FACIAL RECOGNITION SYSTEMS AND THEIR DATA PROTECTION RISKS UNDER THE GDPR

Master Thesis Law and Technology LL.M.
Tilburg University

Supervisors:
PhD researcher Kamara Irene (1st)
Dr. Colette Cuijpers (2nd)

Student: R. Coseraru
u number: 1267884

SEPTEMBER 2017

TABLE OF CONTENTS

CHAPTER 1.

1 Introduction.

The vision that elements of the human body can be used to identify our unique selves is not new at all. Due to their distinctive characteristics, prints of the fingers, foot or hand have been used since the prehistoric times in identification purposes.[1] For example, in Babylonia fingerprints were used in business transactions whereas in China handprints were used as forms of authenticity for the last 2000 years.[2]

Furthermore, by the last decade of the twentieth century, hundreds of millions of fingerprints have been collected. By 1994 the iris algorithm recognition has been patented.[3] Recently, others techniques for automated measuring of face, speech and fingerprints, behavioral characteristics or vascular patterns have been also developed.[4]

In comparison with other new technologies (such as closed-circuit television-CCTV, cell-site simulators, bugging devices, government databases, surveillance through key loggers, police-worn cameras or drones)[5] that are targeting large populations, biometric systems are tightly linked to an individual, as they can use a certain unique property of an individual for identification and/or authentication/verification.[6] Mainly, a very specific cautious approach is needed in the collection of biometric data, as they can expose 'sensitive information' about the persons, including information about health, genetic background, age or ethnicity.[7] Under the new EU Regulation 2016/679[8] **(hereinafter the GDPR),** biometric data has been classed as 'sensitive data'. Processing of biometric data is prohibited unless special requirements are fulfilled. Biometric technologies that required once important computational and financial resources have

---

[1] Kindt Els, Privacy and Data Protection Issues of Biometric Applications A comparative legal analysis (1st edn. Springer, Governance and Technology Series 12, 2013) 14. Available at http://www.springer.com/gp/book/9789400775213 -last accessed 30 of July 2017

[2] Ibid.

[3] Ibid. See also Daugman John, How Iris Recognition Works (IEEE Transactions on circuits and systems for video technology 2004) 21-30. Available at https://www.cl.cam.ac.uk/~jgd1000/csvt.pdf -last accessed 9th of December 2016.

[4] Ibid.

[5] Brownsword Roger and others, The Oxford Handbook of Law, Regulation and Technology (1st edn, Oxford University Press 2017).
See also BBC website, 'The technology of surveillance-Who's watching you?' (BBC.co.uk, 21 May 2009). Available at http://news.bbc.co.uk/1/hi/programmes/whos_watching_you/7978415.stm -last accessed 31 July 2017

[6] Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf -last accessed 29th of July 2017.

[7] Commissioner for Privacy and Data Protection, Information Sheet- Biometrics and Privacy. Available at https://www.cpdp.vic.gov.au/images/content/pdf/CPDP_Information_Sheet_-_Biometrics_and_Privacy_April_2016.pdf -last accessed 8th December 2016.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 191/1/1. Available at http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf -last accessed 30 of July 2017.

now become dramatically faster and cheaper.[9] In consequence, the privacy and security risks linked with the increasing "collection, use, disclosure and retention of personal biometric data has also been developed."[10] In particular, there has been a quick growth in the availability and accurateness of facial recognition systems **(hereinafter FRS)** in the last years. These kind of technologies, that once were considered a science-fiction subject, are now increasingly incorporated in our everyday life. More and more facial recognition systems are integrated into commercial stores, by financial institutions (banks) for authentication/verification purposes, by on-line and mobile services including social-networks and smartphone manufacturers.[11]

Therefore, the domain of the application of the FRS in this thesis is the private sector. However, the following three areas will be covered: automated facial recognition systems **(AFRS**) in the commercial retail, facial recognition systems used for authentication/verification means in banking and FRS used by the social networks sites.

In the commercial retail application, facial recognition technologies with a closed-circuit security system are usually integrated by retailers. Faces of citizens that are caught on cameras are converted in a numerical code known as a 'face template' and cross-referenced with a database for a possible match with known criminals, past shoplifters, celebrities or valued customers.[12] For instance, in 2015, "a recent UK[13] survey of 150 senior IT, marketing or digital retail executives found that 75% of the retailers are using technology that enables the tracking of the customers in stores, whilst 27% of the retailers are already using an automated facial recognition system to track customer's behavior."[14] In addition to determining the identity, more recently, facial recognition systems can be used to "establish characteristics such as ethnic origin, emotion and well-being."[15]

---

[9] See footnote 6. Article 29 WP 193.

[10] Cavoukian Ann, 'Privacy and Biometrics for Authentication Purposes: A Discussion of Untraceable Biometrics and Biometric Encryption.' in Kumar, Ajay, Zhang, David (ed), Ethics and Policy of Biometrics-Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, Hong Kong (Springer Berlin Heidelberg2010) 16. Available at http://www.springer.com/gp/book/9783642125942 -last accessed 30 of July 2017.

[11] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf -last accessed 29th of July 2017.

[12] npr.org, 'High-End Stores Use Facial Recognition Tools to Spot VIPs' (npr.org, 21 July 2013). Available at http://www.npr.org/sections/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips - last accessed 20 January 2017.

[13] CSC press release, 'New CSC Research Reveals Where Shoppers and Retailers Stand on Next Generation In-store Technology-Big Data & Customer Analytics – a key driver for UK Retailers' (CSC, 10 September 2015) . Available at http://www.csc.com/uk/press_releases/133753-new_csc_research_reveals_where_shoppers_and_retailers_stand_on_next_generation_in_store_technology –last accessed 16 August 2017

[14] Lewinski Peter and others, 'Face and Emotion Recognition on Commercial Property under EU Data Protection.' [September 2016] 33(9) Psychology & Marketing, Wiley Periodicals 729-746. Available at http://onlinelibrary.wiley.com/doi/10.1002/mar.20913/abstract last accessed 30 of July 2017.

[15] See footnote 6. Article 29 WP 193.

'In- store cameras can now identify individuals through special software that analyzes unique facial characteristics. In this sense, retailers can ping special offers and discounts to customer's phones only by a simple cross-checking of these unique facial characteristics against customer's smartphone location data. These systems can even recognize and monitor the emotion's change of the customers when they interact with the products.[16] Thus, facial recognition systems may allow the retailers 'to predict the customer's attitude in regards with the products and more specifically whether the customers are likely to buy the products or watch them longer.'[17] Through these systems a wide range of information about customers may be gathered, such as: age, gender, viewing times, facial emotions, people counting, heart rate or face features detection.[18] Thus, on one hand, FRS used in 'digital advertising signage can better target ads based on the demographic characteristics of passersby by providing more tailored and relevant marketing, customized and improved services for the customers.'[19]

On the other hand, consumers have expressed their concerns about identification, commercial tracking and profiling. In this respect, the abovementioned UK survey, held by 2015, revealed that 'nearly three quarters (73%) of the consumers were not comfortable at all with the in-store technology that tracks their behavior whereas 71% were not comfortable with the technologies that record gender, age or the time that consumers spend in-store.[20] Moreover, facial recognition systems may be used for profiling and tracking even if 'there is no knowledge of the real- world identity of the citizens.'[21]

Beyond this specific context, facial recognition systems can be used in the private sector for safety and security purposes, authentication and secure access. FRS are used as techniques of verification/authentication in order to substitute a password or a username and to verify and control the admission to a mobile device or any other on-line service by banking institutions. Financial institutions are starting to use facial recognition systems at access points to verify the identity of the staff and external contractors or to authenticate payments and reduce fraud in mobile banking applications and at ATMs. Nevertheless, internet security firms and hackers have revealed how simple it is to leak face detection

[16] Mathew Wall, 'Is facial recognition tech really a threat to privacy?' (BBC Technology, 19 June 2015). Available at http://www.bbc.com/news/technology-33199275 - last accessed 30 July 2017.
[17] Ibid.
[18] VicarVision, VicarVision Retail Analytics website (2016). Available at http://www.vicaranalytics.com/ -last accessed 18 of January 2016.
[19] Stacy Gray, 'Privacy Principles for Facial Recognition Technology' (Future of Privacy Forum, December 2009). Available https://fpf.org/2015/12/09/facial-recognition-and-privacy/ -last accessed 19 January 2017.
[20] CSC press release, 'New CSC Research Reveals Where Shoppers and Retailers Stand on Next Generation In-store Technology-Big Data & Customer Analytics – a key driver for UK Retailers' (CSC, 10 September 2015). Available at http://www.csc.com/uk/press_releases/133753-new_csc_research_reveals_where_shoppers_and_retailers_stand_on_next_generation_in_store_technology -last accessed 19 January 2017.
[21] Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193, 21. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf -last accessed 29th of July 2017

authentication.[22] In the recent Usenix[23] security conference, held in 2016, security and computer vision specialists have revealed 'a system that is using digital 3-D facial models based on publicly available photos and exposed with mobile virtual reality technology to defeat FRS.' In this sense, it has been proven, how easy it is, to undermine FRS through an accurate facial model that can be made through the usage of the pre-existent publicly available photos, gathered from social network sites of the individuals.[24]

Nevertheless, social networks, like Facebook are using facial recognition software systems to allow automatic tagging of their users. Facebook has developed a sophisticated algorithm that can recognize people with an accuracy of 83%. The users can be identified, even if they cover their face, only on the basis of what they are wearing or on the basis of the shape of their body.[25] For example, when a new picture is posted by a user on his Facebook page, 'the system matches automatically the faces on his photos with the names of his friends.'[26] The significant issue at stake is that Facebook has changed arbitrarily their privacy policies, by offering for their users only the possibility of opting out of this automatic tagging (and only if and when the users have realized this change).[27] The diffusion of this feature is undoubtedly enhancing the traceability of the individuals and is dealing with the user's identity rights.[28] In this way, social networks "could increasingly become targets of access by unauthorized individuals, leading to consumers' facial recognition data being used in ways that consumers cannot anticipate or control, and without their knowledge."[29] The researchers have also proven that by using only photos that were publicly available on social network sites (hereinafter SNS) they succeed in re-identification by simply combining the SNS data with the publicly available FRS.[30] Moreover, profiling, as a result of these automatic tagging systems may simply lead to misrepresentation of citizens. On-line behavioral, profiling might have a relevant negative impact on the users, such as: user's denial to a service

[22] Richardson Deidre, 'Mastercard's new "selfie authentication" takes advantage of photo feature popularity' (Inferse.com, 5 July 2015). Available at http://www.inferse.com/34105/mastercards-selfie-authentication-takes-advantage-photo-feature-popularity/ - last accessed 20 December 2016.
[23] Xu Yi and others, 'Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos' [2016] The University of North Carolina at Chapel Hill. Available at https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_xu.pdf -last accessed 15 of August 2017.
[24] Ibid.
[25] Griffin Andrew, 'Facebook facial recognition algorithms can recognize people even if they hide faces' (Independent UK, 24 June 201. Available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-facial-recognition-algorithms-can-recognise-people-even-if-they-hide-their-face-10342195.html - last accessed 5 January 2017.
[26] Palmer Maija, 'Regulators probe Facebook's facial recognition' (Financial Times, 9 June 2011). Available at https://www.ft.com/content/ffe3edb4-92c8-11e0-bd88-00144feab49a -last accessed 5 December 2016
[27] Monteleone Shara, 'Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?' [2012] 3(3) European Journal of Law and Technology. Available at http://ejlt.org/article/view/168/257 - last accessed 19 January 2017.
[28] Ibid.
[29] See footnote 19. Stacy Gray (2009).
[30] Yanna Welinder, 'A FACE TELLS MORE THAN A THOUSAND POSTS: DEVELOPING FACE RECOGNITION PRIVACY IN SOCIAL NETWORKS' [2012] 6(1) Harvard Journal of Law & Technology 166-192.Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108 –last accessed 25 of August 2017.

or product and discrimination of these users (as they can be included or not in different databases).[31] Recently, more and more social media platforms are consulted by employers (in order to attain information about a candidate) or by law enforcement agencies in criminal investigations.[32]

1.1 Research question.

In view of the above, the central research question in this thesis is:

What are the data protection risks of facial recognition systems (FRS) used in the private sector and how are these risks mitigated through the GDPR?

This research question will be answered through the following sub-questions:

1. **What are the developments of the facial recognition systems (FRS) in the private sector and how do these systems works in practice?**

2. **What are the data protection risks of the facial recognition systems (FRS) that are used in private sectors (automated facial recognition systems in the commercial retail, FRS used for authentication/verification means in banking and FRS used in social networks)?**

3. **How and to what extent does the GDPR mitigate the data protection risks of facial recognition systems used in the private sector?**

1.2 Methodology.

The main type of research used in this thesis is doctrinal legal research. The aim of the research underlying this thesis is to acquire and deliver knowledge with regards to the data protection risks of the facial recognition systems in a systematic and scientific way, by taking into account as a starting point Daniel Solove's taxonomy of 'privacy harms.'[33] Furthermore, an analysis of the relationship between these specific risks and the GDPR will be undertaken, to assess how and to what extent data protection risks of the facial recognition systems in the private sector (automated facial recognition systems in the commercial retail, FRS used for authentication/verification means in banking and FRS used in social networks) are mitigated through the new General Data Protection Regulation.

---

[31] Monteleone Shara, 'Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?' [2012] 3(3) European Journal of Law and Technology. Available at http://ejlt.org/article/view/168/257 - last accessed 19 January 2017.

[32] Ibid.

[33] Solove Daniel, 'A TAXONOMY OF PRIVACY' [2006] 154(3) University of Pennsylvania Law Review. Available at https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf –last accessed 24 of August 2017

The key sources that are used in this thesis are: books and chapters from edited books about facial recognition systems and their data protection risks, journal articles, the new GDPR, decisions, case-law, recommendations and opinions (Article 29 Working Party Opinions), websites and blog-articles and reports that refer to FRS and their data protection risks. The GDPR analysis represents the main focus of the thesis, however, where relevant, reference will be made also to **Directive 95/46/EC**.[34] In addition, even though, it is not the scope of the thesis to assess the entire EU legal framework regarding data protection, a point of concern is the concept of metadata and processing of such data for direct marketing purposes by the FRS. Only in these particular cases, a reference will be made to the proposed **ePrivacy Regulation**.[35]

In the second chapter a descriptive research will be undertaken. The aim is to describe and present the actual state-of affair regarding the implementations of the facial recognition systems in the private sector.

Next, the third chapter provides the outcome of a descriptive and analytical research. In this chapter the data protection risks of facial recognition systems, used in the private sector, are assessed by taking, as a starting point, Solove's taxonomy of privacy harms, as described in his article "A Taxonomy of Privacy."[36] Solove's 'taxonomy of privacy harms' represents an authoritative source under the modern privacy literature. However, this taxonomy has its own distinctive limitations. Firstly, there is a difference in the understanding and application between the US and EU legal framework regarding the notion of privacy (under the US legal framework) and the "right to respect for private life" and data protection in the EU. Whilst, data protection **(article 8 of the EU Charter**)[37] and the 'right to respect for private and family life' (**Article 7 of the EU Charter**) [38] are fundamental rights in the EU, there is a remarkable different understanding of these notions under the US legal framework. In addition, the taxonomy of 'privacy harms' is under-inclusive as it does not refer at all to data protection or entail any reference at all to the concept of risk or to the risk-based approach, notions that are embraced by the General Data Protection Regulation**.**[39] Solove's taxonomy helps to create a better categorization of the FRS risks. The limitations identified and the categorization of the FRS risks will have the role of 'building blocks' for the last chapter. Moreover, these limitations can and will be overcome by adding and highlighting concepts as 'risk' and 'risk based approach.' In addition the identification, security and aggregation risks, as it has been described through Solove's taxonomy of privacy harms, are not the same with the data protection risks depicted under the GDPR. Identification under Solove's interpretation, refers, only, to 'the identification of persons in flesh' whereas the new GDPR is complementing this concept through the adoption of the 'identifiability' notion. Moreover, the concept of 'aggregation harms' is not identical with the profiling

[34] See footnote 8, the GDPR.
[35] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ,COM/2017/010 final - 2017/03 (COD). Available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications last accessed 23 of August 2017.
[36] Ibid.
[37] Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010 (hereinafter **EU Charter**).Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12010P&from=LV –last accessed 23 August 2017.
[38] Ibid.
[39] See footnote 8.The GDPR.

concept, as depicted under the GDPR. Additionally, security risks might be overcome through different means, in the GDPR, through measures such as encryption, pseudonymization, data beach notifications or data protection impact assessments. The fourth chapter describes and explains, through an analytical legal research, how and to what extent the risks of facial recognition for data protection, as identified and categorized in chapter 3, are mitigated by the new GDPR. The final chapter provides the conclusion in this sense.

1.3 Organization of the thesis.

In the next chapter, a general description of biometrics is given. First, the biometric characteristics are described. After that, biometric functionalities are highlighted. Furthermore, the biometric technology phases are described succinctly. In the following section 2.6 of chapter 2 the FRS state of the art is depicted. In this section, in the first part, the FRS processing is explained. In the final part of chapter 2 the automated facial recognition systems used in the private sector are discussed, with a focus on the use in commercial retail, FRS as means of authentication/verification (in the banking sector) and FRS used in social network sites. The third chapter starts with an explanation of the different understanding of the privacy and data protection concepts between EU and US. Furthermore, the FRS data protection risks will be assessed, by taking as a preliminary starting point Solove's categorization of the 'privacy harms' and the FRS state of the art. As it has been already revealed in the methodology, to complement the US oriented taxonomy of Solove and to make it suitable to the current EU situation (the new GDPR), a separation between the concepts of risks and harms will be established. This leads to the analysis of the following risks of the FRS for data protection: identification, security and profiling risks.

The fourth chapter presents an analysis under the GDPR of the identification, security and profiling risks for data protection, identified in chapter 3. The question that has to be answered is: how and to what extent are these risks mitigated and what kind of measures are provided by the GDPR in mitigating these kind of data protection risks?

First, this chapter addresses the concept of risk and the risk based approach from the GDPR perspective. Furthermore, the identification data protection risk are assessed. A distinction between digital images as personal data and biometric data as new category of sensitive data is made. In the section where digital images are presented as personal data a separation is made between directly and indirectly identifiable data. The third section of chapter 4 entails the 'processing of facial images under the GDPR.' The fourth section of chapter 4 describes the security data protection risks of the FRS under the GDPR. The following subsections are provided as well under this section as measures to mitigate these security risks: encryption, pseudonymization, data protection impact assessment and data breach notifications. The fifth section of this chapter highlights profiling data protection risks under the GDPR. The final chapter delivers the conclusion, bringing together the previous chapters and providing an answer to the overarching research question.

Chapter 2

Facial recognition systems (FRS): State of the art.

2.1 Introduction.

In this chapter a general description of biometrics is provided. First, the biometric characteristics are described and secondly the biometric functionalities are highlighted. Furthermore, the biometric technology phases are described succinctly. In the following section, the FRS state of the art is depicted. Firstly, the FRS processing is explained. The last part of the chapter concerns the automated facial recognition systems used in commercial stores used as means of authentication/verification in banking and FRS used in social networks.

