/1 of 1 May 2014.

10 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, in OJ L 119/1 of 4 May 2016.

11 According to Article 34 Par. 3 (a), in case of data breach, data controllers don't need to notify the event to data subjects if the personal data affected are rendered unintelligible by the application of encryption. This provision has a practical relevance since it gives companies the opportunity to avoid damages to their business reputation among clients in case of incidents.

European Court of Human Rights; (3) we analyse the technical issues concerning encryption in mobile devices showing some advantages and disadvantages of the different available options and we highlight some problems concerning the use of the fingerprint as encryption authentication. At the end, we offer a synthesis of our findings and draw some paths for future research.

We argue that is emerging a trend in the EU approach. Indeed, we are facing a shift of paradigm from the – maybe ingenuous – ideal of «transparency» aimed by the Convention of Budapest of 2001, to a kind of pragmatic «strategic control» of cryptography depicted in the most recent initiatives. We believe that such change of approach is paving the path of a deeper understanding of the challenges posed by encryption, yet a lot has still to be done.

2. Cryptography and its complexity

It is known that human interactions can be modelled in terms of transmission of information. In each communication, indeed, among others components[12] we can identify the «code», which could be defined as the system of rules – shared by the transmitter and the receiver – governing the process of encoding and decoding a message. Cryptography is a tool for the communication of a hidden message (called «ciphertext») in an ordinary transmission (called «plaintext»). In it, the «cipher» is the key that enables the processes of encryption and decryption.[13] Hence, in order to give the proper meaning to an encrypted message – a sort of «double coded» communication – the receiver has to be entitled not only with the «code», but also with a decryption key.

This phenomenon can be seen under three perspectives: (1) theoretical; (2) practical; (3) empirical.

From a theoretical perspective, there are two kinds of cryptography: in the «symmetric» one – the oldest – the processes of encryption and decryption depend by the same key, while in the «asymmetric» one – which has been invented in 1976[14] – the credentials are different and completely independent. The latter technologies have been deployed further, having become the theoretical basis of the distinction between «private» and «public» key[15] which is today the most common cryptographic technology (i.e. digital signatures).[16]

From a practical point of view, in cryptography we can identify two main levels of complexity: (1) the one concerning the resources that are encrypted and decrypted; (2) the one regarding the keys and their handling by their owner. We will call the first «resources-level» and the second «key-level». Each one is afflicted by specific issues which are briefly noted in the following paragraphs.

Considering the «resources-level», it can be said that encrypting *plaintext* and decrypting *ciphertext* respectively extends or tightens the domain of available data, which can't be processed without the keys enabling access. Since the ownership of the key is the only condition to access the information stored in encrypted archives, we can argue that this level pertains to the control of the «access».

As regards the second level, every key holder should be aware that, in order to avoid unauthorized accesses, security measures have to protect the keys as such. Remarkably, this happens regardless of the content of the resources, so it can be said that this level refers to the control of the «use» of the keys.

---

12 Components are: message, information source, transmitter, signal, channel, receiver, destination, noise source, Shannon, 1948(a), p. 379–423, Shannon, 1948(b), p. 623–656.

13 Norman, 1973. More recently, cfr. Horn/Ogger, 2003, p. 58–85.

14 Diffie/Hellman, 1976, p. 109–112.

15 Usually the «private» key is used to sign a message (as a guarantee of ownership) by the transmitter, while the «public» key is required to verify such credentials. Alternatively, the transmitter can use the «public» key of the receiver to secure the message from third parties, and the receiver can use its «private» key to access to its content.

16 Depending on the technology deployed it is possible to distinguish between «strong» (i.e. AES algorithm) and «weak» encryption (i.e. DES algorithm). These definitions depend, of course, on the state-of-the art computing technologies.

From an empirical perspective, we need to add a third level of complexity to the two previously mentioned. In common everyday life, indeed, users aren't dealing directly with keys, but with PINs (personal identification numbers) or passwords. Such text combinations – easier to remember by customers – are translated by algorithms in cipher keys, which are managed by the software interface to encrypt the resources.[17] Although passwords share the same issues of cypher keys – if the keys are lost, stolen or forgotten, the resources are unavailable as they were erased – we can argue that the nature of the information provided by them is different from the cypher keys, since they concern the user as an individual, not the resources. For such reason we can name this level as «user-level».