2.2 Biometric technologies.

The term biometrics is derived from the Greek nouns bio (life) and metric (to measure) and represents the "measurement of the living species."[40] The usage of biometric systems entails "that unique or distinctive characteristics of persons are *collected, measured and stored* for the **automated verification** of a claim made by that person or for the **identification** of that person.[41]

The idea that human characteristics are used for **identification** means is not new at all. Hundreds of millions of fingerprints have been collected and used manually in police investigations from the early twentieth century.[42] Through this system, samples taken from individuals, or 'live' data were generally used in a 'one-to-one' matching[43]

Consequently, in the last decades, automated computer aided techniques have started to be used. By 1991 face detection has been pioneered, making real time face detection possible.[44] Now, the recognition process 'has been matured into a science of automated mathematical representation and matching

[40] See footnote 1.Els Kindt (2013). See also Marios Savvides, 'Introduction to Biometric Technologies and Applications, Carnegie Mellon CityLab. Available at https://users.ece.cmu.edu/~jzhu/class/18200/F06/L10A_Savvides_Biometrics.pdf - last accessed 25 of May 2017.
[41] See footnote 1. Els Kindt (2013). See also Rawlson King, 'Explainer: Facial Recognition ' (Biometric Update, 10 January 2016). Available at http://www.biometricupdate.com/201601/explainer-facial-recognition - last accessed 30 July 2017.
[42] See footnote 1. Els Kindt (2013).
[43] Cavoukian Ann, 'Privacy and Biometrics for Authentication Purposes: A Discussion of Untraceable Biometrics and Biometric Encryption.' in Kumar, Ajay, Zhang, David (ed), Ethics and Policy of Biometrics-Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, Hong Kong (Springer Berlin Heidelberg2010) 16. Available at http://www.springer.com/gp/book/9783642125942 -last accessed 30 of July 2017.
[44] Mayhew Stephen, 'History of Biometrics' (BiometricUpdate, 14 January 2015). Available at http://www.biometricupdate.com/201501/history-of-biometrics - accessed 23 February 2017.

process."[45] World-wide revenues, from the biometric mobile sector are expecting to reach by 2020, to 45 billions of dollars. In addition, the biometric smartphone market is expected to increase tenfold, reaching to 2 billion of users by the end of the same year.[46]

However, a clear definition of these systems is hard to provide. The Article 29 Working Party (hereinafter **A29 WP**), described biometric systems, as: "applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person."[47] In addition, in the A29 WP Opinion 3/2012, a biometric system has been defined in a broader sense as "a system that extracts and further processes biometric data."[48]

2.3 Biometric data characteristics.

Biometric features that are used in both identification and verification entail specific qualities. These are presented now, since they will also form the basis of the risks analysis of the next chapter. Biometrics shall be universal, persistent and unique or at least distinctive.

Universal. Universal represents that biometric characteristics exist in all persons.[49] Humans have a noteworthy capability to recognize other individuals based on their facial appearances. Therefore, the face is the natural human feature that is used for automated biometric recognition.[50] However, individuals may have lost some significant characteristics due to accidents. Nevertheless, the expressions of emotions of the faces, are universal.

Uniqueness. It should be necessary to use the biometrics in order to differentiate between two different individuals.[51] The face is undoubtedly an individual's evident unique characteristic. The advantages are rooted in the inimitability and immutability of these particular traits.[52] Humans possess the native ability

[45] Rawlson King, 'Facial recognition' (BiometricUpdate, 10 January 2016). Available at http://www.biometricupdate.com/201501/history-of-biometrics - last accessed 23 February 2017.
[46]Biometric Update Research-Mobile Biometric Market Analysis. Available at http://www.biometricupdate.com/wp-content/uploads/2015/10/287127021-Mobile-Biometrics-Market-Analysis-5.pdf - last accessed 22 February 2017
[47] Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf -last accessed 29 of July 2017.
[48] Ibid.
[49] Article 29 Data Protection Working Party, Working document on biometrics, August 1, 2013. 00720/12/EN WP80. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf
[50] Jain Anil and Kumar Ajay, Biometric Recognition: An Overview in Emilio Mordini and Dimitrios Tzovaras (eds), Second Generation Biometrics: The Ethical, Legal and Social Context (Springer Netherlands- The International Library of Ethics, Law and Technology' 2012) 49- 79. Available at https://link.springer.com/chapter/10.1007%2F978-94-007-3892-8_3 -last accessed 21 April 2017.
[51] De Marisico Maria and others, Face Recognition in Adverse Conditions (1 edn, IGI Global 2014) 361. Available at https://www.di.ubi.pt/~hugomcp/doc/IGI_Face.pdf -last accessed 28 of July 2017.
[52] Vacca John, Biometric Technologies and Verification Systems (1st edn, Elsevier 2007). Available at https://booksite.elsevier.com/samplechapters/9780750679671/Sample_Chapters/01~Front_Matter.pdf -last accessed 30 of July 2017.

to identify and differentiate among diverse faces, computers now have also developed this ability.[53] These recognition's abilities have been developed, as human's faces entail definite discernable landmarks called nodal points.[54] These nodal points are 'peaks and valleys that make-up the facial features.'[55] A human face has approximately 80 nodal points and FRs are usually using the following nodal points as common denominators: "distance between eyes, width of nose, cheekbones, jawlines or chin."[56]
However, despite the high level of recognition ability and accuracy of the advanced FRS, on the 2016 Usenix security conference, 'security and computer vision specialists presented a system which uses digital 3-D facial models based on publicly available photos and displayed with mobile virtual reality technology to defeat FRS.'[57]
In addition to this, 'illumination, gesture, facial make-up, occlusion and variations that harmfully affect the FRS performance or other non-ideal situations are persistently posing challenges.

Persistency. The biometric characteristics necessarily need to be permanent, as they may not alter in time.[58] Faces of a person can undoubtedly, offer trustworthy recognition. However, faces of the persons are more prone to modification than other human features.[59] Simply put, over an extended period of time many difficulties may appear as a consequence of intended or unintended occurrences, like injuries, losing or gaining loss, surgery, growing of the beard or wearing glasses. In consequence, supplementary checks will be necessary, costs will be enhanced and the data subjects will be likely to be re-enrolled more often at a different interval of times.[60]

2.4 Biometric system functionalities.

As revealed before, biometric systems collect and commonly store typical biological and behavioral characteristics of individuals for automated verification or for the identification of that particular person. Therefore, taking into account the application circumstance, and the previous description, a biometric system may run either through an identification or a verification mode.[61]

The verification process or the one-to-one matching process (1:1) enables the process of comparison of the submitted biometric characteristic with regards to only one formerly specific stored biometric

[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] Newman Lily Hay, 'Hackers Trick Facial-Recognition Logins with Photos from Facebook (What Else?)' (Wiredcom, 19 August 2016). Available at https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/ - last accessed 15 August 2017. See also Xu Yi and others, 'Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos' [2016] The University of North Carolina at Chapel Hill. Available at https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_xu.pdf -last accessed 15 of August 2017.
[58] See footnote 1. Els Kindt (2013).
[59] Ibid.
[60] Ibid.
[61] See footnote 52.Vacca John (2007).

characteristic."[62] This function is commonly used for positive recognition and its purpose is to prevent numerous individuals from using the same identity.[63] Verification does not commonly involve an identification function and it does not demand that the biometric features should be deposited in a central database. They may be stored, for example, on a card that is in the possession of the users.[64] In this system, a person who is willing to be recognized asserts his/her identity username or PIN commonly via a smart card, user name or PIN.[65] Nevertheless, this functionality was discussed now, for a better understanding of the modern face authentication systems that will be presented in **section 2.6**.

On the other hand, through the identification function, a biometric system recognizes a person through a comparison of the given biometric characteristic with all the pre-existent biometrics features stored in one or multiple databases. This so-called one-to-many (1:n) comparison is aimed to identify an individual through a search of the templates of all the users existent in a database. Identification is a pivotal element in negative recognition in order to prevent an individual from using multiple identities.[66] The distinction based on the functionality of the biometric systems is essential, as different possible risks may arise. In the verification systems, biometric data are stored, locally, under the control of the individual. In contrast, under identification systems biometric data are not under the physical control of the targeted person.[67] Hence, identification may pose higher privacy risks in the private sector.

2.5 Biometrics technologies phases.

In the next section, an overview of the functioning of biometric systems, will be given.

In general, biometric technologies are following the three steps: enrollment, comparison and decision.

Firstly, there is the enrollment phase. In this first step, biometric technologies are gathering the specific individual physiognomies. Through this process a so-called 'template' is created.[68] Commonly, the templates are accessible in digitalized forms.'[69] The enrollment phase, "plays a key-role", since all raw

[62] See footnote 1. Els Kindt (2013).
[63] See footnote 50. Jain Anil et.al. (2012).
[64] Iglezakis, I. 'EU Data protection legislation and case-law with regard to biometric application'. (Aristotle University of Thessaloniki, 18 June 2013). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2281108 – last accessed 18 February 2017.
[65]See footnote 50. Jain Anil et.al. (2012).
[66] Ibid.
[67] Kindt Els, 'Biometric application and the data protection legislation- the legal review and the proportionality test' [2007] 31(3) Datenschutz und Datensicherheit 166-170. Available at http://www.fidis-project.eu/fileadmin/fidis/publications/2007/DuD3_2007_166.pdf - last accessed 30 of July 2017.
[68] De Luis Garcia Rodrigo et al, 'Biometric Identification Systems' [2003] 83(12) Elsevier Signal Processing. Available at http://dx.doi.org/10.1016/j.sigpro.2003.08.001 - last accessed 16 February 2017.
[69] Article 29 Data Protection Working Party, Working document on biometrics, August 1, 2013. 00720/12/EN WP80.Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf -last accessed 30 of July 2017.

data (an image), extraction, protection of algorithms and templates are present."[70] In the second step, the biometric data, that are gathered from "the submitted biometric sample (query sample) are compared with the template."[71]

In the third step, the final outcome of the comparison or decision is established. There are two types of decisions for biometric systems: identification and verification. The verification decision is the 'determination of the validity of a biometric claim' whereas the identification decision defines "whether a biometric reference of a specific biometric data subject is in a biometric reference database or not."[72] The decision-making process is done, sometimes, under uncertainty and "requires, human interpreters of its results."[73] The uncertainty comes from both the automated facial recognition system and also from the human interpreters. The decision-making has an interpretable foundation, from which the most probable solution can be selected.[74] A biometric match embodies not a definite recognition but a probability of a correct recognition whilst a non-match is characterized through a probability rather by a decisive deduction that a person is unknown to the system.[75] In this sense, a relatively recent study reveals that computers might outpace human interpreters in regards with the 'frontal still faces images across changes in illumination.'[76] Humans perform well in recognizing familiar faces but not in regards with the unfamiliar ones. However, they can adapt better than computers for combinations of changes in pose, illumination, blur, and resolution images.[77]

2.6 Facial recognition systems (FRS).

The face is a universal feature of humans and one of the most suitable biometrics.[78] But, even though, people have adopted faces as means of recognition since immemorial stage, the 'effort' to empower computers for human face's recognition has been taking place since the mid-1960s.[79] Back then,

[70] Ibid.
[71] See footnote 1.Els Kindt (2013).
[72] Ibid.
[73] Pato Joseph and Lynet Myllet, Biometric Recognition: Challenges and Opportunities (1st ed. National Academy of Science 2010) 4. Available at https://dataprivacylab.org/TIP/2011sept/Biometric.pdf -last accessed 25 of August 2017.
[74] Ibid.
[75] Ibid.
[76] Phillips P.J. et al., "FRVT 2006 and ICE 2006 Large Scale Results," IEEE Trans. Pattern Analysis and Machine Intelligence, forthcoming; DOI 10.1109/TPAMI.2009.59. See also Rama Chellapa and others, 'Face recognition by computers and humans' [2010] 1(1) IEEE Computer Society 46-55. Available at http://pages.cs.wisc.edu/~dyer/cs534/papers/face-recog-2010.pdf- last accessed 30 of July 2017.
[77] Ibid.
[78] Patil Shailaja and PJ Deore, 'Face Recognition: A Survey' [2013] 1(1) Informatics Engineering, an International Journal (IEIJ) 31-41. Available at https://pdfs.semanticscholar.org/9166/643aabcd5261299fbcd7c949246d71ec0b3e.pdf -last accessed 25 of August 2017.
[79] Jain Anil and others, '50 years of biometric research: Accomplishments, challenges, and opportunities' [2016] 79(1) Pattern recognition letters- Elsevier 80-105. Available at https://pdfs.semanticscholar.org/dc97/ceb1faf945e780a92be651b022a82e3bff5a.pdf -last accessed 23 of August 2017.

Woodrow W. Bledsoe and his associates of Panoramic Research have defined the FRS as a 'man-machine system since it has been necessitated exclusively human experts to detect facial landmarks on an image.'[80] Nowadays, the real-time FRS has been made viable in a broad range of applications due to the developments in the face acquisition systems either 2D, 3D, infrared, or other video cameras, developments in algorithms and semi-conductor technology (smaller and cheaper image sensor). Currently, it is possible to acquire good quality images through wearable devices and smartphones. Therefore, facial recognition systems, that once seemed to be out of the movies, are more and more incorporated in our current lives.

According to a report, made by Tractica[81], it has been forecasted that "facial recognition and licenses will increase from 28.5 million of dollars in 2015 to more than 122.8 million worldwide by 2024." During the same period the annual revenue gained from facial recognition technologies will reach 882.5 million dollars.[82] Since 2015, Europe is the second largest contributor to global biometrics.[83] Moreover, in UK stores, currently 27% of the retailers are using automated facial recognition systems in order to track customer's behavior.[84]

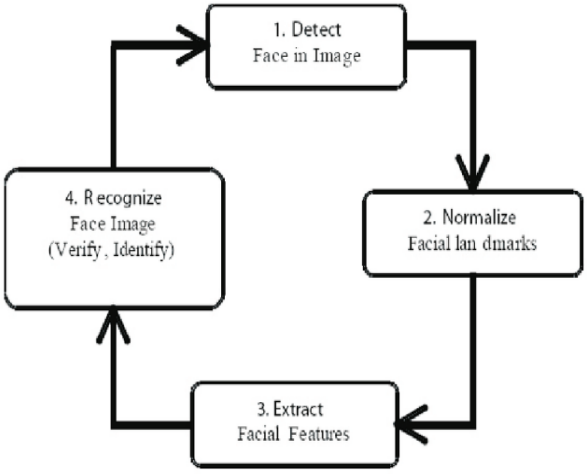
According to A29 WP Opinion 2/2012 on facial recognition on mobile and online devices, facial recognition is defined as "the automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorization."[85] Thus, following the same pattern, face recognition scenarios may be acknowledged in: *face verification (one- to- one match)* and *face identification* (one-to-many match). Face verification or the authentication is the simplest mission for a FRS. In this stage, a person with a predefined affiliation (that is enrolled previously in the gallery or reference database) simply presents the biometric feature (face or probe image) to the FRS, requesting the existence in the database.[86] In consequence, there are two outcomes: either the person is recognized or not. When the individual is not recognized it might be a result of an error (false rejections), or the individual is an impostor (identity theft).[87] On the other hand, identification is a bit more complex than

[80] Ibid.
[81] Tractica, 'Facial Recognition Devices and Licenses Will Reach 122 Million Annually by 2024' (Tractica.com, 26 June 2015). Available at https://www.tractica.com/newsroom/press-releases/facial-recognition-devices-and-licenses-will-reach-122-million-annually-by-2024/ - last accessed 16 February 2017.
[82] Ibid.
[83] Ibid.
[84] CSC press release, 'New CSC Research Reveals Where Shoppers and Retailers Stand on Next Generation In-store Technology-Big Data & Customer Analytics – a key driver for UK Retailers' (CSC, 10 September 2015) . Available at http://www.csc.com/uk/press_releases/133753-new_csc_research_reveals_where_shoppers_and_retailers_stand_on_next_generation_in_store_technology –last accessed 19 January 2017.
[85] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192.Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf -last accessed 25 of August 2017.
[86] Introna Lucas D. and Nissenbaum, Helen, Facial Recognition Technology: A Survey of Policy and Implementation Issues (July, 22 2009). Center for Catastrophe Preparedness and Response, New York University. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1437730 – last accessed 28 of March 2017.
[87] Ibid

the verification task.[88] That is the situation of the one-to-many matches where a query face image is compared against all the existent template face images in the database, with the purpose to determine the real identity of the query face image.[89]

Fig. 1 Phases in FRS

2.6.1 Face recognition processing.



The FRS has normally four phases or steps that are inter-related (**See Fig. 1**).[90] The first step is the face detection, the second one is normalization, the third one is the feature extraction, whereas the final fourth step is the recognition. *Firstly*, there is the image acquisition or face detection. Image acquisition represents the process of taking a photo of an individual and translating it to a digital form.

Detecting the face in the image is not an easy task for computers, since it has to be concluded which pixels in the photos are part of the face. Blurred background and other inanimate elements might also generate complex issues towards the detection of the face. *Secondly,* after the image has been taken, it has to be normalized. A standardization of the illumination, pose or other conditions is more than necessary. Moreover, facial landmarks (like eyes or face color) are paramount to be identified. If not the entire process will be unsuccessful. Normalization enables recognition. Recognition may succeed only if the probe image and gallery images are similar. *Thirdly*, the feature extraction will be undertaken. Hereinafter, a biometric template will be created and will be stored in the database. This template will be the basis of any further recognition assignment.[91] The final step of the FRS process is the recognition. For an effective recognition it is required that a maximum amount of information is gathered. It is important for successful recognition that maximal information is retained in this process so that the biometric template is sufficiently distinctive. If this cannot be achieved, the algorithm will not have the discriminating ability required for successful recognition. In addition, A29 WP Opinion 2/2012[92] alongside the afore-mentioned four steps is mentioning the enrollment and comparison stages. Under the enrollment stage, the A29 WP

[88] Ibid.
[89] See footnote 78. Patil Shailaja (2013).
[90] Agagu TT and Akinnuwesi B., 'Automated Students' Attendance Taking in Tertiary Institution using Facial Recognition Algorithm' [2012] 19(2) Journal of Computer Science and Its Application. Available at https://www.researchgate.net/publication/236003526_Automated_Students'_Attendance_Taking_in_Tertiary_Institution_using_Facial_Recognition_Algorithm -last accessed 2 September 2017.
[91] See footnote 86. Introna Lucas D. and Nissenbaum (2009).
[92] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

Opinion 2/2012 mentions that: "if this is the first time an individual has encountered the facial recognition system the image and/or reference template may be stored as a record for later comparison."[93]

Furthermore, next to the identification and verification, the categorization is mentioned as a consequence of comparison. Categorization system has the purpose to extract features from photos of individuals and to make categorization on the basis of their gender, age, ethnicity, clothes etcetera. Therefore, facial recognition systems are not only used just for identification of individuals but for identification of specific characteristics about individuals.[94]

2.6.2 Automated facial recognition systems in commercial retail.

A practical example of facial recognition technology that allows the retailer to analyze emotion and to predict the attitude of the customers towards the product is the digital advertising signage. This method is usually used by shopkeepers. They are installing mid-to-large electronic displays in order to attract the customer attention and for supplementary advertising of the products.[95] By taking into account the 'Aberdeen Research, the global market around the digital signage have been expanded from $1.3 billion in 2010 to almost $4.5 billion in 2016.'[96] The digital signage in combination with the computer vision systems is providing an effective re-identification and 'an out of home advertisement that can provide an accurate audience measurement of data'[97]

In the case of digital signage, the biometrics data 'inferred from the face of users that are in front of the advertising screen (e.g. gender recognition age, classification of the people behavior) can provide objective measurements essential for building user's profiling.[98] These systems are capable of acknowledging the customer's preferences for a particular product, the view time in front of a product, the audience behavior and emotional reaction in order to establish an enhanced program for advertising and a better understanding of the customer's attraction to a particular campaign.[99] The technology is able to make a distinction between the genders or people moods. The individuals that usually spend in front

[93] Ibid.

[94] Ibid.

[95] Buckley Ben and Hunter Matt, 'Say cheese! Privacy and facial recognition' [2011] 27 Computer Law & Security Review, 637–640. Available at http://www.its.ohiou.edu/bernt/ITS351/say%20cheese%20privacy%20and%20facial%20recognition.pdf –last accessed 25 of August 2017.

[96] Farinella GM and others, 'Face Re-Identification for Digital Signage Applications' [2014] Springer Image Processing Laboratory, Department of Mathematics and Computer Science University of Catania. Available at http://iplab.dmi.unict.it/download/VAAM2014/FinalPaper.pdf -last accessed 1 August 2017. See Aberdeen Research: Digital Signage: A Path to Customer Loyalty, Brand Awareness and Marketing Performance, [2010].

[97] Borut Batagelj and others, 'Computer Vision and Digital Signage' [2008] Tenth International Conference on Multimodal Interfaces. Available at http://eprints.fri.uni-lj.si/1162/1/computer.vision.and.digital.signage.pdf - last accessed 1 August 2017.

[98] See footnote 96. Farinella et. al.(2014).

[99] Exeler J and others, 'Digital Signs that react to Audience Emotion. 2nd Workshop on Pervasive Advertising, [2009] 38-44. Available at https://pdfs.semanticscholar.org/ad2f/73a6f3735d4651c1199aa595385e2c65effc.pdf - last accessed 29 of July 2017

of the screen a particular longer period of time, were targeted and they were receiving personalized e-mails.[100]

Taking into account the previous section, digital signage technology, similarly, is entailing four phases. Firstly, there is the face detection module, where the facial areas are separated from the background. Facial features as 'the eyes, nose or other outlines' are extracted.[101] Secondly, there is the normalization in regards with the geometrical characteristics such as size and pose, but also on the basis of the photometrical properties.[102] Thus in order to eliminate, the photometric shifts of illumination, local shadowing and highlights, the normalization phase is applied.[103]

Thirdly, there is the feature extraction phase that has the aim to provide useful information in differentiating the individual faces and fix the so-called photometrical and geometrical variations.[104] In this stage, "features to distinguish different classes of ages, gender, race group and even different expressions (disgust, fear, joy, surprise, sadness, anger) are extracted."[105] A "detailed analysis can recognize facial hair (beard, mustache), makeup, eyeglasses, headgear, shawl, and hair (style, color, and length)."[106] In the end, there is the face re-identification phase where the FRS system has to answers questions like: 'is the current customer and the previous seen customer the same person?'[107] In its final stage, the FRS are classifying the psychological features of the persons by comparison to a pre-existent database.[108]

In the shopping context, the FRS are used for understanding behavior or for influencing behavior of the customers.[109]

To summarize, a digital signage system might have the ability to generate 'live data' that can be further utilized in different manners: 'estimating the number of the viewers and the profiles of them; use the viewer's statistics in order to generate useful data for the advertisers; make links between the audience and the content: by providing tailored campaigns (e.g. selection of the specific message for a certain age category or gender category, or in relation to the particular conduct of the customers).'[110]

In addition, another big threat of these technologies may be identified. By linking these technologies to social network sites or, other kind of databases, the retail companies may be able to target on-line promotions to individuals on the basis of their particular characteristics and they might tab directly to the

[100] Russel Daniel 'Interactive Digital Signage: An ebay Pop up with Face Recognition in London' (Digital Signage Summit Event, 15 December 2016). Available at http://digitalsignagesummit.org/blog/2016/12/15/interactive-digital-signage-an-ebay-pop-up-with-face-recognition-in-london/ - last accessed 21 February 2017.
[101] See footnote 97.Borut Batagelj et.al. (2008).
[102] Ibid.
[103] See footnote 96. Farinella et.al (2014).
[104] See footnote 97.Borut Batagelj et.al. (2008).
[105] Ibid
[106] Ibid
[107] See footnote 96. Farinella et.al (2014).
[108] See footnote 14. Lewinski et.al. (2016)
[109] See footnote 16. Mathew Wall (2015).
[110] See footnote 97. Borut Batagelj et.al. (2008).

social network's profile of customers.[111] In this respect, the Information Commission Officer's (ICO) group manager, Simon Rice has concluded that:

"This technology, which is starting to be rolled out in shops, allows retailers to use the customer journey to build up a picture as to how people typically use the store. It uses the MAC address of a smartphone which can, in many cases, be linked to a specific individual."[112]

Apart from the particular usage of facial recognition technologies in commercial retail stores, this technology is used for authentication/verification in banking.

2.6.3 Facial recognition systems as means of authentication/verification in banking.

By the last decades, face authentication systems have faced an on-going development that can be seen in the improved security feature in the desktop computers and smart mobile devices.[113] There is no doubt, that nowadays mobile phones cannot be seen only as mobile devices, but as comprehensive online client systems, ones that are enabling the performance of different applications. Thus, since the computer vision algorithms have advanced, a relative high number of the application's developers and vendors have begun to deliver solutions in the mobile device area with different amounts of security.[114] The biggest players in the software industries (like Google and Apple) have already implemented[115] FRS and recently bought facial recognition start-up software companies.[116] In this sense, financial institutions have announced the use of FRS in order to authenticate payments or other financial transactions. [117] The new selfie authentication will 'allow the users to validate their identity after validating the purchase.'[118] Despite of the usage of passwords or other PINs, banks are more interested now in digitizing their products by using the FRS mobile application.

---

[111] See footnote 95. Buckley Ben and Hunter Matt (2011).

[112] Rice Simon, 'How shops can use your phone to track your every move and video display screens can target you using facial recognition' (Information Commissioner's Office,(21 January 2016). Available at https://iconewsblog.org.uk/2016/01/21/how-shops-can-use-your-phone-to-track-your-every-move/ - last accessed 24 February 2017.

[113] See footnote 23.Xu Yi et.al. (2016).

[114] Ibid.

[115] CDT Comments on the Federal Trade Commission's ,'Seeing Is ID'ing: Facial recognition and Privacy', facial recognition forum 8 December 2011, published 22 January 2012 Available at https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf

[116] Forbes, 'Forbes.com' (*Why Did Apple Acquire Facial Recognition Company RealFace?* (22 February 2017) Available at https://www.forbes.com/sites/quora/2017/02/22/why-did-apple-acquire-facial-recognition-company-realface/#3e51d528500b –last accessed 15 August 2017.

[117] Richardson Deidre, 'Mastercard's new "selfie authentication" takes advantage of photo feature popularity' (*Inferse.com*, 5 July 2015). Available at http://www.inferse.com/34105/mastercards-selfie-authentication-takes-advantage-photo-feature-popularity/ - last accessed 20 February 2017. See also "Lloyds says Hello to the facial recognition banking". Available at https://www.ft.com/content/923fec7c-205c-11e7-b7d3-163f5a7f229c last accessed 28 of March 2017.

[118] Ibid.

FRS used as techniques of verification/authentication are commonly used to substitute a password or a username and to verify and control the admission to a mobile device or any other on-line service. Under, the enrollment stage, the cameras of these systems are used to obtain the user's photograph with the final aim to authorize the operators of these devices.[119] FRS used for authentication are rooted on a "learning mechanism to collect the data."[120] The reference template that is generated will be deposited on a face database existent on the service or on other on-line services (as cloud services). Nevertheless, in order to attain authorization/access, a different photo of the person trying to get access is captured by the FRS. The process will include the above-mentioned processes like face detection, normalization and feature extraction of the newly captured picture. In the end, the reference template is compared with the new image and if a positive match identifies the user, access will be granted. Besides the identification risks, given the predominance of the high resolution of the face images that are shared via social network sites and the pervasive nature of the image acquisition of the users, nowadays, is it relatively simple for the attackers to initiate easily spoof-attack towards the FRS.[121]

Spoofing is defined as an "act of masquerading as valid user by falsifying data to gain an illegitimate access." [122] Spoof-biometric attacks, initiated against the mobile authentication/verification systems might enable the malign users to gain admission to the smartphones and to allow the leak of sensitive bank information of the customers.[123] Different type of spoof attacks are presented in the section 3.6 of the following chapter.

2.6.4. FRS used in social networking sites (SNS).

Nowadays the quantity of the photographs have been reckon an explosive growth rate. Considering, Facebook, for example, was entailing by 2014 more than 250 million of photos uploaded.[124] In this sense, due to the broad accessibility of the images and videos on-line, FRS will be likely to enable to identify the persons behind the cameras with the on-line photos. Moreover, as the personal information is more and

[119] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf -last accessed 30 of July 2017

[120] Duc Nguyen and Buy Minh, 'Your face is not your password' [2009] 1(1) Security Vulnerability Research Team Bach Khoa Internetwork Security (Bkis) Ha Noi University of Technology – VietNam. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.8363&rep=rep1&type=pdf -last accessed 30 July 2017.

[121]Keyurkumar Patel and others, 'Secure Smartphone Unlock: Robust Face Spoof Detection on Mobile' [2015] 15(15) MSU Technical Report MSU-CSE-15-15, Oct 21, 2015 1-13. Available at https://pdfs.semanticscholar.org/bfd2/505fbc432cd0def950b7d099fd4797b562e1.pdf -last accessed 23 of August 2017.

[122] N. Erdogmus and S. Marcel. Spoofing face recognition with 3d masks. Information Forensics and Security, IEEE Transactions. Available at https://www.researchgate.net/publication/262605045_Spoofing_Face_Recognition_With_3D_Masks -last accessed 20 Of July 2017

[123]Ibid.

[124] Acquisti Alessandro and others, 'Face Recognition and Privacy in the Age of Augmented Reality' [2014] 6(2) Journal of Privacy and Confidentiality 1-20. Available at http://repository.cmu.edu/jpc/vol6/iss2/1/ -last accessed 20 of August 2017

more disclosed with the others, the information becomes co-owned, and a better 'coordination will be necessary between co-owners, in order to not break with social norms or to violate data privacy norms.'[125] However, the discretion and coordination is not frequently offered within the SNS and other similar applications.[126]

By December 2010, Facebook has announced a new function called 'Photo Tag Suggest' which is using FRS in order to enable the identification of the individuals in the newly uploaded photos by making a link with the earlier labeled images of the users.[127] When a new picture is posted by a user on his Facebook page 'the system matches automatically the faces on his photos with the names of his friends.'[128]

This feature also suggest the name of the person and provides a hyperlink of the Facebook user's profile. The profile might disclose personal information as gender, religious beliefs, sexual orientation, phone numbers or other status updates.[129] In addition, a recent study has demonstrated that ""a proof-of-concept [of an] iPhone application can snap a photo of a person and within seconds display their name, date of birth and social security number."[130] In this sense, the risk of identification of a simple walking stranger may arise.[131]

2. 7 Conclusion.

After a general presentation of the biometric characteristics, functionalities and their technological phases, FRS state of the art has been highlighted. In the FRS state of the art section, the FRS processing steps have been depicted.

As it has been already described, the biometric systems (in particular FRS) are used for identification and authentication/verification purposes and they imply mandatory qualities as: universality, persistency and uniqueness. Verification/authentication is the 'determination of the validity of a biometric claim' whereas the identification defines "whether a biometric reference of a specific biometric data subject is in a

[125] Wisnieski Pamela and others, 'Facebook Apps and Tagging: The Trade-off between Personal Privacy and Engaging with Friends' [2015] 66(9) JOURNAL OF THE ASSOCIATION FOR INFORMATION SCIENCE AND TECHNOLOGY 1883-1896. Available at http://onlinelibrary.wiley.com/doi/10.1002/asi.23299/abstract -last accessed 23 of August 2017.

[126] Ibid.

[127] See footnote 30. Wellinder (2012).

[128] Palmer Maija, 'Regulators probe Facebook's facial recognition' (Financial Times, 9 June 2011). Available https://www.ft.com/content/ffe3edb4-92c8-11e0-bd88-00144feab49a - last accessed 5 December 2016

[129] Justin Mitchell, *Making Photo Tagging Easier*, THE FACEBOOK BLOG (June 30, 2011, 8:16 PM). Available at http://blog.facebook.com/blog.php?post=467145887130 –last accessed 30 of July 2017.

[130] See footnote 30.Wellinder (2012). See also David Goldman, *In the Future, Can You Remain Anonymous?* CNN MONEY (Jan. 13, 2012). Available at http://money.cnn.com/2012/01/13/technology/face_recognition/indexhtm?iid=EL – last accessed 31 of July 2017.

[131] Application as Google Googles. See in this sense Arthur Charles, 'The Guardian' (Facebook in new privacy row over facial recognition feature, 8 June 2011). Available at https://www.theguardian.com/technology/2011/jun/08/facebook-privacy-facial-recognition - last accessed 15 February 2017.

biometric reference database or not."[132] The distinction based on the functionality of the biometric systems and biometric data characteristics is essential to ascertain, since different possible risks might arise. These risks will be revealed in the next chapters of this thesis. Following section 2.5 (biometric technologies phases: enrollment, comparison and decision), it has been revealed that FRS normally entail four phases or steps that are inter-related. The first step is the face detection, the second is normalization, the third one is the feature extraction, whereas the final fourth step is the recognition. Face detection is not a simple task due to the existence of the pixels in the photos, blurred background and inanimate elements. In the recognition phase, it is required that maximum information is retained, in order for the template to be sufficiently distinctive. If not, the recognition will not be successful. The last step is defined as, the 'decision', and sometimes necessitates human interpreters.
The FRS processing phases are bearing a paramount role and they will be used in the next two chapters. Additionally, a specific distinction between the automated facial recognition systems used in the commercial store (digital signage technologies), FRS as means of authentication/verification in banking and FRS used in social network sites have been undertaken. Firstly, as it has been highlighted, the digital signage in combination with the computer vision systems can provide an effective re-identification and 'an out-of home advertisement, one that can provide an accurate audience measurement of data.'[133] These systems possess, also, the capability to track users in an environment via their MAC address. In this sense, individuals can be tracked, also, via their facial image.[134]

These systems are used for both re-identification and profiling in commercial retail. In addition, the possibility of a linkage of these technologies to social network sites or, other kind of databases have been identified. The commercial retail companies that are using FRS, besides their possible ability to target online promotions, might tab directly into SNS profiles of their customers.[135]

Furthermore, it has been revealed that FRS can be used in verification/authentication. In particular, only FRS used to verify and control the admission to a mobile device or any other online service by banking institutions, were analyzed. In this situation, FRS have the role to substitute a password or a username and to verify and control the admission to a mobile device or any other online service by banking institutions. These types of FRS usages have been presented in this chapter, in order to build upon the next chapters where security risks will be highlighted. FRS used for means of authentication/verification are more likely to require the storage of the template for use in a later comparison. In consequence they will entail higher security risks.

Finally, FRS might be used in social networking sites (SNS) and applications for identification. Thus, due to the broad accessibility of the images and videos online, FRS will likely be able to identify the persons behind the cameras through the usage of on-line photos. Besides the identification risks these technologies entails security risks.

[132] Ibid.
[133] See footnote 97. Borut Batagelj et.al. (2008).
[134] Ibid.
[135] See footnote 95. Buckley Ben and Hunter Matt (2011).

CHAPTER 3.
Identification, security and profiling risks of the FRS for data protection.

3.1 Introduction.

In this chapter, the FRS data protection risks are succinctly described, by taking as a starting point Solove's categorization of privacy harms. Solove's taxonomy has been depicted by 2006, in his "A Taxonomy of Privacy" article.[136] The decision to choose Solove's 'taxonomy of privacy harms', in this chapter, came upon the following rationale: Solove's 'taxonomy of privacy harms' represents an authoritative source in the modern privacy literature. However, this taxonomy has its own distinctive limitations in regards with the new GDPR.

Firstly, there is a difference in the understanding and application between the US and EU legal framework regarding the notion of privacy (under the US legal framework) and the "right to respect for private life" and data protection in the EU. Whilst, data protection **(article 8 of the EU Charter**)[137] and the 'right to respect for private and family life' (**Article 7 of the EU Charter**)[138] are fundamental rights in the EU, there is a remarkable different understanding of these notions under the US legal framework. In addition, the taxonomy of 'privacy harms' is under-inclusive as it does not refer at all to data protection or entail any reference at all to the concept of risk or to the risk-based approach. These limitations can and will be overcome by highlighting the difference between the notion of 'privacy and 'data protection' within the EU and US legal framework and by complementing the notion of 'harm' with the 'risk' and 'risk based approach' concepts of the GDPR. Moreover, Solove's taxonomy helps to create a better categorization of the FRS risks. But, this categorization, again, has its boundaries. The identification, insecurity and aggregation harms are not the same with the data protection risks depicted in the GDPR. Identification, under Solove's interpretation, refers, only, to 'the identification of persons in flesh' whereas the new GDPR is complementing this concept through the adoption of the 'identifiability' notion.

The 'identifiability' concept will be analyzed in chapter 4. 'Aggregation harms' are not the equivalent to 'profiling' concept under the GDPR. In addition, the 'insecurity' harms categorization, as defined by Solove, has limits, since this classification, dates from more than decade ago. Security lapses and risks have diversified over time.

In this chapter, after the limitations of Solove's taxonomy are explain, the FRS risks will be described. By taking into account the FRS state of the art, respectively, the technologies that have been described in the previous chapter (automated facial recognition in commercial retail store, FRS as means of authentication/verification in banking and the FRS used in social network sites) the following risks will be considered: identification, security and profiling risks of the FRS. The decision to focus on these particular risks follows naturally the fact these are the most notable risks identified.

---

[136] See footnote 33. Solove Daniel (2006).

[137] Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010 (hereinafter **EU Charter**).Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12010P&from=LV –last accessed 23 August 2017.

[138] Ibid.