To sum up, we can say that, for common users, cryptography works on three layers – «resources-level», «key-level», «user-level» – each pertaining to a specific object and to the control of a different set of data. According to the taxonomy recently adopted by the «Philosophy of Information»,[18] we can qualify the «resources-level» as «information *as* reality», the «key-level» as «information *for* reality» and the «user-level» as «information *about* reality». This distinction will be useful to draw the final remarks.

3. Legal framework on cryptography: international law and public order

Legal issues concerning cryptography are quite more complicated than usually thought even by experts. It is convenient to discuss first the international-diplomatic aspects – and then focus on the legal and political profiles.

From the perspective of the international law, it seems appropriate to observe that «Crypto-Wars» aren't ended with the «PGP case».[19] Indeed, cryptographic technologies are included in the «control list» established by the Wassenaar Arrangement, which is an international treaty aimed at controlling the proliferation of «dual-use» technologies.[20] It is noteworthy that many EU Member States are also parts of such treaty, yet not the European Union as such, hence at EU level cryptography is not qualified as a weapon.[21] Furthermore, we have to mention that OECD provided a few guidelines on cryptography policy, recommending to recognize the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only, suggesting that «*a cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key*».[22]

---

17 A «Key Derivation Function» is a mathematical algorithm used to convert a password into a cryptographic key.

18 According to cybernetics, «information» can undertake three different ontological statuses: (1) technical, (2) semantic, (3) influential, Weaver, 1949, p. 11–15. Such classification has evolved in a more abstract taxonomy: «information *as* reality» (technological information), for example, the electrical signal, which is transmitted regardless of the message contained; «information *about* reality» (natural information), such as the information about natural phenomena, which can be true or false (alethic); «information *for* reality» (cultural information), which conveys instructions or algorithms to one or many recipients, Borgmann, 1999. The same distinction has been accepted by the most contemporary theoretical perspective, named «Philosophy of Information», Floridi, 2011, p. 30. Ultimately, such vision has been endorsed by the European Union, Floridi, 2015.

19 From a historical-political perspective, cfr., Schulze, 2017, p. 54–62. For an overview from a legal-international perspective, Sundt, 2010, p. 2–7.

20 Cryptography is included in §. 5. A. Part 2. Systems, Equipment and Components, Cryptographic «Information Security». The «control list» has been amended very recently in the twenty-third WA Plenary meeting held in Vienna on 6–7 December 2017.

21 At EU level there are two similar but distinct definitions of weapons. According to Directive 2008/51/EC and Regulation (EU) No 258/2012, a «firearm» is «*any portable weapon that expels, is designed to expel or may be converted to expel shot, bullet or projectile by the action of a combustible propellant*». This definition does not cover military weapons. Following Council Joint Action of 12 July 2002 on the European Union's contribution to combatting the destabilising accumulation and spread of small arms and light weapons and repealing Joint Action (1999/34/CFSP), military weapons are included under the name «small arms and light weapons» (SALW) which is generally used in United Nations *fora* and in the field of the EU's Common Foreign and Security Policy.

22 Cfr. §. 6. Lawful Access, OECD Recommendation Concerning Guidelines for Cryptography Policy adopted on 27 March 1997. In this OECD Recommendation, cryptography is defined as «*a discipline that embodies principles, means, and methods for the trans-*

The conflict between States and citizens (in particular, investigative authorities and private individuals), or among individuals (specifically, between companies and customers) are the most discussed legal issues of cryptography and raised the attention of public opinion since the before-mentioned «Apple/FBI case».[23] Furthermore, they became urgent since 2014, when Facebook, Google and Apple – world's biggest Internet providers and electronic devices manufacturers – implemented encryption by default in their services and products.[24] When the owner of the encrypted resources cannot – i.e. being dead, as in the «Apple/FBI case», for example – or is not willing – i.e. being accused of criminal offenses – to provide the encryption key to public authorities, are available remedies with low degrees of efficiency and efficacy.[25] A recent interesting contribution identifies six different «encryption workarounds»:[26] (1) find the existing copy of the key,[27] (2) guess the key,[28] (3) compel the key, (4) exploit a flaw in the encryption software,[29] (5) access plaintext while the device is in use,[30] (6) locate another plaintext copy.

In our opinion the third case is the most interesting because, of course, in it we can find the ultimate conflict on the control of the keys between public powers and fundamental rights. We intend to deepen briefly such topic comparing U.S. and European perspectives.

Concerning the U.S.A., as an immediate aftermath of Apple, Facebook and Google encryption initiatives of 2014, a very lively debate arose, encrypted resources being protected under the privilege against self-incrimination provided by the Fifth Amendment to the United States Constitution.[31] According to its current interpretation, a statement involving an individual requires three elements in order to be granted by such privilege: (1) has to be compelled by the government; (2) has to be incriminating; (3) has to be testimonial, or in other words it has to be a certain kind of communicating act. Of course, since revealing a password consists in a «communication», investigative authorities were concerned of «going dark», becoming impossible to grant a lawful access to encrypted resources without the consent of their owner.[32] Although, jurispru-

formation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use».

23 Encryption is included among Fundamental Rights, being considered under the Freedom of opinion and expression, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40: «*§.89. Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys*».

24 Apple released a new operating system, iOS8, which encrypted most data stored on iPhones, likewise Google upgraded Android Lollipop 5.0 with similar features and Facebook brought encryption to its newly acquired messaging service Whatsapp. For example, Apple's Whitepaper stated as follows: «*For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess*». In iOS8 the encryption key is generated combining user's password and the UID (Unique Identification Number) of the device, so the key is not stored in the device.

25 Some encryptions systems are provided with precaution functionalities – key-escrow, trusted third-party access, exceptional access, data recovery – though they are not widely accepted because they are considered security flaws. Among the proposers of a «third party» controlled access we can find those who favour a public institution and those who prefer a private independent entity. Such preferences are conditioned by several factors, Potoglou/Dunkerley/Patil/Robinson, 2017, p. 811–825.

26 Kerr/Schneier, 2017.

27 Indeed, passwords can be archived in a document available outside the encrypted resources, ibid..

28 It was estimated that 15% of the iPhones are protected by 10 combinations of numbers on over 10.000 possible. Among them, 4% is protected by «1234», in Amitay, 2011.

29 This was the case of the «Apple / FBI» controversy.

30 The arrest of Ross Ulbricht, the famous Silk Road founder, was specifically planned in a way that could allow prosecutors to access the laptop while it was working.

31 «*No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation*».

32 https://cyber.harvard.edu/pubrelease/dont-panic/. Berkman Center for Internet & Society at Harvard University, 2016.

dence found a conceptual difference between a statement revealing the password of incriminating encrypted resources (granted by the Fifth Amendment) and a statement referring to an external source with incriminating contents (not granted by the privilege).[33]

With regard to Europe, it is known that in many European countries – being part of the Council of Europe – can be applied Article 19 Par. 4 of the «Budapest Convention» of 2001[34] but also Article 6 Par. 2 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECtHR) of 1950.[35] We can simplify the discussion of this topic observing that the decisions of the ECtHR draw a distinction similar to the one provided by U.S. Courts. We can stress out that it is still debated if the statement revealing other sources of incriminating evidences (i.e. documents) is granted by the privilege against self-incrimination and the right to remain silent descending from Article 6 paragraph 2 of the European Convention of Human Rights.[36]

It can be said that the «Crypto-Wars» definitely left the global diplomacy and made their way in U.S. and European courts. In the EU, concerns were raised in an institutional report of 2015, where cryptography was qualified as an obstacle not only in accessing physical devices, but also to communication interceptions and inspection of cloud-stored data. As a recommendation, it was suggested by experts to Member States representatives to «*assist in developing standardised requirements for service providers to make unencrypted communications data available to law enforcement*».[37]