3.2 Solove's taxonomy of 'privacy harms' and their limitation.

The typologies of privacy harms and their limitation pose a paramount role in the further description of the FRS risks. Privacy harms represent a vital but an 'under-theorized aspect of an important use.'[139] In consequence, an understanding of the mechanism and its purpose is more than necessary for the sake of theoretical transparency.

For instance, among all the privacy classifications, one leading privacy scholar has examined the likelihood and utility in defining the privacy concept and privacy harms. In the successions of his books and well-known articles, Daniel Solove abandons the attempt to define the concept of privacy by concluding that the 'notion of privacy cannot or should not be reduced to any one, or even multiple concept(s).[140] In Solove's vision, all earlier efforts have erred by being under or over-inclusive.[141] Therefore, despite for a definition, he advanced a 'taxonomy' of similar but different activities that are the source of privacy issues.[142] Solove's 'taxonomy', as a mean of classification "accounts for privacy problems that have achieved a significant degree of social recognition."[143] Solove is apprehending "the types of privacy problems that are addressed in various discussions about privacy, laws, cases, constitutions, guidelines, and other sources."[144]

But Solove's taxonomy of 'privacy harms' has its limitations. Firstly, the limitation that there is a striking difference in the understanding and application between the US and EU legal framework in regards with the notion of privacy (under US legal framework) and the "right to respect for private life" and data protection in the EU. Whilst, data protection (**article 8 of the EU Charter**)[145] and the 'right to respect for private and family life' (**Article 7 of the EU Charter**)[146] are fundamental rights in the EU, the assessment and protection of these right is different in the US.

3.2.1 The different understanding of privacy and data protection in EU and US.

The notion of privacy is, in particular, difficult to apprehend. The concept has been depicted in multiple ways as being far too vague in order to guide adjudication and lawmaking.[147] As a concept, 'privacy' is

[139]Calo M, 'The Boundaries of Privacy Harm ' [2011] 86(1) Indiana Law Journal p. 1132-1161.Available at http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf -last accessed 23 of August 2017.
[140] See footnote 33. Solove Daniel (2006).
[141] See footnote 139. Calo M. (2011).
[142] Ibid
[143] Solove Daniel, Understanding Privacy (1 edn. Cambridge: Harvard University Press 2008).p. 101-102. Available at http://www.hup.harvard.edu/catalog.php?isbn=9780674035072 –last accessed 26 of August.2017.
[144] Ibid.
[145] Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010 (hereinafter **EU Charter**)
[146] Ibid.
[147] See footnote 33. Solove Daniel (2006).

prone to 'definitional instability'[148] or 'in disarray.'[149] Insofar, different scholars have expounded different models, indicating 'multiple clusters of meaning surrounding the word.'[150] Fuster has indistinctively defined that the legal notion of 'privacy' is connected with the 'private in the way of individual, personal one's own life.'[151] Historically, the concept was connected with the idea of freedom.[152] In this respect, the concept of privacy was associated with the individuals and enforced the right of the individuals to select the life they want to live. This freedom of choice is, however, in opposition to the controlled life of individuals or their alienation from themselves or society. Additionally, the concept has been linked with the notion of human dignity.

The unitary concept of the right to privacy in the comparative constitutional law field was settled more lately.[153] Under international law, by 1948 the Universal Declaration of Human Rights **(hereinafter UDHR)** under article 12 has distinctively delineated the right to privacy. The UDHR states that "no one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks to his honor or reputation."[154]

Conversely, under the European legal framework, the Convention for the Protection of Human Rights and Fundamental Freedoms (**ECHR**)[155] under article 8(1) foresees that "everyone has the right to respect for his private and family life, his home and his correspondence."[156] In addition, Charter of the Fundamental Rights of the European Union **(EU Charter)**, proclaimed and published by 2000[157], includes the explicit right of respect to privacy under article 7 in a similar way: "everyone has the right to respect for his private and family life, home and communications."

Up to now, in parallel with ECHR, the European Court of Human Rights **(ECtHR)** has developed a substantial impact in ensuring a better legal understanding of the right to privacy in Europe. However, the Court has steadily circumvented the usage of the word 'privacy', when refers to any of the rights protected by article

[148] Bygrave Lee, 'Privacy and Data protection in an international perspective ' [2010] 56(1) Scandinavian Studies in Law 165-200. Available at https://pdfs.semanticscholar.org/695f/434a1111f254c2c3104811f4851324b1de35.pdf -last accessed 23 of August 2017.

[149] See footnote 143. Solove Daniel (2008).

[150] Fuster Gloria Gonzalez, The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer: Law Governance and technology Series 2014) 21. Available at http://www.springer.com/gp/book/9783319050225 -last accessed 26 of August 2017.

[151] Ibid.

[152] Koops Bert-Jaap and others, 'A Typology of Privacy' [2016] 38(1) University of Pennsylvania Journal International law. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043 -last accessed 22 March 2017.

[153] Ibid.

[154] Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).Available at http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf -last accessed 30 of July 2017.

[155] Council of Europe, ETS no. 005, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, 4 November 1950. Available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 -last accessed 30 of July 2017

[156] Ibid

[157] EU Charter of Human Rights, O.J. C 364, 18 December 2000.Available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf -last accessed 7of September 2017.

8 ECHR.[158] The Court refers to the 'reasonable expectance of privacy' that comes from the US.[159] Nevertheless, the right to respect of one's private life is not an absolute right. Therefore, any interference of the FRS with the right to privacy should be in accordance with Article 8(2) of the ECHR. The interference shall be adequately based in accordance with the law, in a clear and comprehensible way, pursuing a legitimate way and any interference should be 'necessary in a democratic society.'[160]

Whilst the right to respect privacy is already acknowledged for a long time as a human right, the acknowledgement of the right to data protection as a fundamental right is by far more new. In the EU, the right to data protection was recognized by 2000, under article 8 of the EU Charter. After the proclamation of the right on the basis of Article 8, the literature gradually started to recognize the existence of an independent right.[161] The existence of the concept of 'privacy' and 'data protection' were "nevertheless closely related" and "this tight relationship between privacy and personal data protection has been described in the manner of a partial overlap."[162] Under traditional approach, data protection was regarded as a part of the broader right to respect for private life whereas under the modern approach the right to personal data represents a consequence of the widening of the right to privacy.[163]

However, in the new GDPR[164], the concept of an EU personal data protection right was not mentioned in connection with the right to privacy.[165] The new General Data Protection Regulation, in extension (that will be discussed under the following chapter) will replace the current Directive 95/46/EC by entering into force by 25 of May 2018.[166] The biggest effect that the GDPR will bring is that it has direct legal effect and it does not to have to be implemented in the national legislation of the Member States. In this sense, along with the introduction of the GDPR, the right to data protection is regulated at the highest level possible. 'The new GDPR must be regarded as an implementation of the right to data protection: Article 8(1) of the EU charter and Article 16 of the TFEU'[167]

Whilst, the right to data protection and privacy is highly regulated in the European legal framework, having the statute of fundamental rights, data privacy has not a similar statute in the US. Historically, the privacy regulation was rooted on the industry self-regulation, 'a laissez- faire governance where markets, industry

[158] See footnote 150.Fuster (2014).
[159] Ibid.
[160] Council of Europe, ETS no. 005, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, 4 November 1950. Available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 -last accessed 7 of September 2017.
[161] See footnote 150.Fuster (2014).
[162] Ibid.
[163] Rodotà S. (2009) Data Protection as a Fundamental Right. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht. Available at https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_3 -last accessed 23 of August 2017
[164] See footnote 8. The GDPR.
[165] Ibid.
[166] See article 99 para. 2 GDPR.
[167] Fuster Gloria Gonzales and Raphael Gellert, 'The fundamental right of data protection in the European Union: in search of an uncharted right' [2012] 26(1) International Review of Law, Computers & Technology 73-82.Available at http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.646798 -last accessed 23 of August 2017.

agenda, and governments intervene only when the private sector fails.'[168] There are a multitude of sources of privacy law in the US, entailing laws and regulations that are enforced by federal and state authorities.[169] The privacy concept has progressively developed as a 'part of common law across the US and helped to shape the idea that privacy is a commodity and essentially a tool against the government.'[170] But unlike the EU, there is no single overarching privacy law. The US does not entail a single dedicated data protection law.[171] The concepts of personal data varies in accordance with the underlying law or regulation.[172] Moreover, Solove's approach is narrow in the sense that it is only concerns 'privacy harms' and it does not make any reference to data protection, whereas the new GDPR refers exclusively to the data protection concept.

In the next section, Solove's taxonomy of 'privacy harms' will be presented. As the new GDPR is approaching, besides the minimum and non-negotiable level of protection 'risk-based approach', one that will be depicted under the following chapter, it will be more than useful that a link between the notion of 'harm' and 'risk' should first be assessed.

3.2.2 Harms and risks.

The privacy concept is regarded as an umbrella term and it is better to focus on the activities that create the privacy harms.[173] In this sense, Solove widely recognizes the 'four basic groups of harmful activities' involving information: **collection** (surveillance; interrogation); **processing** (aggregation; identification; insecurity; secondary use exclusion); **dissemination** (breach of confidentiality; disclosure; exposure; increased accessibility; blackmail; appropriation; distortion); and **invasion** (intrusion; decisional interference).

Firstly, Solove is referring to the information collection activities. This process emphasizes the harmful activities that may occur in regards with the collection of information about the data subjects. However, not all the information that is collected should be regarded as harmful activity to the individuals.[174] Secondly, after the collection of the information, the "data holder" may perform information processing activities. In this process the holder of the data might undertake processing operations in the form of

[168] Farrel Henry, 'Constructing the International Foundations of E-Commerce—The EU-US Safe Harbor Arrangement' [2003] 57(1) International Organization <DOI: 10+10170S0020818303572022> accessed 17 August 2017. Available http://www.henryfarrell.net/IO.pdf -last accessed 23 of August

[169] Jay P Rosemary, 'Data protection and Privacy in 31 jurisdiction wordwide' (Hunton and Williams, 2015). Available at https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf -last accessed 3 August 2017.

[170] Movius L and Krup N, 'US and EU Privacy Policy: Comparison of Regulatory Approaches [2009] (3) International Journal of Communication 169-187. Available at http://ijoc.org/index.php/ijoc/article/viewFile/405/305..- last accessed 15 of August 2017.

[171] See footnote 169. Jay P Rosemary (2015).

[172] Ibid.

[173] See footnote 33. Solove Daniel (2006).

[174] Ibid.

"storing, combining, manipulating, searching or usage of the data"[175] that have been previously collected. Thirdly, the information dissemination process has been highlighted. In this course, Solove is emphasizing the harms that may appear in the transmission of the data from one holder to another or the harms that may appear in releasing the information. In the end, the invasion of harmful activities is mentioned. These activities involve invasion into the individual's private matters and do not always include personal information.[176]

In this thesis, only the second group of activities will be discussed, the information processing harmful activities of the FRS and the manner how the information is stored, manipulated and used by the FRS. In this respect, Solove is making a categorization between: **aggregation, identification, insecurity, secondary purposes and exclusion.** However, taking into account the previous chapter only: identification, insecurity and aggregation harmful activities will form the basis of the analysis of the actual chapter.

On the other hand, Solove's classification has limits. What happens if 'someone' has different views on these sources?[177] Simple similarity with this categorization of other privacy harms is not enough.

Moreover, the relation between privacy harms and risks should be delineated. The characterization of the privacy harms is not an easy assignment. But taking into consideration Solove's description, De Sourya Joyee and Le Metayer describe privacy **harms** as "the negative impact of the use of a processing system on a data subject, or a group of data subjects, or society as a whole, from the standpoint of physical, mental, financial or well-being reputation, dignity, freedom, acceptance in society…"[178]

However, Solove is highlighting only the harms and not at all the risks. Therefore, an understanding of the concept of 'risk' is more than necessary.

To begin with, there is no integrated explanation of **risk**, and "the most common uses are: risk as a hazard, as probability, as consequence, and as potential adversity or threat."[179]

In a general manner, the concept of risk can be determined as a 'tool for decision-making that allows the transformation of the uncertain in certain.'[180] The risk can be demarcated as an 'event that has a certain severity, a number of probabilities of occurrence and as well as a number of consequences.'[181] According

---

[175] Ibid.

[176] Ibid.

[177] See footnote 139.Calo M. (2011).

[178] De SJ and Daniel Le Metayer, Privacy Risk Analysis (Morgan & Claypool Publishers 2016) 7. Available at http://www.morganclaypool.com/doi/pdf/10.2200/S00724ED1V01Y201607SPT017 -last accessed 26 of August 2017.

[179] Slovic Paul and Elke U. Weber, Perception of Risk Posed by Extreme Events Center for Decision Sciences, (CDS) Working Paper Columbia University, (2002), 4. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2293086 –last accessed 23 August 2017.

[180] Bernstein P., Against the Gods - The Remarkable Story of Risk (1996) 3. See Also Gellert R, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the... European Data Protection Law Review (EDPL), 4/2016, Vol. 2. Available at https://www.researchgate.net/publication/312652929 last accessed 10 of July 2017.

[181] Gellert R., 'Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing'' [2017] 1(1) Trends and Communities of legal informatics: IRIS2017 - Proceedings of the 20th International Legal Informatics Symposium Schweighofer, E, Kummer, F & Sorge, C (eds) Austrian Computer Society 527-532.

to Bernstein, two different mechanisms are embedded in the risk analysis: 'forecasting the future (through statistics and probabilities) and constructing outcomes on the roots of it.'[182] In this respect, any decision in relation with the risk entails two distinct elements: 'the objective facts and the subjective view (of the desirability of what is to be gained or lost through the respective decision)'[183] Slovic claims that the risk concept 'in his tradition is inherently' subjective.'[184] Since there is no 'real risk' or 'objective risks', subjective 'conclusions are involved at every stage of the assessment process, from the initial structuring of a risk problem to deciding which endpoints or consequences to include in the analysis.'[185] However, the likelihoods and outcomes are rooted in risk-assessment communities.[186] The public opinion bear a paramount role in the analysis of the risk, by 'adding issues of values, process, power and trust towards to the quantification issues considered by the risks-assessment professionals.'[187]

The main goal of the risk- analysis is: i) to assess the risks ii) to take a decision – to manage the risks.[188]

In regards with the risk-management Kuner et.al. reminds that 'the goal of risk management is not to eliminate risk, but to reduce the risk as fully as practical and to be explicit about the remaining risks and how they will be managed.'[189] In addition, risk-management provides 'exponential benefits for the data protection application, managing scant resources where they are necessary and ensures protection of the fundamental rights of the individuals in an effective and appropriate way.'[190]

Since the GDPR is adopting, besides the data protection principles, a risk-based approach and Solove's taxonomy of 'privacy harms' is under-inclusive (as it does not refer to risks at all), the understanding of the concepts of *harms, risks and risks-based approach* is more than important. In this thesis the reference will be to the risks and not to harms, under the following part of it. The concept of harm is used only to understand Solove's taxonomy and its limits.

Available at https://www.researchgate.net/publication/314839054_Why_the_GDPR_risk-based_approach_is_about_compliance_risk_and_why_it's_not_a_bad_thing -last accessed 25 of August 2017.

[182] Ibid

[183] See footnote 181.Bernstein (1996). See also R Gellert,'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection' [2016] 4(2) European Data Protection Law Review (EDPL) 481-492. Available at https://www.researchgate.net/publication/312652929_We_Have_Always_Managed_Risks_in_Data_Protection_Law_Understanding_the_Similarities_and_Differences_Between_the_Rights-Based_and_the_Risk-Based_Approaches_to_Data_Protection - last accessed 10 of July 2017.

[184] Slovic Paul and Elke U. Weber, Perception of Risk Posed by Extreme Events Center for Decision Sciences, (CDS) Working Paper Columbia University, (2002), 4. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2293086 –last accessed 23 August 2017.

[185] Ibid.

[186] Ibid.

[187] Slovic Paul.,'Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield.'In M H Bazerman, D M Messick, A E Tenbrunsel, & K A Wade-Benzoni (Eds), Environment, ethics, and behavior (pp 277-313) San Francisco: New Lexington' [1999] 19(4) 689-701. Available at https://www.ncbi.nlm.nih.gov/pubmed/10765431 -last accessed 25 of August 2017.

[188] Ibid

[189] Kuner Cristopher and others , Risk management in data protection, International Data Privacy Law, Vol. 5, No. 2, (2015), 95. Available at https://academic.oup.com/idpl/article/5/2/95/645238/Risk-management-in-data-protection -last accessed 23 of August 2015.

[190] Ibid.

In the following section, having the information processing harmful activities categorization (aggregation, identification, insecurity, secondary purposes usages and exclusion), as a starting point, FRS risks will be described. Taking into account the features and the risks that their usages may impinge to the individuals, in the next sections only aggregation, identification and insecurity will be highlighted. The categories of secondary purposes usages and exclusion will be indirectly embodied in the first three categories. However, as discussed, Solove's categorization has limits as it applies only to privacy harms and not to the risk and refers only to privacy concepts and not to data protection. The GDPR provisions are mentioned, in this chapter, only for a better understanding of the differences between Solove's 'privacy harms' and data protection risks. For example, aggregation is not the same as profiling under the GDPR and the identifiability is a particular concept of the new GDPR. By taking into account the FRS state of the art, respectively, the technologies that have been described in the previous chapter (automated facial recognition in commercial retail store, FRS as means of authentication/verification in the banking sector and the FRS used in the social network sites), the following risks will be considered: identification, security and profiling risks of the FRS.

3.3 Identification risks of FRS.

To begin with, according to Solove's taxonomy, identification is defined as a result of information processing activities by the data holder. In simple words, identification represents the process of linking information to the individuals. The identification is somehow comparable to the aggregation (as it is explained hereinafter in this chapter) as both processes involve different arrangements of information, from which at least one involves the identity of the individuals. The difference is that the identification has the effect of direct identification of the individuals, or how Solove claims: "the identification of a person in flesh."[191] But this classification has its own limits as the new GDPR acknowledges four levels of identifiability[192] of the persons that are referred to: (1) identified (2) identifiable (3) de-identified and (4) anonymous data.

Identifiable data is specific to an individual whose identity is not obvious from the data. Data is not directly linked with other data that identifies the individuals. However, 'there is a known systematic method to reliably create or re-create the link with identifying data.'[193] Pseudonymous data is a subcategory of identifiable data.

In addition, Article 11 of the GDPR referrers to de-identified data or 'the data could potentially be re-identified if matched to additional identifying data provided by the data subject, but there is no known, systematic way for the controller to reliably create or re-create a link with identifying data.'[194] Finally,

[191] Ibid

[192] Mike Hintze, 'Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency' [2017] Hintze Law PLLC; University of Washington School of Law 1. Available at https://fpf.org/wp-content/uploads/2016/11/M-Hintze-GDPR-Through-the-De-Identification-Lens-31-Oct-2016-002.pdf -last accessed 18 of August 2017.

[193] Ibid. See Article 4 (1) GDPR

[194] Ibid.

anonymous data in Recital 26 GDPR refers to the data that are 'stored without any identifiers or other data that could identify the individual or device to whom the data relates; and aggregated with data about enough individuals such that it does not contain individual-level entries or events linkable to a specific person.' [195] Anonymization should be irreversible and should ensure that the individuals cannot be identified by any means or by any person.