As observed in the European Parliament Resolution against Cybercrime of 3 October 2017, cryptography can be used both in confidential communications and in ransomware attacks (whereas «C»)[38]. In the same document, European Commission stresses that strong cryptography improves the overall security of communication yet allowing «malicious users» to conceal their unlawful activities (§. 7)[39] – since encryption can help fulfil the need of protect communications from cyber crimes (§.17) – and encourages providers to promote «practical security measures» – such as encryption, indeed – among citizens in order to spread the use

33 Privilege against self incrimination was granted in a case where the government asked the defendant to disclose not the password but to produce an unencrypted version of the hard drive, provided that officials managed to access the incriminating content before defendant's laptop were shut down, *In re Grand Jury Subpoena to Sebastien Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb 19, 2009). In a following case, the same privilege was granted to the defendant on the basis that the hard drive containing incriminating evidence was partially examined by the prosecutors during investigations, *In re: Grand Jury Subpoena Duces Tecum*, 25 March 2011, Nos. 11–12268 & 11–15421 D.C. Docket No. 3:11–mc–00041–MCR–CJK, decided 23 February 2012. Electronic Frontier Foundation filed an amicus brief in support of the defendant. In another leading case, a third party – the ex-husband – brought to prosecutors a list of known password used by the defendant and one of them worked giving access to the encrypted resources, *United States v. Fricosu*, 841 F.Supp.2d (United States District Court for the District of Colorado 2012).

34 «*Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2*».

35 «*Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law*»,

36 Cfr. *Funke V. France* (Application no. 10828/84) ECLI:CE:ECHR:1993:0225JUD001082884, *Saunders V. United Kingdom* (Application no. 19187/91) ECLI:CE:ECHR:1996:1217JUD001918791.

37 Di Nicola/Gounev/Levi/Rubin/Vettori (Eds.), 2015, p. 265. Chapter 9 of the Report is devoted to the Italian mob, considered as a case study.

38 Such kind of attacks recently outnumbered traditional malware threats, cfr. EUROPOL, Internet IOCTA 2016 Crime Threat Assessment, 2016.

39 European institutions focused three priorities – organized crime, terrorism, cybercrime – fostering a coordinate response to internal and external threats, COM(2015) 185 final, of 28 April 2015, *The European Agenda on Security*. Terrorism became a key issue after the 9/11, as confirmed by institutional documents such as COM(2004) 698 final, of 20 October 2004, on Prevention, preparedness and response to terrorist attacks. A great effort was given to raise the level of security in detonators, bomb-making equipment and fire-arms, including their components, since the initiative endorsed by the European Council of November 2004, cfr. The Hague Programme, in OJ C 53/1 of 3 March 2005. Recently the EU become member of the European Council Convention on the Prevention of Terrorism (CETS n. 196), cfr. COM(2017) 606 final and COM(2017) 607 final, of 18. October 2017.

of privacy-enhancing technologies (§. 30). Meanwhile, States Members are urged not to impose obligations to encryption providers – such the creation of «backdoors» – and calls to cooperation among them (§. 51).[40]

4. Encryption, biometrics and data protection in mobile devices

As we know, information technologies that use human – physical (i.e. fingerprints) or behavioural (i.e. voice recognition) – characteristics to identify individuals are called «biometrics».[41] Nowadays, such techniques are commonly used to verify a person's identity when accessing to resources or devices.[42]

From a legal perspective, there is a tremendous difference between a password and a biometric key in encrypting a resource. In U.S legal system, where the first cases appeared, from the beginning it was quite obvious that providing the biological trait needed to access a device does not involve any kind of «communicative act», so no «testimony» is required: here the Fifth Amendment cannot entitle to legitimate refusals against prosecutors» access requests.

According to the jurisprudence of the ECtHR, collecting biometric data in order to identify individuals allows other usages of the information stored.[43] In EU, traditionally the collection of biometric data – fingerprints, in particular – has always been considered a very sensible issue. Still today such data are collected by public institutions in very limited cases and with very specific purposes.[44] Above all, as suggested by OECD guidelines, biometric data are shared to identify individuals by investigative authorities.[45]

---

40 Cryptography has been specifically discussed in the Strategic seminar «Keys to Cyberspace» organized in The Hague on 2 June 2016 by the Netherlands presidency of EU and Eurojust. Cfr. also the document Encryption: Challenges for criminal justice in relation to the use of encryption – future steps – progress report, Brussels, 23 November 2016. Cfr. finally Gutheil/Liger/Heetman/Eager/Crawford, 2017, p. 18. Encryption is discussed as an «investigative barrier».