Faces are specifically suitable for the identification of persons as they attain distinctiveness and in the majority of the cases are particular visible.[196] However, the people can continue to be anonymous in public since a restricted number of acquaintances may recognize them. But with the new developments in FRS and their usages in social network sites and applications this hypothesis will be likely to be changed. The FRS can link an image of the face not only to a specific name but to the whole available personal information which is present on the social networks site profile. Nowadays, substantial volumes of identified and unidentified facial data have become accessible via WEB 2.0 applications. Since the FRS infrastructure is available, FRS might navigate in real time across these already available data, with the aim to match this pre-available images with the persons through the on-line facilities without the person consent or even knowledge. [197] The Facebook photo tag suggest might reveal all of the personal information on a user profile, as it links the facial features of a newly uploaded photo to the user's SNS profile through a hyperlink. Therefore, when an image is uploaded the users might 'manually tag a person in the uploaded photo by marking a square around the person's face and to provide the person's name.'[198] The profile that is hyperlinked entails sensitive information like 'gender, birthday, political beliefs or any other status updates.'[199] Nevertheless, the uploaded photos on the SNS may reveal specific metadata like the 'the time, date or the user's physical location.' [200]

In a brief presentation, FRS metadata refers to any data that is linked with the FRS. FRS metadata might be separated into different categories: the ones that result from the system set-up used by the system administrators and the ones that result through the actual usage of the metadata by the FRS users.[201] The metadata field can be identified in the form of a: 'pick list (is a specific list of selections that define a discrete set of options- such as male assigned as M, and females as F), a numerical value (as height or weight), the dates, a derived value (such as classification within groups e.g. male 20-40 years).[202]

In addition, metadata might be formed at the moment of enrollment (whenever the data is analyzed, sorted, transformed and prepared for enrollment) or the moment of filtering in the pre-existent

[195] See footnote 192.Mike Hintze (2017).
[196] See footnote 30. Wellinder (2012)
[197] See footnote 124. Acquisti et.al. (2014)
[198] E. A. Vander Veer, FACEBOOK: THE MISSING MANUAL 13–14 (Dawn Mann and Nellie McKesson eds., 3rd ed. 2011).
[199]See footnote 30. Welinder (2012).
[200] Ibid.
[201]Fiswg, 'MetadataUsage' [2014] 1(1) FISWG. Available at https://fiswg.org/FISWG_Metadata_FR_Systems20140509.pdf -last accessed 1 August2017.
[202] Ibid.

database.[203] Nevertheless, in the case of processing of images in the online environment two types of metadata are created: embedded metadata and social metadata.[204] The first, embedded meta-data is created within the header of the image in the moment when the image is captured and they include: geolocation (such as location coordinates), timestamps, free-form text and copyright information. In the case of geolocation metadata, location coordinates might enable the SNS to establish the captured location whereas on the basis of timestamps it might be concluded that the images are related to the same event.[205] Free-form text might be used by the SNS to identify images that are related. Furthermore, social metadata is generated when the users of SNS are uploading and sharing images using a social network site or photo sharing service. Behavior-based social metadata are strictly connected to the user's photo upload methods or the user's frequency of interactions with particular SNS contacts.'[206]

In relation to the FRS metadata, as revealed through the Queens University of Belfast Research, held in 2017, a 'mixture of facial recognition systems and a phone MAC address tracking for authorizing access to Wi-Fi' might be used. In this sense, the Wi-Fi systems require a picture of the user's face necessary to allow the user to join the Wi-Fi network. For example, when the user is joining for the first time the network, this is linked to the MAC address (a unique identifier of the user's phone) of the device. As the image and the MAC address are deposited in the device, the face of the user must match with the initial apprehension, at the time when the further admission is endeavored.[207] Therefore, whenever the user is coming back to the place where they already used the Wi-Fi network and they demand for access, the system will be likely to verify the new captured face to the already captured one, and whether the stored MAC address is in alignment with the MAC of the user device. In this sense, the access to the Wi-Fi network will be guaranteed.[208] In consequence, these systems have the power to track users in an environment via their MAC address. Individuals can also be tracked via their facial image.
In addition social metadata is generated when the users of social network sites that are uploading and sharing images using a SNS or photo sharing service.

Furthermore, a Carnegie Mellon University (CMU) privacy research has revealed that through the combination of the WEB 2.0 data (images) and the FRS available at large scale it might be possible to re-identify users.[209] The experiment included both on-line and of-line re-identification, and has revealed sensitive information about individuals. The researchers used photos that were publicly available on SNS (in Facebook without being logged-in). The research revealed the re-identification of the individuals by a

[203] Ibid.
[204] Novetta Whitepaper, "Opportunities in Analyzing and Processing Online Face Images", August 2016. Available at http://www.novetta.com/wp-content/uploads/2016/09/NovettaBiometrics_OnlineFaceProcessing_WP-W_9112016.pdf -last accessed 11 of July 2017.
[205] Ibid.
[206] Ibid.
[207] Millar Stephen, 'Privacy Impact Assessment (PIA) - BioConnect: combining facial recognition and MAC address tracking for authorising access to Wi-Fi' [2016] Queen's University Belfast. Available at http://pure.qub.ac.uk/portal/files/123692281/StuartMillar_13616005_PIA.pdf%20p.3 - last accessed 1 August 2017.
[208] Ibid.
[209] See footnote 124. Acquisti et.al. (2014).

simple combination of the SNS data with the publicly available FRS.[210] Through this combination at least one of-three scanned individuals was identified in a matter of seconds. Even persons that did not possess a SNS profile were identified as being tagged in their friend's photo.[211] Various scientific works have been also demonstrated that 'a face can be reconstructed from the templates of the images and this reconstruction and identification is sufficient to obtain a positive image that sometimes is higher than 90% accuracy.[212]

Moreover, a risk of misidentification, due to the potential human error tagging is possible to occur. Specific activities will be accredited to the wrong users and in consequence a hyperlink to a misidentified profile end-user will be generated.[213]

Nevertheless, the FRS used in commercial retail are also posing identification risks. To make it simpler, a practical example of the FRS usages in a clothing store will be presented. In a hypothetical example a customer was registered after the first visit in the store under the store's software. At the next visit, the FRS will be able to identify the customer, their preferences, how many times he/she visited the store and to track the customer around the store.[214]

But how does the identification work in practice in the case of FRS used in commercial retail? Generally, every AFRS starts with,[215] an examination of the 'training images' of previously acknowledged individuals and a measurement of their facial characteristics.[216] These unique face features are deposited in a biometric database. In addition, other distinguished information about them is stored in the database. Secondly FRS technology will be applied to a newly acquired image of the customer. Firstly, there is the face detection stage, followed by feature extraction and normalization. The technology, finally, identifies and measures the biometric features in the normalized face and in the end compares it with the pre-existing database. The scenario presented above is simple: the digital signage technologies possess the ability to re-identify the customers that 'were seen in a time slot.' The only information necessary to perform this process is the customer's face. Complementary to these risks, profiling and behavioral on and offline advertising might occur.

[210] See footnote 30. Welinder (2012).
[211] See footnote 124. Aquisti et.al. (2014).
[212] See Section 2.6.1 and Michel Chiba and Alex Stoianov, 'On Uniqueness of Facial Recognition Templates' [2014] 1(1) Information and Privacy Commissioner's Office of Ontario, Canada. Available at https://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf -last accessed 1 August 2017.
[213] Ibid.
[214] See footnote 14.Lewinski et.al. (2016).
[215] Viola, P. and Jones, M., 2004. Robust Real-time Face Detection. International Journal of Computer Vision 57(2), 137–154. Available at http://www.vision.caltech.edu/html-files/EE148-2005-Spring/pprs/viola04ijcv.pdf -last accessed 23 of August 2017.
[216] See footnote 30. Welinder (2012).

To conclude, facial recognition systems are imposing 'identification' risks towards the individuals. In the absence of facial recognition systems, 'a stranger seeking to easily identify an individual would need more information than a simple facial feature.'[217]

In this respect, few individuals may expect, that by exposing their faces on public, other passerby or companies in retail business will be likely to recognize their faces and to affix a name to them. Therefore, data protection risks of identification are higher.

3.4 Security risks for FRS.

Solove is underlining that identity theft is 'the fastest growing white collar crime.'[218] In addition, "glitches, security lapses, abuses, and illicit uses of personal in-formation all fall into this category."[219] Thus, 'security' is an issue triggered by the way our information is handled and protected. Although, Solove's classification has its own limits as it dates from almost a decade ago. Moreover, FRS have acknowledged a high pace of development. In consequence, the security lapses and abuses have been diversified as well. Security breaches are more prone to occur during the data transit in the case of online and mobile FRS. For example, in the case of 'uploading an image from a camera to a website for feature extraction and comparison[220] Security breaches might appear in the case of identification and authentication/verification purposes, since 'FRS for identification and authentication/verification are likely to require the storage of the template for use in a later comparison 'but also in the case of data transit in the on-line and mobile devices.'[221]

On the one hand, despite the high accuracy of the FRS for the authentication and verification purposes Duc and Minh[222] have demonstrated that sophisticated FRS might be by-passed in an easy way by only presenting fake photographs to the software. Even-though FRS authentication technologies have recently developed, by implementing 'robust- face authentication protocols.'[223] This security measures still have a lot to be improved. For example, as an additional protection for the image-spoofing counter-attacks, financial institutions[224] have implemented blinking authentication measures. Although, it has been demonstrated that little protection was fulfilled since the FRS were by-passed by only presenting two

[217] CDT Comments on the Federal Trade Commission's,'Seeing Is ID'ing: Facial recognition and Privacy', facial recognition forum 8 December 2011, published 22 January 2012. Available at https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf -last accessed 14 of July 2017.

[218] See footnote 33. Solove (2006)

[219] Ibid.

[220] Article 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

[221] Ibid

[222] See footnote 120. Duc Nguyen and Buy Minh (2009).

[223] See footnote 23. Xu Yi et.al. (2016).

[224] Vincent James, MasterCard unveils 'selfie' security checks, says heartbeat authentication could follow", The Verge, 23 February 2016. Available at http://www.theverge.com/2016/2/23/11098540/mastercard-facial-recognition-heartbeat-security -last accessed 25 March 2017.

simple images- one with an eye-closed and the other with an eye-opened.[225] In the specialized literature there is a distinction within two types of attacks against the FRS: a so-called Hill Climbing attack (an attack that starts with an impostor image that runs against the template) and the Break-In set Attack (through reconstruction of the image).[226]

Usually three methods of spoofing attacks are commonly used against the FRS: image-spoofing; video-spoofing; and 3D-mask spoofing. An image of the person's that was initially authenticated, a pre-recorded video of the victim or a 3D-masked printed[227] are the mutual method of hacking the live FRS.

A29 WP Opinion[228] 2/2012 is highlighting the risks of security breaches that may occur during the transit and data storage of facial features. Specific recommendation as local processing, usages of cryptographic key or other encryption techniques are also delivered, in order that 'untraceable biometrics' to be created.[229] Therefore, it seems that it would be more difficult for hackers to access and use the facial features of the individuals. But the risks may be higher than they look. For example, if the data holders will not endeavor a reasonable effort in securing the data, the risk will be that once "the biometric data is stolen it is stolen forever."[230] A concern is the growing peril of the 'virtual reality and computer vision as an adversarial tool that may be used against FRS.'[231] In this respect, in the Usenix Conference, held in 2016, it was determined that: 'designers of face authentication systems have usually assumed a rather weak adversarial model wherein attackers may have limited technical skills and be limited to inexpensive materials.'[232] This approach is risky, at best.

To conclude, the security risks are higher and higher. Due to the uniqueness and persistency characteristics of the facial features, the impact of the security breaches or spoofing attacks will be, by any doubt, way complex.

[225] See footnote 23.Xu Yi et.al. (2016).

[225] See footnote 224.Vincent James (2016).

[226] Chibba Michelle and Alex Stoianov, 'On Uniqueness of Facial Recognition Templates' [2014] 1(1) NTIA US Department of Commerce Privacy Multi-stakeholder Process: Facial Recognition Technology. Available at https://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf -last accessed 1 August 2017.

[227] N. Erdogmus and S. Marcel. Spoofing face recognition with 3d masks. Information Forensics and Security, IEEE Transactions. Available at https://www.researchgate.net/publication/262605045_Spoofing_Face_Recognition_With_3D_Masks -last accessed 20 Of July 2017

[228] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf -last accessed 29 of July 2017.

[229] Ibid

[230] Allison Grande, 'Amazon's Execution Key To Dodging 'Selfie Pay' Woes' (Law 360, May 2016). Available at https://www.law360.com/articles/773543/amazon-s-execution-key-to-dodging-selfie-pay-woes last accessed 3 August 2017.

[231] See footnote 23. Xu Yi et.al. (2016).

[232] Ibid.

3.5. FRS profiling risks.

Under Solove's approach, aggregation is the process of collecting data about individuals.[233] A mere or simple part of information will not be sufficient to reveal a portrait of an individual. But by gathering small pieces of information, "the whole may become greater than the parts."[234] Through this way, new details about individuals, ones that would not have been expected to be acknowledged by looking only to the small picture, may be revealed. Solove emphasizes that the profile that is created by the aggregation of the data will be likely to be used against that person in a judgmental and negative way. Thus, the aggregation may enhance the 'power' that the aggregator will be likely to have over the others that are profiled. However Solove's approach has limitations. Solove's approach does not mention anywhere the decision-making factor' (which is specific to the GDPR) and it only represents a starting point in our discussion. In contrast, the GDPR in recital 71 defines **profiling** as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behavior, location or movement." Kindt defines biometric profiling as a 'use, by automatic means, of biometric characteristics, whether biological or behavioral characteristics, whether unique for a given individual or not, for extracting and applying (group) profiles to individuals."[235]

Furthermore, the A29 WP Party Opinion is revealing the potential risks of profiling of FRS. In this sense, FRS may be used even if there is no information about 'the real-world identity of the individuals.'[236] In addition, the same Opinion reminds about the profiling risks that FRS may impose in the commercial and retail area. An automated facial recognition system may be able in the 'shopping experiences to track the routes and habits of the customers and along with this particular ability emerges also the capability of profiling and to deliver targeted advertising to the customers.[237]
In the commercial retail, FRS are developed to perceive 'emotions, attentions and different psychological states 'through the means of a face modeling.'[238] In the first stage is the extraction of the face features. After that a 'compression is used to reduce the dimensionality' (or the normalization phase). Finally, the

[233] Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP19. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf -last accessed 29th of July 2017
[234] Ibid.
[235] Hildebrandt M and Serge Gurtwirth, 'Profiling the European Citizen, Springer (2008). Available at http://www.springer.com/gp/book/9781402069130 -last accessed 26 of August 2017.
[236] Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193. Available at Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf -last accessed 29th of July 2017.
[237] Ibid.
[238] Cootes, T., & Taylor, C. (2000). Statistical models of appearance for computer vision. Technical report, University of Manchester, Wolfson Image Analysis Unit, Imaging Science and Biomedical Engineering. University of Manchester. Available at http://www.face-rec.org/algorithms/AAM/app_models.pdf -last accessed 17 of July 2017.

FRS analyze the individual psychological features.'[239] FRS is allowing the identification of the individuals and the software is processing personal data. Along with the identification purposes, FRS is enabling this software to create a profile and a categorization of the consumers based on their emotions or other socio-demographic features. The FRS is used in the commercial retail for understanding behavior and for influencing the behavior of the customers by creating different layers of market segmentation.

In consequence, a complete emotional and personalized profile of the customers is created[240] and various advertisements will be displayed. AFRS will also enable to provide digital content to the customers on-line.[241] In addition, by linking the AFRS with other databases or social networking sites, these companies will be capable to target individuals in accordance to their particular needs. AFRS can identify individuals and match a new captured photo of an individual with a pre-existent Facebook photo of SNS user. In this sense, the individual's 'image' will become complete. The separate bits of information could be gathered to obtain a detailed image of the individual, like friendships, habits and tastes.[242]

Profiling and non-distributive group profiling, as a consequence of the FRS, can have a negative consequence and may conclude to misrepresentation of the individuals. Many companies are already focusing on creating 'bad faces' databases – people that may be identified, for heightened scrutiny.[243] Moreover, as a result of automatic tagging systems used by social networking companies, like Facebook on-line behavioral profiling can occur. Profiling may have negative impact on the users. User's denial to a service or a product and discrimination between this users that are enrolled in different databases is common practice.[244]

3.6 Conclusion.

First, in this chapter, Solove's 'taxonomy of privacy harms' has been chosen in order to reveal the different levels of acknowledgement and applications of the US and EU legal framework regarding the notion of privacy (US), the "right to respect for private life" respective data protection in the EU. Unlike the EU, in the US legal framework, there is not a single overarching privacy law or a single dedicated data protection law. [245] Whilst, the right to data protection and privacy is highly regulated in the European Legal framework, having the statute of fundamental rights, data protection and privacy has not a similar statute in the US. However, as it will be revealed in the next chapter, where a separation between the concept of privacy and data protection is ascertained, in the EU, data protection rules have been gradually disconnected to the right to privacy and the European Court of Justice has elevated all data protection rules to the level of 'fundamental rights.'[246] The new GDPR must be regarded as an implementation of the

[239] See footnote 14. Lewinski et.al. (2016)
[240] Ibid.
[241] See footnote 14. Lewinski et al. (2016).
[242] See footnote 16. Mathew Wall (2015).
[243]Kashmir Hill, You are secretly tracked with facial recognition even in church June 2015, Fusion net Available at http://fusion.net/story/154199/facial-recognition-no-rules/ -last accessed 18 of March 2017.
[244] See footnote 19. Stacy Gray (2009).
[245] See footnote 169.Jay P Rosemary (2015).
[246] Ibid.

right to data protection.[247] Solove's taxonomy is under-inclusive as it entails only 'privacy harms', and does not make any reference to the concept of risk or to the risk-based approach. Therefore, these limitations of Solove's taxonomy have been overcome by highlighting and supplementing the concept of 'harms' with the notions of 'risk' and 'risk-based' approach. The acknowledgment of the concepts of 'risk' and the 'risk-based approach' is very important, since the GDPR is adopting the 'risk-based' approach. However, as it is revealed in the chapter 4, the EU data protection legal framework is adopting partially the risk-based approach in the GDPR, meaning that the main principles of data protection are still rights-based approach.[248]

Furthermore, Solove's taxonomy helps to create a better categorization of the FRS risks. The following information processing harmful activities were used as a fundament for the analysis: identification, insecurity and aggregation. These harms have been complemented through a succinct presentation, of the identification, security and profiling risks (in alignment with the particular case of FRS). Firstly, in regards with the identification information processing harmful activity, Solove is referring to "the identification of persons in flesh" [249] whereas the GDPR has acknowledged different degrees of identifiability.[250] As to the FRS identification risks, it has been exposed that FRS possess the ability to link an image of the face not only to a specific name but to the whole available personal information which is present on the social network sites. Additionally, FRS metadata bear a paramount role in the increasing of the identification risks of the FRS. In this sense, a recent research experiment has revealed that the re-identification of the users of SNS is possible through the combination of the WEB 2.0 data (images) and the FRS available at large scales.[251] This experiment proved that the risks of re-identification was found very high as, even persons on the streets that did not have SNS have been identified.
Secondly, the security risks of the FRS were identified. Solove is mentioning the 'insecurity harms' such as identity theft and other 'glitches, security lapses, abuses, and illicit uses'. But, since a decade ago, this categorization has limitations. Security breaches and abuses have diversified as well. In the case of FRS, security breaches might occur both in the situation of the data storage and data transition. Furthermore, in spite of higher level of accuracy of the FRS, three kinds of spoofing attacks were identified: image-spoofing; video-spoofing; and 3D-mask spoofing. In this respect, there is a threat in the increasing power of the virtual reality and computer vision capabilities as adversarial tools and a continuous wrong assumption of the FRS designers and users that the attackers do not hold the necessary technical skills or the suitable materials for the attacks.