41 According to Article 4 (14) GDPR, «biometric data» are «*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*». Cfr. an introduction in Prins, 1998, p. 159–165. Biometric technologies work in a two-phases process: in the «enrolment», the body feature is acquired, measured, processed by an algorithm and converted in data which are stored; in the second phase takes place the verification in which the pattern is confronted with the template.

42 In other words, they are recognition technologies for authentication, authorization, security. It is known that there are three kinds of automated verification of a person's identity: «*Something I know*» (i.e. password), «*Something I have*» (i.e. physical token), «*Something I am*» (i.e. biological trait). More precisely, «identification» is establishing who a person is while is accessing a resource, «verification», instead, is establishing if a person is the same who is expected to access, cfr. a seminal contribution Grijpink, 2001, p. 154–160. Not all biological traits are suitable to be collected in a biometric system, but only those who fulfil certain requirements such as universality, distinctiveness, permanence, collectability. Furthermore, there are some practical issues that a biometric system has to guarantee, such as performance (speed and accuracy), acceptability by people, circumvention (resistance against fraudulent methods), Jain/Ross/Prabhakar, 2004, p. 4–20.

43 As decided by the ECtHR, «*Article 4(3) of Regulation No 2252/2004, as amended by Regulation No 444/2009, must be interpreted as meaning that it does not require the Member States to guarantee, in their legislation, that biometric data collected and stored in accordance with that regulation will not be collected, processed and used for purposes other than the issue of the passport or travel document, since that is not a matter which falls within the scope of that regulation*», *W.P. Willems and others c. Burgermeester van Nuth and others*, C-446-449/12 (interpretation), fourth Chamber, decision of 16 April 2015, ECLI:EU:C:2015:238.

44 It is noteworthy that, according to Articles 14 and 15 of Council Decision of 28 February 2002, setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63/1 of 6 March 2002) as amended by Council Decision 2003/659/JHA of 18 June 2003 (OJ L 245/44 of 2 June 2003) and Council Decision 2009/426/JHA of 16 December 2008 (OJ L 138/14 of 4 June 2009, p. 14), Eurojust is entitled to process personal data in very limited cases and with very strict purposes. Only for suspected or previous criminal offenders it is allowed to process «*DNA profiles established from the non-coding part of DNA, photographs and fingerprints*» (Article 15, §. 1, lett. n). cfr. Communication from the Commission to the European Parliament, the European Council and the Council on Twelfth progress report towards an effective and genuine Security Union, COM(2017) 779 final, of 12 December 2017.

45 On such matter, cfr. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119/89 of 4 May 2016). On the impact of the Directive 680/2016

From a technical perspective, we have to acknowledge that, when using a biometric key to encrypt data, we face two important elements[46].

First, the biometric key is (usually) very strong and unique, but is also not changeable. We have only one set of fingerprints, one face, etc., and if these keys leak to public domain or black market due to a data breach, we cannot change them as we can do with our passwords when they are compromised. Moreover, these biometric keys aren't stored in our mind, like passwords, and can be stolen even without our knowledge[47].

Such uniqueness of biometric keys leads to the second important element: how are these keys stored in the devices? Not only encrypted data are valuable: due to their uniqueness, the biometric keys themselves are very important and their protection is critical. Security researchers have found that many devices store user's fingerprints without proper protection[48].

And even if some devices store biometric keys in the proper way (for example hashed and with restricted access), other devices are £black box£ (they can't be examined) and users has to trust the companies who produce them: are can we be sure that those companies don't store the biometric keys of the customers in their servers?[49]

5. Conclusion

As we know, information technology is the core of our society. Cryptographic systems are the most advanced form of control of information and this is the reason of its strategic importance not only in public affairs but also in private matters: they are not only technological tools, but «weapons», according to International law. Provided that, maybe the EU should review its approach, which by now is restricted in a pragmatic perspective. Indeed, information can be shared among peers, of course, but cannot be owned by anyone, hence information security, even if granted by encryption, is based on risk-management evaluations.