[247] Fuster Gloria Gonzales and Raphael Gellert, 'The fundamental right of data protection in the European Union: in search of an uncharted right' [2012] 26(1) International Review of Law, Computers & Technology 73-82.Available at http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.646798 -last accessed 23 of August 2017.
[248] R. Gellert, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the... European Data Protection Law Review (EDPL), 4/2016, Vol. 2, pp. 481-492. Available at https://www.researchgate.net/publication/312652929 last accessed 10 of July 2017.
[249] See footnote 33 Solove Daniel (2006).
[250]See footnote 192.Mike Hintze (2017).
[251] See footnote 124. Acquisti et.al (2014).

Thirdly, having as starting point the 'aggregation harms' profiling risks of the FRS were presented. According to Solove, aggregation is the process of collecting data about individuals. But, this definition has limits and it has been complemented through the introduction of the profiling concept.
In the commercial retail, through the creation of complete profiles, FRS enables the understanding and persuading the behavior of the customers that will be categorized under different levels of market segmentation. Knowing the identity of their customers enables the retailers to make an association and to observe the data of the customers from other sources (like online behavior). In consequence, tailored advertisements will be displayed, both offline and online.

The aim of this chapter is to complement and make suitable the US oriented taxonomy of Solove for the application to the GDPR, in respect with the following data protection risks of FRS: identification, security and profiling. These risks are assessed from the perspective of the GDPR in the following chapter.

CHAPTER 4.

Identification, security and profiling data protection risks under the GDPR.

4.1 Introduction.

After many years of debate and negotiation, the General Data Protection Regulation (hereinafter **GDPR**) has been finally adopted. The GDPR will replace the old Directive 95/46/EC (in accordance with Article 94 Para. 1) and will be directly applicable in all the Member States of the European Union starting on 25 May 2018 (Article 99 Para. 2 GDPR). Regardless of their place of residence, the organizations which collect and process personal data of EU citizens, will have to conform to the requirements imposed by the GDPR. If they do not, they will have to pay significant financial penalties and suffer reputation damage.

In recent years, facial recognition technology and its accuracy have been developed in a consistent manner, and it is used more and more in areas such as commercial retail, banking (for authentication and verification purposes) and social networking sites. However, the usage of these technologies raises data protection risks. The identification, security and profiling risks of the FRS have been already discussed in the previous chapter. This chapter analyzes these risks, from the perspective of the new GDPR. The first section assesses the difference between the right of privacy and the right of data protection in the EU legal framework. After that, the concept of risk and the risk-based approach from the GDPR perspective is highlighted. The risk-based approach and its circumstantial application represent the basis of the assessment of the different types of risks highlighted.

Furthermore, the treatment of facial images and the concept of personal data, under the new GDPR, is underlined. In general, as it may be depicted in the following section and as A29 WP 192 states: "a digital image that contains an individual's face which is clearly visible and that permits an individual to be identified' is considered personal data."[252] In consequence, prima facie, there might be no problem in

[252] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf -last accessed 29th of July 2017

classification of the facial images as personal data. Whenever the images are referring to directly and indirectly identifiable persons, these images should be considered personal data. On the other hand, the matter as for whether facial images are personal data still raises debate. Images that contain blurred faces and templates, which generally allow only categorization of the persons, are not to be considered personal data.[253] Parameters such as quality or accuracy of the image or the acquisition conditions of FRS need to be taken into account. Moreover, the questions of whether facial images are personal data or whether these images fall under the special category of sensitive data have to be answered. These categories of queries and their related answers are helpful in the assessment and mitigation of the identification risks of the FRS. On the condition that, facial images are considered to be personal data, the processing should be compliant with the principles determined under Article 5 of GDPR. In addition, when facial image are considered to be sensitive personal data, special requirements determined under Article 9(2) GDPR need to be fulfilled. Processing of these special categories of data is in general prohibited.

Furthermore, organizations need to implement and comply with the new organizational and technological measures imposed through the GDPR. In this sense, technological measures, such as pseudonymization or the encryption of facial images processed by FRS are more than necessary to be taken. Data breach notification and privacy impact assessment are crucial measures required to adopt in order to ensure compliance and accountability of the FRS data security risks under the GDPR. Finally, profiling risk of the FRS, from the perspective of the GDPR, is discussed.

4.2 The separation between privacy and data protection in the EU legal framework.

A separation between the notion of privacy and data protection in the EU legal framework is necessary to determine. Article 7 of the Charter of Fundamental rights of the European Union (the EU Charter)[254] reproduces Article 8 of the ECHR relating to the "right to respect for private and family life."[255] The Charter not only asserts the respect for private and family life, but also, highlights explicitly the right to data protection under Article 8 (1).[256] Article 8 of the EU Charter must be interpreted as embodying the pre-existent EU Data Protection legal framework, inclusive of the upcoming GDPR. Article 8(2) of the EU Charter mentions the fundamental data protection principles (personal data must be processed fairly, for specified purposes and on the basis of a legitimate ground laid down by law). Lastly, Article 8(3) of the Charter guarantees the control of an independent authority with regards to putting these principles into

[253] Ibid.
[254] European Union (Consolidated Version of the Treaty on the Functioning of the European Union) art. 16, 2008 O.J. C 115/47. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT –last accessed 25 of August 2017.
[255] CoE, European Convention on Human Rights, [1950], CETS No. 005.Available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005 -last accessed 25 of August 2017.
[256] European Court of Human Rights –Council of Europe, 'Handbook on European data Protection law'. Available at http://www.echr.coe.int/Pages/home.aspx?p=caselaw/otherpublications&c= -last accessed 25 of August 2017.

practice.[257] Consequently, data protection rules have been gradually separated from the right to privacy. The European Court of Justice has elevated all data protection rules to the level of 'fundamental rights.'[258] The right of data protection has been extended and broadened over time and with the new GDPR, the right is regulated at the utmost existent level in the EU.

Under the recent Schrems[259] case, the Court concluded that "Article 25(6) of Directive 95/46 implements the express obligation laid down in Article 8(1) of the Charter to protect personal data and […] is intended to ensure that the high level of that protection continues where personal data is transferred to a third country." Furthermore, the upcoming GDPR is approaching a crucial change. The right to privacy seems to have been wholly removed, as there is no mention at all.[260] Notions as 'privacy be design' or 'privacy impact assessment' have been changed with 'data protection by design' or 'data protection impact assessment.'[261] In conclusion, it should be reminded that Article 8 and 7 of the Charter to 'some extent they overlap, yet in the same time they have a different scope.'[262] Consequently, the GDPR should be seen as implementing the right to data protection.[263] Therefore, in this thesis, only the data protection risks from the perspective of the GDPR are assessed. The GDPR analysis represents the main focus of the thesis. However, where relevant, reference will be made also to Directive 95/46/EC.[264] In addition, even though, it is not in scope of this thesis to assess the EU legal privacy framework, a point of concern is the concept of metadata and processing for direct marketing purposes. Only in these particular cases, a reference will be made to the Proposal for a Regulation of the EU Parliament and the Council for the respect for private life and the protection of personal data in electronic communications (hereinafter **proposed ePrivacy Regulation**).[265]

[257] Ibid see also van der Sloot B. (2017) Legal Fundamentalism: Is Data Protection Really a Fundamental Right? In: Leenes R., van Brakel R., Gutwirth S., De Hert P. (eds) Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series, vol 36. Springer, Cham

[258] Ibid.

[259] Case C-362/14 Maximillian Schrems v Data Protection Commissioner available at http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre= last accessed 12 of July 2017

[260] See footnote 257.Van der Sloot B. (2017).

[261] Ibid.

[262] Juliane Kokott and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No. 4 (2013). Kokott Juliane and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No. 4 (2013). Available at http://oxfordindex.oup.com/view/10.1093/idpl/ipt017 -last accessed 23 of August 2017.

[263] See footnote 257. Van der Sloot B. (2017).

[264] See footnote 8. The GDPR

[265] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ,COM/2017/010 final - 2017/03 (COD).

4.3 The concept of risk and risk-based approach under the GDPR.

Under recital 75 of the GDPR, " the risk to the rights and freedoms of natural persons, of **varying likelihood and severity,** may result from personal data processing which could lead **to physical, material or non-material damage**, in particular: **where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymisation**, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; **where personal data is processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;** "or in case of **profiling activities**.
Even though, there is no clear distinction between different categories of the risk, under Recital 77, the objective calculation of the likelihood of risk should include the 'nature, context, scope and purposes of processing.' The high risk is defined under Recital 89 such as a process that 'involves new technologies or are a new kind, where no data protection privacy impact assessment has been undertaken or where they become necessary." In addition, the 'high risk may result from the extent and frequency of processing'[266]

Risk-based approach under the GDPR

Kuner, reveals the 'importance of the publication of A29 WP's Statement on the role of a risk-based approach in data protection legal framework, under which a support for 'the inclusion of a risk-based approach in the EU Data protection legal framework' is noted.[267] The upcoming GDPR also follows this path. As an explicit risk-based measure, the GDPR makes reference to the 'security' measures under Article 32 and Recital 83 of the GDPR.[268] Nevertheless, as presented in the following section, the GDPR is introducing explicit data breach notifications and data protection impact assessment, where, as well, the risk based approach was adopted as a basis. Gellert[269] defines the risk-based approach as a substitute of the traditional EU data protection principles (the-right based approach).[270] The purpose of the risk-based approach is two-fold: to assess the risk (risk assessment measures the level of risk) and to decide if the risk should be taken or not. Therefore, in case the risk is found to be too high, the decision of processing

[266] Recital 94 of GDPR.
[267] See footnote 189.Kuner et.al. (2015).
[268] See Recital 83 and Article 32 of GDPR where "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks…those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected."
[269] R. Gellert, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the... European Data Protection Law Review (EDPL), 4/2016, Vol. 2, pp. 481-492. Available at https://www.researchgate.net/publication/312652929 last accessed 10 of July 2017.
[270] See Article 5(1) of the GDPR

should not be taken.[271] However, even though the risk based approach and the right-based approach are seen as twin practices, they are not similar.

The issue of the risk-based approach is that it is contextual and provides insufficient and uneven protection, depending on how risky the processing is found to be. A29 WP[272] opinion emphasizes this 'namely, granular, scalable, logic of risk analysis' and that the risk-based approach is 'being increasingly and wrongly presented as an alternative to well-established data protection rights and principles' (the rights-based approach).

On the other hand, the right-based approach (as it is defined under Article 5 and 6 of the GDPR) manages risks from the outset once and for all, irrespective of the level of the risks[273] and offers 'minimum and non-negotiable protection for all the individuals.'[274] In consequence, the 'rights must be just as strong even if the processing in question is relatively 'low risk'.[275] Though, as Gellert reminds, it has yet to be seen whether the risk-based approach and the contextual application is or is not an appropriate tool for assessing the risks. In cases of data breaches, data protection impact assessment or profiling, risk-based approach might be a valuable instrument. A29 WP 218[276] mentions that the risk-based approach is 'only limited to accountability (Article 22 of GDPR), data protection impact assessment (Article 33 of GDPR), obligation to security (Article 30 of GDPR) etc.'[277] In consequence, the main principles of data protection are still right-based approach.[278]

4.4 Identification data protection risks of FRS under the GDPR.

4.4.1 Digital images as personal data.

This section answers the question of whether digital facial images are personal data, and if they are, why they are considered as such. The answer to these questions is deeply related to the mitigation of the identification data protection risks of the FRS. On condition that, digital facial images are found to be personal data, the protection granted by the principles rooted in Article 5 of the GDPR will be applicable.

---

[271] Ibid. See also Christopher Hood et al, 'Risk Management' in The Royal Society (ed), Risk: Analysis, Perception and Management - A Report of a Royal Society Study Group (The Royal Society 1992).

[272] Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN, WP 218, Adopted on 30.05.2014 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf -last accessed 14 of July 2017.

[273] Lynskey O,The Foundations of EU Data Protection Law (Oxford University Press 2015). Available at https://global.oup.com/academic/product/the-foundations-of-eu-data-protection-law-9780198718239?cc=nl&lang=en& -last accessed 26 of July 2017.

[274] See footnote 272. Article 29 WP 218.

[275] Ibid.

[276] See footnote 272. Article 29 WP 218.

[277] Ibid

[278] R. Gellert, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the... European Data Protection Law Review (EDPL), 4/2016, Vol. 2, pp. 481-492. Available at https://www.researchgate.net/publication/312652929 last accessed 10 of July 2017.

To begin with, facial images might be depicted as 'images that are taken of the face of individual persons, either in analog or in digital form, containing equally single pictures or video images.'[279] When it comes to FRS, a digital image is "a representation of a two-dimensional image in a digital form."[280] Moreover, due to the recent advances in facial recognition technology, three dimensional images are more and more used in the form of static and moving images (i.e. photographs, recorded and live video)."[281] As it has been presented in the previous chapters, facial images have been ''made, collected and/or registered for a very long time, with different technologies for personal and private use."[282] Once these images are digitalized, they are suitable to be used by commercial retail stores, in banks as means of authentication/verification and by social network sites.

Initially, Directive 95/46/EC anticipated the dispute of whether facial images should be considered personal data or not. In this sense, four recitals tried to settle this dispute.[283] The most clear is Recital 14 of the Directive 94/46/EC, which held in this sense that, ''given the importance of the developments…in the framework of the information society, of the technique used to capture, transmit, manipulate, record, store or communicate image data relating to natural persons, the Directive should be applied to processing involving those data."[284]

As a result of the expansive scope of FRS use, nowadays, it is almost impossible for the users of FRS, to implement FRS without processing personal data. In commercial retail, FRS might only collect data that will be analyzed instantly in the cloud, without actual storage of the data, and conclude outcomes before deleting the data. On the other hand, the data might be stored for further reference. In both situations, if the collected data allows for identification, the processing should be considered processing of personal data (even if the data is not stored).[285]

The GDPR is defining the concept of personal data under Article 4(1) as "any information relating to an identified or identifiable natural person."[286] In relation to the above-mentioned Directive 95/46/EC, the concept has not faced any substantial change. This broad term is still encompassing a wide range of

[279] Kindt Els, Doctoral thesis 'The processing of Biometric Data. A Comparative Legal Analysis with a focus on the Proportionality Principle and recommendations for a Legal framework', Katholieke Univerisiteit Leuven 2012. Available at https://lirias.kuleuven.be/bitstream/123456789/345184/1/PH_D_text_PartI%2BPartII_17.04-Pservice.pdf -last accessed 3 of June 2017.

[280] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf -last accessed 21 August 2017.

[281] Ibid.

[282] See footnote 279. Kindt Els (2012).

[283] Ibid.

[284] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf -last accessed 9 of July 2017

[285] See footnote 14. Lewinski et.al (2014).

[285] See footnote 16. Wall Mathew (2015).

[286] See footnote 8. The GDPR.

information. It seems that the aim of the legislators was to develop a wide-reaching notion of personal data. This is articulated through the usage of ''any information'' phrasing.[287]

In this sense, the information should not only relate to an identified person but also to an identifiable natural person. According to Article 4 of the GDPR an identifiable person is "one who can be identified directly or indirectly by reference to an identifier such as name, **identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic cultural or social identity to that person**."[288]

From a first look prospective, it can be argued that a person's image may, by itself, represent personal data that benefits from data protection safeguards.[289] Although the situation is not as simple as it looks. Thus, for a better understanding a distinction between data concerning 'directly' and 'indirectly' identifiable persons must be made.

- ### Digital images as personal data concerning directly identified persons in the case of FRS.

According to A29 WP 136,[290] with regard to the 'directly' identified persons, the most common identifier, is the name of a person. In order to be directly identified, a person must be prominently discernable from the other persons. The elements entailed in the data set, which cause direct identification of a particular individual, are known as 'direct identifiers'.

In the UK, for example, the Information Commission Officer has already made it obvious in the code of practice of CCTV, that information derived from the images of individuals and the related information from these kind of images are connected to the individuals.[291]

The concept of 'identified person' is directly tied with the 'person's name'. However, in order to determine the identity of the individuals, the name of the persons have to be merged with other pieces of information (such as the address of the individual or a photograph of a person's face).[292] This process might be undertaken to ''prevent confusion between that person and eventual namesakes" and will have the impact on "zooming on the individuals in flesh and bone."[293]

The A29 WP 192, mentions that "when a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data."[294] Consequently, there are some circumstances that have to be taken into account when it should have to be decided

[287] Article 4(1) of the GDPR
[288] Ibid
[289] See footnote 95.Buckley Ben and Hunter Matt (2011).
[290] Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data, June 20, 2007. 01248/07/EN/ WP 136 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf last accessed 4 June 2017.
[291]See footnote 95. Buckley Ben and Hunter Matt (2011).
[292] Ibid.
[293] Ibid.
[294] See footnote 11. Article 29 WP 192.

whether a digital image is personal data or not.[295] In this sense, the quality of the image or the particular viewpoint might matter.

For example, the images of individuals which are taken from far distance or the ones which are blurred, are usually not considered personal data. In order for their faces to be detected and for them to be identified, data subjects must look straight ahead and fill the area of the AFRS. The Facial Recognition Vendor Test 2000 study highlights that "environmental factors like camera angle, facial expression and other parameters can have significant effects on the ability of these systems to recognize individuals."[296]

In this respect, aging (loosing or gaining weight), supplementary deviations that are caused by disguises and spoofing attacks (such as image spoofing, video-spoofing or the 3D-masked printed)[297] can influence the original individual's face images. In addition, processing of the on-line face images are significantly different from the customary biometric applications.[298]

Therefore, the 'burden' of the FRS is to identify the individuals by taking into account the incidence of these variations.[299] The photo's accuracy requires a complete understanding of online face processing together with its threats and opportunities.[300]

Furthermore, by default, a reference template is likewise personal data as long as it embodies particular characteristics of an individual's face that might be associated with that individual and put away for a forthcoming comparison, identification or authentication/verification purposes.[301]

Nonetheless, templates of the image or the extracted particular characteristics of the individuals, in particular, utilized just for categorization (e.g. on the basis of their gender, age, ethnicity, clothes of the entities), will not be regarded as personal data.[302] To exemplify, when a video frame is caught and the

---

[295] Ibid.

[296] Woodward John, Horn Christopher, Gatune Julius "Biometrics. A look at facial recognition" Virginia State crime Commission, RAND Documented briefing. Available at https://www.rand.org/pubs/documented_briefings/DB396.html -last accessed 23 of August 2017. See also WP 193 explanations on the concepts of False Accept Rate (FAR) or False Reject Rate (FRR)

[297] Erdogmus N and Marcel S., Spoofing face recognition with 3d masks. Information Forensics and Security, IEEE Transactions *on*, 9(7):1084–1097, 2014. Available at https://www.researchgate.net/publication/262605045_Spoofing_Face_Recognition_With_3D_Masks -last accessed 20 Of July 2017 and Yi Xu and others, 'Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos' [2016] The University of North Carolina at Chapel Hill, This paper is included in the Proceedings of the 25th USENIX Security Symposium August 10–12, 2016 • Austin, TX 1-17

[298] Novetta Whitepaper, "Opportunities in Analyzing and Processing Online Face Images", August 2016 available at http://www.novetta.com/wp-content/uploads/2016/09/NovettaBiometrics_OnlineFaceProcessing_WP-W_9112016.pdf last accessed 11 of July 2017

[299] Chellapa Rama and others, 'Face recognition by computers and humans' [2010] 43(2) IEEE Computer Society. Available at < 10.1109/MC.2010.37> -last accessed 10 July 2017.

[300] Ibid.

[301] See footnote 11. Article 29 WP 192. See also **Section 2.6.1 Face Recognition Processing.**

[302] Ibid

only contained information is the summary statistics, it is unlikely that data will identify 'any person or will yield to highly accurate or reliable results.'[303]

In commercial retail, although FRS are posing identification risks (as it has been described under **Section 3.3**), the direct identification of the customers, is not always as essential to commercial retailers as the prospect of categorization of the customers on the basis of their emotions or other socio-demographic features. Thus, whilst the task of identification of the consumer's identity will lead to processing of personal data, spotting the individuals emotions or their socio-demographic characteristics, only, will not lead, specifically, to identifiable consumers.[304]

In consequence, on the one hand, if the information is not clear or sufficient for 'direct identification' the processing of images will not be considered personal data. On the other hand, if this template or the end result is linked with a pre-determined individual's record or profile, the outcome will likely be considered personal data.

Furthermore, facial images as personal data relating to 'indirectly identified' or 'identifiable' persons will be depicted.

- **Digital images as personal data concerning indirectly identified or identifiable persons in the case of FRS**

The classification of "indirectly" identified or identifiable persons, relates to the phenomenon of 'unique combinations.'[305]

The definition given in Article 4(1) of the GDPR is explicitly referring to the categorization of the individuals on the basis of factors like **"physical, physiological, genetic, mental, economic cultural or social identity to that person."** The above-mentioned features, when they are considered together, might enable the identification of the specific individuals through their particular patterns. Therefore, the availability of the further indirect identifiers (or even quasi-identifiers) enables the data controllers or other third parties to single-out the individual from the collectivity.

When it comes to digital images of faces, the characteristic or behavior of the individual revealed though the digital image may be taken into account. If the digital image possesses a specific characteristic or behavior and that information is used to identify the individuals, then that specific information might be considered as personal data.[306] Additionally, a reference template might be regarded as well as personal data. Instead of the raw biometric data, significant features such as facial measurements from an image, might be extracted, gathered, and used for further processing.

---

[303] Rodrigues and others (2016). Data protection and privacy issues concerning facial image processing in public spaces. Athens Journal of Technology and Engineering, 3 (1), 39-52. Available at https://www.athensjournals.gr/technology/2016-3-1-3-Rodrigues.pdf -last accessed 23 of July 2017.

[304] See footnote 14. Lewinski et.al. (2016).

[305] Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data, June 20, 2007. 01248/07/EN/ WP 136. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf last accessed 4 June 2017.

[306] See footnote 11.Article 29 WP 192.

A reference template is personal data when it entails several specific characteristics of the person's face that are linked with a person. Therefore, the reference template is personal data, only if, the template is used for identification or authentication/verification purposes. Although, if the template is used for categorization purposes (e.g. to establish a gender distinction: male/women), it will not be linked to an original image, profile or other personal record. As it does not capture enough information to identify the individuals, the template will not be considered personal data. [307]

In addition, A29 WP 193, outlines the following recommendation and measures in order to mitigate the identifiability risks: "a biometric template should not be too large in order to avoid re-construction, (e.g. re-identification). At the same time, a one-way process in order to avoid regeneration of the raw biometric data merely from the template" is recommended by the A29 WP 193[308]

As presented in the Chapter 3, nowadays, due to the vast amount of pre-existing facial data, the risk of identification or identifiability of individuals is very high since it can be easily attained through a simple intersection of the pre-available facial images of the individuals with online platforms. The Carnegie Mellon University (CMU) privacy research has revealed that through the combination of the WEB 2.0 data (images) and the FRS available at large scale, re-identification of the users may be possible.[309] Thus, Acquisti et al. have demonstrated that the combination of unidentified facial images (available on-line but anonymized or images of faces of strangers on the street) or pseudonymised with available facial recognition software will generate the risk of on-line and off-line re-identification.[310] The studies have revealed the capability to identify strangers both online and offline on the basis of facial images that were publicly available on the social network sites. The rate of online identification in these cases was 10%, whereas in the case of the offline re-identification, at least a third of the individuals were re-identified. Thus, 'photos that were already accessible on Facebook, without logging in, were sufficient to identify college students on a campus with a 31.18% success rate when using face recognition technology that was publicly available until it was recently acquired by Google.'[311] These studies are revealing a FRS model, which permits to display in a matter of seconds details as the name, date of birth or social security number of the individuals.[312]

In addition, social networking sites introduced functions such as photo tagging. These functions enable the connection between the pre-existent personal information of the users with their facial characteristics, perceived in an uploaded photo on SNS. Therefore, according to Welinder, FRS should be

[307] Ibid.
[308] See footnote 6. Article 29 WP193.
[309] See previous chapter; See also Alessandro Acquisti and others, 'Face Recognition and Privacy in the Age of Augmented Reality' [2014] 6(2) Journal of Privacy and Confidentiality 1-20.
[310] Ibid.
[311] See footnote 30. Welinder (2012).
[312] Ibid.

cautiously regulated, as they develop the ability to convert the information shared by the users (e.g. photo) to personally identifying information.[313]

Under the GDPR, the risk of re-identification from allegedly anonymized data or pseudonymised data is likely to become far more significant due to technological progress (actual FRS) and the desire of entities to associate existing datasets.[314]
A29 WP 216[315] highlights 'anonymization' as a technique "used to irreversibly prevent identification." But, these techniques still present 'residual risks' as they can entail, the risk of singling-out an individual, the linkability and interference risks.[316] Singling-out represents "the capability to isolate some or all records to isolate the dataset."[317] Whereas, linkability is related to the capability of "linking two or more datasets or a group of data subjects." The interference is then the possibility to "deduce…the value of an attribute.[318] The applicability of the GDPR does not necessitates, however, a high level of identification.[319]

In alignment with Directive 95/46/EC, the new GDPR is imposing a "proportionality test."[320] The definition of personal data should be read in accordance with Recital 26 of the GDPR, where: an "account should be taken to **all means reasonably likely to be used,** such as singling out […] to identify the person directly or indirectly." By 'all means' the Regulation refers to **"all objective factors, such as the costs, the amount of time, available technology at that time of processing and technological developments**."[321] The threshold is presented in the form, as whether there are likely reasonable means already available, that might be administered by the foreseeable users of the information.[322] In this sense, the GDPR is replicating the pre-existent "likely reasonable test."[323]

---

[313] Ibid.
[314]S Path, 'General Data Protection Regulation- Anonymization and Pseudonimization And I sit here without identity: faceless. My head aches' [2016].PricewaterhouseCoopers Legal LLP (London). Available at https://www.pwc.lu/en/general-data-protection/docs/pwc-anonymisation-and-pseudonymisation.pdf –last accessed 6 September 2017.
[315] Article 29 Data Protection Working Party (2014). Opinion 5/2014 on Anonymization Technique, April 10, 2014. 0829/14/EN WP216. Available at https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf -last accessed 18 August 2017.
[316] Ibid.
[317] Ibid
[318] Ibid.
[319]European Court of Human Rights –Council of Europe, 'Handbook on European data Protection law'. Available at http://www.echr.coe.int/Pages/home.aspx?p=caselaw/otherpublications&c= -last accessed 25 of August 2017.
[320] Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" Computer Law and Security Review [2016] 32 (2) 179–94.Available at http://daneshyari.com/article/preview/466369.pdf -last accessed 3 of September 2017.
[321] Recital 26 GDPR.
[322] European Court of Human Rights –Council of Europe, 'Handbook on European data Protection law'. Available at http://www.echr.coe.int/Pages/home.aspx?p=caselaw/otherpublications&c= -last accessed 25 of August 2017.
[323] Lundevall-Unger P and Tranvik T, 'IP Addresses – Just a Number?' (2011) 19 International Journal of Law and Information Technology 53.Available at https://academic.oup.com/ijlit/article-abstract/19/1/53/706223/IP-Addresses-Just-a-Number?redirectedFrom=fulltext –last accessed 23 of August 2017.

Additionally, according to A29 WP 136, an accurate reflection of "the state of the art technology, the advantage expected by the controllers, the interest of the individuals, technical failures, and the risks of organizational dysfunctions should be also taken into account" in this dynamic test.[324]

Nowadays, as it has been discussed in chapter 2, advancements in algorithms and improvements in face acquisition systems, either 2D (intensity image) or 3D (intensity in depth/range), infrared, or video cameras have contributed to the face recognition accuracy and identification.[325] Nevertheless, good quality of images may be feasibly obtained through cheap, easily available applications such as wearable devices and smartphones.[326] Therefore, by taking into account the available technology, technological developments in FRS, and these new conditions presented in recital 26 of the GDPR, the risk that an individual is identified or 'can be identified' is considerably high. The test that is proposed by the Article 29 WP is the one of the 'motivated intruder.' Therefore, the threshold imposed is a low one. In order to identify the individual from the 'anonymized personal data', this 'intruder' does not need to have a knowledge of a "specialist such as computer hacking skills, or access to specialist equipment or to resort to criminality such as burglary, to gain access to data that is kept securely."[327]

In the case of FRS used in commercial retail, consumers need not to be identified by the AFRS in order for the use to be qualified as processing personal data, but there rather needs to be a possibility that this software would enable consumer's identification.[328] In this respect Trzakowski[329] et al. identified the following four factors, so as to consider the processing of personal data by the automatic FRS*: '1) the expenses of identification 2) the data subject's interest 3) the threshold of the security features that have been agreed by the data controller 4) and for what purposes the technologies will be used.'*

Furthermore, Article 4 (1) of the GDPR incorporates "online identifiers" and "location data" explicitly in the text of the definition of personal data. The concept of metadata, direct marketing, and the usage of MAC address through the FRS are succinctly highlighted.

---

[324] Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data, June 20, 2007. 01248/07/EN/ WP 136 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf last accessed 4 June 2017, 15

[325] Jain Anil and others, '50 years of biometric research: Accomplishments, challenges, and opportunities' [2016] 79(1) Pattern recognition letters- Elsevier 80-105 .Available at https://www.researchgate.net/publication/290509735_50_Years_of_Biometric_Research_Accomplishments_Challenges_and_Opportunities -last accessed 23 of August 2017.

[326] Ibid.

[327] Article 29 Data Protection Working Party (2014). Opinion 5/2014 on Anonymization Technique, April 10, 2014. 0829/14/EN WP216. Available at https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf -last accessed 18 August 2017.

[328] Shi, J., Samal, A., & Marx, D. (2006). How effective are landmarks and their geometry for face recognition? Computer Vision and Image Understanding, 102(2), 117–133. Available at doi:10.1016/j.cviu.2005.10.002.-last accessed 23 of July 2017.

[329] Trzaskowski, J., Savin, A., Lundqvist, B., & Lindskoug, P. (2015). Introduction to EU Internet Law. Copenhagen: Ex Tuto Publishing. Available at http://research.cbs.dk/en/publications/introduction-to-eu-internet-law(f3be5ade-8036-4c1a-a27d-510ee97d46de)/export.html -last accessed 23 of August 2017.

- **Metadata. Direct marketing. MAC addresses as personal data under the GDPR**

The uploaded photos on the social network sites may reveal specific metadata like the 'time, date or the user's physical location.'[330] Montjoye has demonstrated already in his article that "four spatial temporal points are enough to identify individuals on the basis of their metadata of their mobile phone data set and credit data set.[331] Metadata, in a succinct presentation, refers to any data that is linked with the FRS functioning. Two categories of metadata may be highlighted: embedded metadata, which is generated under the caption of an image file when an image was captured.[332] These include items such as geo-location, timestamps, social metadata and behavioral-based meta-data.[333] Moreover, as depicted under the previous chapters, the digital signage technologies, aside from their potential to provide a personalized profile of the customer and to display tailored advertisement offline, are also able to provide digital content to the customers online**.**[334] By linking these technologies to social network sites or, other types of databases, the companies may be able to target online promotions to individuals.[335] In addition, a 'mixture of FRS and phone MAC addresses for authorizing access to Wi-Fi' has been highlighted. These systems possess the capability to track users via their MAC address.[336] As they are inter-related, all these issues are analyzed now all together.

Although, it is not the aim of this thesis to assess the EU legal privacy framework, due to the insufficient granted protection, a reference will be made to the new proposal of an **ePrivacy Regulation**.[337]
In this respect, it should be noted that, as an implementation of Article 7 of the EU Charter, the European Commission announced its plan by 10 January 2017 to review Directive 2002/58/EC[338] **(ePrivacy Directive)** and to replace the directive with an **ePrivacy Regulation.**[339] The aim of this Regulation is to ensure consistency with the General Data Protection Regulation."[340] Article 1(3) of the Proposal mentions that the ePrivacy Regulation 'particularizes and complements' the GDPR, and therefore will have an effect of lex specialis.

---

[330] Ibid.
[331] Montjoye, "Computational Privacy: Towards Privacy Conscientious Use of Metadata", Massachusetts Institute of Technology 2015 available at https://dam-prod.media.mit.edu/x/files/thesis/2015/yva-phd.pdf
[332] Ibid
[333] Ibid
[334] See footnote 14. Lewinski et. al. (2014).
[335] See section 2.6.2 and Section 3.6 and See Footnote 95 Buckley Ben and Hunter Matt (2011).
[336]Ibid.
[337] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ,COM/2017/010 final - 2017/03 (COD). Available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications last accessed 23 of August 2017.
[338] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002).
[339] See footnote 337.
[340] Article 29 Data Protection Working Party (2017). Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) 4 April 2017. 17/EN WP 247.

A point of concern is the definition of the metadata, that according to the Art. 29 WP 247[341] needs to be extended. Metadata is defined under Article 4(3) (c) as "*data processed in an electronic communications **network** for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication'*[342]
The 'network' wording "seems to refer only to data created under the 'lower level' and not in the course of a so-called over-the-top (OTT)[343] service."[344] Therefore, due to the actual definition, legal protection granted to metadata is not sufficient and the actual tracking technologies like FRS will likely not be protected under the **proposed ePrivacy Regulation.** [345] This is not, however, in alignment with the **proposed ePrivacy Regulation's** intended aim of extending its scope of application.[346]

However, according to the same A29 WP 247, any processing of metadata or the content of metadata should require consent of all the end-users.[347] The processing of these data is of a high risk, and might include sensitive data that falls under Article 35 GDPR.[348] In any situation, the processing 'always requires consultation with the Data Protection Authority.'[349]

In regards to direct marketing, recital 47 of the GDPR mentions that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."[350] As A29 WP Opinion 6/2014[351] already admitted, 'direct marketing' can represent a valid legitimate interest in the Directive 95/46/EC. The A29 WP Opinion has also delivered a recommendation on how a balancing test should be

---

[341] Ibid.
[342] Ibid.
[343] See European Data Protection Supervisor Opinion 5/2016,Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC) [2016] available at https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf - last accessed 15 of August 2017. Over the top (OTT) refers to services and applications that are accessible using the Internet and rely on a network provided to offer Internet access services. Examples include communications (voice and messaging) services such as Skype, WhatsApp and Facebook Messenger, but also a broad range of other services and applications, such as social networks like Facebook, Twitter or LinkedIn, or video and audio streaming services such as Netflix or YouTube. For more on OTTs. See http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf -last accessed 30 of August 2017.
[344] See footnote 340. Article 29 Data Protection Working Party (2017). Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) 4 April 2017. 17/EN WP 247.
[345] Ibid.
[346] European Data Protection Supervisor Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC) [2016] available at https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf - last accessed 15 of August 2017.
[347] Ibid.
[348] Ibid.
[349] Ibid.
[350] Recital 47 GDPR.
[351] Article 29 Data Protection Working Party (2014). Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, April 9, 2014. 844/14/EN WP 217. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf -last accessed 7 of September 2017.

performed in concluding whether direct marketing activities are carried out for a legitimate interest. The following three key factors should be considered when assessing the balancing test: controller's legitimate interest, impact on data subject and additional safeguards applied by data controller to prevent the undue impact towards data subjects. [352] 'In the marketing, the object of balancing interest is about companies' interest in knowing their customer's preference and promoting better personalized offers, products and services, against individual's interest not to be unduly monitored and spammed.' [353] Thus, besides controller's legitimate interest, the intrusion impact of the processing towards the individuals, is an important element to be taken into account in the final outcome of the balancing test. The A29 WP mentions that, it is significant to acknowledge that the impact is 'a broader concept than the harms and it entails any potential or actual consequences of data processing'.[354] Elements such as "the irritation, fear and distress that may result from a data subject losing control over personal information, or realizing that it has been or may be misused or compromised, for example through exposure on the internet"[355] are necessary elements to be assessed by data controllers.