Not always the deployment of cutting-edge technologies is, as such, the most secure solution. Biometric recognition systems represent intrinsic risks – and sometimes serious threats – both from a legal and a technological point of view. Indeed, very often biometric keys award public authorities and service providers with data – our biological traits – far more valuable than the resources they are meant to protect.

In previous paragraphs, according to the approach provided by «Philosophy of Information» we detected three layers in encryption: «resource-level» (the encrypted data to be accessed), «key-level» (the cypher keys to be handled) and «user-level» (the individual traits used as biometric keys). It can be said that «Crypto-Wars» are being conducted at each level, yet with different technologies, tools and arguments.

We claim that keeping separated such levels would be useful in order to clarify the debate on cryptography and to bring new arguments on the discussion. Cryptography, indeed, is neither just an asylum for terrorists, mobsters and paedophiles, as prosecutors tend to depict it, nor solely a marketing leverage for customers willing to pay for extra-services, as providers often advertise it. For example, it could be said that the Fifth Amendment and Article 6 ECHR operate on the second layer («key-level»), because they both pertain to «information *for* reality» provided by communicating acts. On the contrary, they don't apply to the first layer

and Regulation (EU) 679/2016 on European judicial institutions, cfr. Marquenie, 2017, p. 324–340. For a background overview, it may be helpful our previous contribute on the topic, cfr. Costantini/De Stefani, 2017, p. 461–468.

46 Biometric keys examples are fingerprints, face recognition, retina scan, iris scan, hand geometry, voice analysis, signature, DNA analysis, etc.

47 For example, in different cases researchers and hackers were able to counterfeit fingerprints from standard photos taken at events or from social networks. People can also be forced to use their biometric keys, for example using the fingerprints of a sleeping person, or coerced by criminals or totalitarian regimes.

48 For example, some devices saved fingerprints scan as plaintext bitmap images, readable by unprivileged processes or apps.

49 This lead to an interesting argument: it's common opinion that Governments shouldn't have access to backdoors or secretly analyse their data, but people trust private companies and freely give them personal data and business info.

(«resource-level») nor on the third («user-level»), because they don't refer neither to «information *as* reality» nor to «information *about* reality».

We believe that this conceptual framework could be fruitful in developing a different approach to legal issues in cryptography and we intend to proceed along this research path.

6. References

Amitay, Daniel, Most Common iPhone Passcodes. http://danielamitay.com/blog/2011/6/13/most-common-iphonepasscodes, 2011.

Barlow, John Perry, Introduction. In: Zimmermann Philip (Ed.), The official PGP user's guide MIT Press, Cambridge, Mass., 1995.

Berkman Center for Internet & Society at Harvard University, Don't Panic. Making Progress on the «Going Dark» Debate, 2016.

Borgmann, Albert, Holding on to reality. The nature of information at the turn of the millennium, University of Chicago Press, Chicago, 1999.

Canetti, Ran/Dwork, Cynthia/Naor, Moni/Ostrovsky, Rafall Deniable Encryption, Annual International Cryptology Conference Springer, Berlin, Heidelberg, 1997, p. 90–104.

Costantini, Federico/ De Stefani, Marco Alvise, Collecting evidence in the «Information Society»: theoretical background, current issues and future perspectives in «Cloud Forensics». In: Schweighofer Eric, Kummer Franz, Hötzendorfer Walter, Sorge Christoph (Eds.), Trends un Communities des Rechtinformatik. Tagungsband des 20. Internationalen Rechstinformatik Symposion / Trends and Communities if Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium, Österreichische Computer Gesellschaft, Wien, 2017, p. 461–468.

Di Nicola, Andrea/Gounev, Philip /Levi, Michael/Rubin, Jennifer/Vettori, Barbara (Eds.), Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime – Final report, Publications Office of the European Union European Union, Luxembourg: 2015.

Diffie, Whitfield/ Hellman, Martin E., Multiuser cryptographic techniques, Proceedings of the June 7–10, 1976, national computer conference and exposition ACM, New York, 1976, p. 109–112.

Floridi, Luciano (Ed.), The Onlife Manifesto. Being Human in a Hyperconnected Era, Open Access Springer International Publishing, Cham 2015.

Floridi, Luciano, The philosophy of information, Oxford University Press, Oxford-New York, 2011.

Grijpink, Jan, Biometrics and Privacy, Computer Law & Security Report, volume 17, issue 3, 2001, p. 154–160.

Gutheil, Mirja /Liger, Quentin /Heetman, Aurélie/Eager, James /Crawford, Max, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, European Union, Bruxelles, 2017.

Horn, Eva/ Ogger, Sara, Knowing the Enemy: The Epistemology of Secret Intelligence, Grey Room, volume 11, 2003, p. 58–85.

Jain, A. K./Ross, A./Prabhakar, S., An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, volume 14, issue 1, 2004, p. 4–20.

Kerr, Orin S./ Schneier, Bruce Encryption Workarounds, 2017.

Marquenie, Thomas, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, Computer Law & Security Review, volume 33, issue 3, 2017, p. 324–340.

Norman, Bruce, Secret warfare, Dorset Press, New York, 1973.

Potoglou, Dimitris/Dunkerley, Fay/Patil, Sunil/Robinson, Neil, Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study, Computers in Human Behavior, volume 75, 2017, p. 811–825.

Prins, Corien, Biometric Technology Law. Making Our Body Identify for us: Legal Implications of Biometric Technologies, Computer Law & Security Report, volume 14, issue 3, 1998, p. 159–165.

Schulze, Matthias, Clipper Meets Apple vs. FBI – A Comparison of the Cryptography Discourses from 1993 and 2016, Media and Communication, volume 5, issue 1, 2017, p. 54–62.

Shannon, Claude E., A Mathematical Theory of Communication, Bell System Technical Journal, volume XXVII, issue 3, 1948(a), p. 379–423.

Shannon, Claude E., A Mathematical Theory of Communication, Bell System Technical Journal, volume XXVII, issue 4, 1948(b), p. 623–656.

Sundt, Chris, Cryptography in the real world, Information Security Technical Report, volume 15, issue 1, 2010, p. 2–7.

Weaver, Warren, The Mathematics of Communication, Scientific American, volume 181, issue 1, 1949, p. 11–15.

Colloquium

Erich Schweighofer / Franz Kummer /
Ahti Saarenpää / Burkhard Schafer (Hrsg. / Eds.)

Datenschutz / LegalTech
Data Protection / LegalTech

Tagungsband des 21. Internationalen Rechtsinformatik Symposions IRIS 2018

Proceedings of the 21st International Legal Infomatics Symposium IRIS 2018

EDITIONS WEBLAW

Nach dem Jubiläum im letzten Jahr geht das IRIS in die dritte Dekade und blickt in die Zukunft. Das 21. Internationale Rechtsinformatik Symposion befasst sich mit den herrschenden Strömungen der Rechtsinformatik: Datenschutz und LegalTech. Während in den letzten Jahren die großen Axiome dominiert haben – Projektkultur, Kommunikation und Sprache, Abstraktion, Applikation, Transparenz, Kooperation, Netzwerke und Communities – liegt diesmal der Fokus auf den wesentlichen Fragen des Jahres 2018.

Schwerpunkte:

- Generalthema: Datenschutz
- Generalthema: LegalTech
- DLT & Blockchain
- Juristische Informatik-Systeme
- Rechtsinformation & Suchtechnologien
- Robolaw
- Recht, Sprache & Kommunikation
- E-Government & E-Justiz
- E-Demokratie, E-Partizipation & E-Gesetzgebung
- Rechtstheorie
- Rechtsvisualisierung & Multisensorisches Recht
- Sicherheit & Recht
- Urheberrecht
- E-Commerce
- TRUESSEC
- E-Procurement

Der Band umfasst neben neuen wissenschaftlichen Erkenntnissen auch Beiträge zu praktischen Problemstellungen und Anwendungen der Rechtsinformatik. Die IRIS-Tagungsbände sind online in der Zeitschrift Jusletter IT unter http://www.jusletter-it.eu verfügbar.

ISBN: 978-3-906940-21-2
9 783906 940212

II.24