When the processing involves activities such as 'extensive profiling, data-sharing, online and offline direct marketing or behavioral advertisement, consent of data subjects is needed.'[356] Thus, targeted advertising always requires consent of data subjects. In addition, data controllers have to implement safety measures, in the form of opt-out solutions and to safeguard the right of the data subject to object to direct marketing activities.[357] According to Recital 70 and Article 21 of the GDPR, the data subjects have the right to object to the processing of personal data for direct marketing purposes. The GDPR is guaranteeing not only "the right to object to processing for the purposes of direct marketing in an easy manner, but also to do so "free of charge."[358] In this sense, Article 7(3) gives assurances that, the data subject shall have the right to withdraw his or her consent at any time and that the withdrawal and the offering of the consent should be undertaken in an easy manner.'[359]

Furthermore, A29 WP 247 identifies that in relation to the ePrivacy Regulation, 'the scope of direct marketing is too limited' and outdated. Direct marketing communications are defined as "any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services"[360]
Consent should be required as well under the GDPR, whenever the data controller gathers and deposits 'indirectly identifiable (Wi-Fi or Bluetooth) MAC addresses of the devices, and establishes the location, in

[352] Ibid.
[353] Iplens, 'Personal data processing for marketing purpose under the new GDPR: consent v legitimate interest and Recital 47 – first thoughts' (IPlens, 12 July 2017). Available at https://iplens.org/2016/07/12/personal-data-processing-for-marketing-purpose-under-the-new-gdpr-consent-v-legitimate-interest-and-recital-47-first-thoughts/ - last accessed 7 September 2017.
[354] Article 29 WP 217.
[355] Ibid.
[356] Ibid.
[357] Ibid.
[358] Article 29 WP 247.
[359] Article 7(3) of GDPR.
[360] See footnote 340.Article 29 WP 247.

order to track the user's location in public spaces.'[361] This situation might occur, also, in commercial retail where digital signage technologies that entail FRS are used. MAC addresses are personal data and anonymization techniques should be applied immediately after the data is gathered. These data might be processed without being anonymized whenever "(i) the purpose of the data collection must be restricted to mere statistical counting (see the examples below), (ii) the tracking is limited in time and space to the extent strictly necessary for this purpose, (iii) the data is deleted or anonymized immediately afterwards and (iv) there must be an effective opt-out possibility." [362] However, in any situation the adequate information in relation to the processing should be offered as well as the possibility to opt-out for the data subjects.

In conclusion, as the chances of identification and identifiability gets higher, facial images or other data collected through the FRS should be considered personal data.[363] Under the next section the concept of *sensitive personal data* is highlighted.

4.4.2 Biometric data as a new category of sensitive data under the GDPR.

The GDPR, in Article 9(1), is imposing stricter rules on the processing of "*racial or ethnic origin, political opinions, religious or philosophical beliefs*, or trade union membership, and the processing of genetic data, ***biometric data for the purpose of uniquely identifying a natural person***, ***data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited***. Therefore, the new GDPR is intervening by including expressly in Article 9 (1), **"biometric data that are processed to uniquely identify a person."** These categories of data might be processed only if one of the requirements of Article 9(2) GDPR is fulfilled. Member States may intervene and add further limitations for the protection of biometric data.[364]

Moreover, it can be argued that facial images fall under the stricter legal protection of sensitive data since they are enabling the user of FRS to identify the individual's racial or ethnic origins. Taking into account the unique biometric characteristics, facial images may disclose specific 'visible differentiations in skin color and other racial and morphometric differences (as width of the face or nose). In this sense, an automated ethnic classification may occur. [365] For example, a facial image may similarly deliver supplementary but very specific evidence about individuals, such as about the Marfan syndrome and cleft lip and palate.[366] Hitherto, some European member states, like Estonia or the Czech Republic, have already concluded that the image of persons requires extended legal protection, and they have been expanding the concept of sensitive personal data automatically to include biometric data.[367] However, the upcoming

[361] See footnote 340.Article 29 WP 247.
[362] Ibid.
[363] See footnote 323. Lundevall-Unger and Tranvik (2011).
[364] See Article 9(4) GDPR.
[365] S. Lu and A. Jain, 'Ethnicity identification from face images' in Proceedings SPIE Defense and Security Symposium, Orlando, April 2004, previously. Available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.2036 –last accessed 23 of July 2017.
[366] See footnote 1. Els Kindt (2013).
[367] See footnote 95. Buckley Ben and Hunter Matt (2011).

GDPR, under recital 51, has intervened in establishing the following threshold: "the processing of photographs should not be systematically considered to be processing of special categories of data since they are covered by the definition of biometric **data only when processed through a specific technical means allowing the unique identification and authentication of the natural person**." In this sense, as FRS usage is deploying specific technical means that give data controllers the ability of identification and authentication of the natural persons, the processing of facial images shall fall under the special protection of the sensitive personal data. However, what is interesting in the new GDPR is that in relation to the protection afforded through Article 9 of the GDPR, there is a distinction made with regard to biometric data, between images and data resulting from a specific technical process. The protection is especially guaranteed for the photographs uniquely used for identification and for verification and not for other purposes.

After it has been assessed that facial images fall under the protection of personal data or sensitive data, that require identification of the users, a succinct presentation of the general requirements that the new GDPR is imposing in regard to these particular types of data will follow.

4.5 Processing of facial images under the GDPR.

The GDPR is highlighting that the processing of personal data should be compliant with the principles determined under Article 5 GDPR. In this sense the processing of facial images shall be:

- "Lawfully, fairly and transparent."
- "Collected for specified, legitimate and explicit purposes and not processed in a manner that is incompatible with these purposes" (the purpose limitation principle). This is an important yardstick in determining whether the processing made through the FRS is lawful.
- "Adequate, relevant and limited in relation to which the data are processed."
- "Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."
- "Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

A29 WP 193 when analyzing biometric data concludes that "these data may be processed only if there is a legal basis and the processing is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[368] Furthermore, it has been held that "photographs on the internet, may not be further processed in order to enroll them into a biometric system in order to recognize the persons in the images automatically (facial recognition) without a specific legal basis (e.g. consent)."[369]

[368] See footnote 6. Article 29 WP 193.
[369] Ibid.

For secondary purposes, the processing should be also adequate, relevant, not excessive and only if there is a legal basis for the processing. If a user consented to photo-tagging, by a FRS, the processing should be undertaken in a privacy friendly manner. After the photo-tagging "the images with the name, nickname or any other text specified in relation with the data subject, should be deleted."[370] When it comes to the FRS used in commercial retail, the retailer has the obligation as a data controller to define in an adequate manner the purpose of the data collection. "A purpose that is vague or general, such as improving user's experience, marketing purposes, IT security purposes or future research will be not seen as sufficiently specific."[371] Nevertheless, since facial images might fall under the special legal protection of sensitive personal data, processing of these special categories of data is in general prohibited, unless special requirements determined under Article 9(2) GDPR are fulfilled. In the GDPR these grounds of processing of sensitive data are mostly reproducing the ones of Directive 95/46/EC. Among all the requirements, the 'consent' will be succinctly discussed. In the case of processing of personal data, the consent should not be explicit. In accordance with Article 4(11) of the GDPR, consent should be freely given, specific informed and unambiguous. In order that the consent be unambiguous, this should not allow for any doubt regarding the data subject's intentions, and it should oblige the data controllers to adopt robust procedures for individuals to give their consent.[372] In commercial retail, this poses a problem because customers can neither opt out nor explicitly accept the processing of personal data by the FRS.

In general, noticeable signs which are attesting that FRS are being implemented in the stores, might 'implicitly' denote the consumer's consent. In this case, the consent to processing of personal data by the FRS in commercial retail shops might be implied, as when the consumers are entering the shops.

In contrast, according to Article 9 (a) GDPR, processing of data undertaken though the FRS might occur, on the condition that, the data subject has given its explicit consent.

Even though, the GDPR does not necessarily define what 'explicit consent' means, under the A29 WP 187[373] "[i]n legal terms "explicit consent" is understood as having the same meaning as express consent. It encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a handwritten signature. For example, explicit consent will be given when data subjects sign a consent form that **clearly outlines why a data controller wishes to collect and further process personal data**." As the burden of proof is on the retailers and due to the GDPR's requirements regarding the processing of sensitive data, the retailers should be more interested in attaining such consent explicitly in writing.[374] Usually, this consent is acquired along with other relations with the customers (e.g. enrollment in a loyalty program).[375]

---

[370] Ibid.

[371] See footnote 6. Article 29 WP 193.

[372] Lewinski, P. (2015a). Automated facial coding software outperforms people in recognizing neutral faces as neutral from standardized datasets. Frontiers in Psychology, 6, 1386. Available at doi:10.3389/fpsyg.2015.01386- last accessed 28 of March 2017

[373] Article 29 Data Protection Working Party (2011). Opinion 5/2011 on the definition of consent, July 13, 2011. 00197/11/EN WP187. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf -last accessed 25 of August 2017.

[374] See footnote 14.Lewinski et.al. (2016).

[375] Ibid.

In this sense, users and consumers consent to processing of their personal data, giving up in exchange their right of privacy.[376] However, in the case of FRS used in commercial retail, consumers do not have the opportunity to deny the processing, and it is debatable whether and how they consent to the data processing.

Furthermore, in the case of social network sites, the users should be undoubtedly informed, and they should have an option to consent, before they upload an image that would be subjected to the FRS processing of personal data. The consent, however, should not be understood as a legitimate legal background for other individuals that are in the pictures or for other intermediate stages of FRS (face detection, normalization, comparison).[377] In the same alignment, it has been argued that, the customary framework of notice and consent cannot shield entirely the users of FRS that do not comprehend the whole process and who carelessly continue to make public and distribute their personal information.[378] In this sense, Welinder mentions that, 'only once the users will be completely free to switch the SNS, (ones that present strong network effects), they will be capable to manifest their consent.[379] The consent should be 'informed', according to A29 WP Opinion 15/2011 on the definition of consent of the Working Party.

Moreover, in the case of FRS used for authentication/verification, besides consent, an additional data privacy consistent mechanism should be ensured (e.g. reliable passwords).[380] It is debatable, with regards to the condition of 'explicit consent', whether an individual that merely presents himself in front of a camera device, has been provided this 'explicit consent'. As previously highlighted, usually, an explicit consent will be given when the users are signing a consent form that implies sufficient information which "clearly outlines the reasons why the data controllers wishes to collect and further process personal data."[381]

Therefore, even though granted with the right of denial of the processing of their personal data, the consequences of refusal have the potential to keep the users out of the systems and to be helpless. This option of granting consent, might not be in the end a good option at all.[382]

---

[376] Luzak, J. (2013). Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies. European Review of Private Law, 1, 221–246. Available at https://www.kluwerlawonline.com/abstract.php?area=Journals&id=ERPL2013007 –last accessed 23 of August 2017.

[377] Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at< http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf>

[378] See footnote 30. Welinder (2012).

[379] Ibid.

[380] Ibid.

[381] Kindt. Els (2013).

[382] See also Article 29 Data Protection Working Party (2011). Opinion 5/2011 on the definition of consent, July 13, 2011. 00197/11/EN WP187. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf -last accessed 15 August 2017

4.6 Security data protection risks under the GDPR

- **Data security: encryption, pseudonymization, data breach notifications and data protection impact assessment (DPIA).**

As highlighted in the previous chapter, recent research and studies have demonstrated how actual face authentication systems are capable of fooling or by-passing external attacks.[383] According to A29 WP 192 Opinion[384], security breaches during the data transit in the case of online and mobile FRS and security breaches during data storage are likely to occur in the case of identification and authentication/verification.

In the new GDPR, data security is given a paramount role, by showing a synergetic relationship with the state of art technologies and with the modern inclusive data privacy regimes.

In comparison with Directive 95/46/EC, the new GDPR is enacting stringent requirements and obligations on both data processors and controllers, in relation to data security and risks. Whilst imposing more supervision on suitable security standards, (Article 32 GDPR) the new GDPR is ,in addition, introducing for the first time explicit data breach notification guidelines (Article 33 and 34 GDPR).[385] Furthermore, Article 35 of the GDPR has implemented the notion of Data Protection Impact Assessment (hereinafter **DPIA**) as a process for building and demonstrating compliance with the Regulation.

In this section, the following data security requirements are discussed by taking into consideration the GDPR and the FRS: encryption, pseudonimization, and data beach notifications. Nevertheless, the DPIA as highlighted under article 35 GDPR and the opinion 249 of the A29 WP,[386] is succinctly presented.

As revealed, Article 5 of the GDPR is placing security at the foundation of data protection among with the other principles.[387]

The controller, in order to guarantee a suitable level of the security risks involved, should implement all technical and organizational requirements by taking into account "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons"[388] "The link to the 'state of art and the cost' shall not, however, be concluded as a backdoor for the controllers not to act. But instead as a

[383] See footnote 23. Xu Yi et.al. (2016).

[384] Nevertheless, the weakness of the actual popular FRS has been highlighted under the Article 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf -last accessed 21 August 2017

[385] R. Heimes, 'Top 10 operational impacts of the GDPR: Part 1- Data security and breach notification' available at https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/ last accessed 14 of June 2017

[386] Art. 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. April 2017, 2012. 17/EN WP248.

[387] Ibid.

[388] Ibid.

fair way to diminish the necessary expenses for the security actions to be taken." [389] Thus, the implementation of the suitable measures and the oversimplification of the risk concept (to ensure a level of security appropriate to the risk)[390] are crucial actions that have to be taken for the appropriate adoption of Article 32 GDPR.

Furthermore, the GDPR highlights the specific circumstances under which the processing of personal data might represent a risk. In this respect, in recital 75, the GDPR mentions as risky activities "processing of personal data that may give rise to discrimination, identity fraud and professional secrecy; processing where data subjects might be deprived of their rights, or control over data; processing that may lead to disclosure of racial, religious, genetic or other categories of data."[391]

Article 32 (1) of GDPR highlights as guidance, inter alia, the following technical and organizational measures: a) pseudonymisation and encryption of personal data; b) measures to ensure a continuous confidentiality, integrity, availability and resilience of the processing systems; c) measures that allow for the ability to restore the availability and access to the data in the event of a security breach; d) recurrent testing of the efficiency of the technical and organizational measures. These measures should be adopted in light of the on-going shifting data security threat landscape.
The required above-mentioned security procedures should be enacted, at the moment of the initiation of the processing. As described under Chapter 2, this moment of initiation is the feature extraction, when the biometric data are converted into templates or images.[392] It is crucial that data controllers should acknowledge that "any loss of confidentiality, integrity or availability features"[393] will be likely to cause a negative impact to any further processing activities and irreparable damage towards to the data subjects.[394]
In addition, A29 WP 192 emphasizes, the possibility of security breaches during the transit of personal data and during the storage of the data for identification and authentication/verification purposes.[395] The first situation applies to the case of a transit between image acquisition and the later processing activities. For example, whenever the user is uploading an image to a website for further feature extraction and comparison, the controller has to adopt proper steps in order to guarantee the security of the data transfer. A29 WP 192 recommends encryption of both the facial image that is acquired but also for the communication network. Thus, when a user has commenced processing the transfer of the digital image, the transfer of the image should be encrypted. Afterwards, the encrypted image is sent to the central

[389] Ibid.
[390] See Article 32 GDPR.
[391] Article 75 GDPR.
[392] See Article 29 Data Protection Working Party Working documents on biometrics, August 1st, 2003. 12168/02/EN WP80. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf last accessed 12 of July 2017.
[393] Ibid.
[394] Ibid.
[395] See footnote 11. Article 29 WP 192.

server where it is stored.[396] Nevertheless, when FRS are used for authentication/verification purposes, local processing should be preferred.
Whenever the data is already stored for **identification or verification/authentication,** the controller should undertake suitable measures to forbid unauthorized access to the pre-existent image.

4.6.1 Encryption.

A29 WP 192 has proposed encryption as a security technique in transmission of the information and in the case of storage for identification or verification/authentication purposes.
In a short description, encryption is a technique under which a so-called cryptographic key is linked with the biometric data. The key will likely be re-generated when a "correct live biometric is presented on verification, whereas no template is stored ('untraceable biometric')."[397]
The encryption of the personal data represents a 'security technique with the outcome of rendering data unintelligible to any person that is not authorized to access it as result of encoding that particular information into a mutilated stated.'[398] In consequence, only the individuals that have the right to use the specific 'decoding mechanism and the secret decryption key might have access to the information.'[399]
The GDPR, mentions the encryption technique under the technical and organizational measures (article 32 GDPR).[400]
In addition, GDPR holds that in the situation of a security data breach, there is no need for communication to the data subject, if the controller been already implemented encryption measures.[401] Nonetheless, encrypted personal data will remain 'personal data' for the controllers that have the decryption key. Consequently the GDPR safeguards will apply. Moreover, encryption is considered an appropriate safeguard, in the case of processing the data for a new purpose, different than the one for which the data has been gathered initially.[402]

---

[396] Millar Stephen, 'Privacy Impact Assessment (PIA) - BioConnect: combining facial recognition and MAC address tracking for authorising access to Wi-Fi' [2016] Queen's University Belfast. Available at http://pure.qub.ac.uk/portal/files/123692281/StuartMillar_13616005_PIA.pdf%20p.3 - last accessed 1 August 2017
[397] Ibid.
[398] Gerard Spindel and Phillip Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' [2016] 7(1) JIPITEC- Journal of Intellectual Property Information technology and E-commerce Law. Available at http://www.jipitec.eu/issues/jipitec-7-2-2016/4440/spindler_schmechel_gdpr_encryption_jipitec_7_2_2016_163.pdf -last accessed 12 of July 2017
[399] Ibid. See also ENISA, Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics, 2015, p. 38. Available at: https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics -last accessed 10 July 2017.
[400] See also Article 4 (b) of the proposal of the European Parliament for a GDPR (LIBE proposal) defines encrypted data as "personal data, which through technological protection measures is rendered unintelligible to any person who is not authorized to access it", thus, according to LIBE, encrypted data shall just be a subcategory of personal data, which shall not lose its personal reference due to encryption.
[401] Article 34 (3) para. a) GDPR.
[402] See Article 6(4) (e) GDPR.

Technically, the key has to be deposited separately from the encrypted data, in a secure way, in order that the attackers will not be capable of decrypting the data.
Otherwise, the attackers may be capable of simply decrypting the data.[403] However, the 'knowledge how the lock operates or the algorithm used for encrypting the document is not enough to access it the content, since there are multiple ways to breakdown the encryption.'[404] In this sense, emphasis should be added on the available technology of encryption existing at the time of processing. The 'simplest and the most common way for attackers for decryption' is, as Spindler and Schmechel emphasized, through the usage of exhaustive key search or brute force attacks by trying all the possible keys.[405]
The robustness of FRS technologies, however, for identification and authentication/verification has already been demonstrated. Reliable face-locked computers might be by-passed through a mere presentation to the software of publicly available images or fake pictures of the users' faces (e.g. still-image based-spoofing, video-based spoofing and 3D-masking spoofing).[406]
As long as the key is regenerated when a 'correct live biometric is presented', a pertinent question that has to be answered is whether the encryption techniques proposed by the GDPR and A29 WP 192 can be regarded as a viable technical and organizational measure.

4.6.2 Pseudonymization.

As an alternative, the new GDPR is proposing the pseudonymisation technique in order to minimize the data security risks towards the data subjects (recital 28 GDPR). Pseudonymization, as depicted in the GDPR, is an appropriate technical and organizational measure.[407]
In contrast with Directive 95/46/EC, the GDPR does include a definition of 'pseudonymisation'. According to Article 4 (5) of GDPR, pseudonymisation means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." Thus, it should be noted that there are additional measures that are required in order to lower the risk of processing and to "help processors and data controllers to meet their data protection

403 Hon,Kosta,Millard,Stefanatou, Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation Tilburg Law School Legal Studies Research Paper Series No. 07/2014, p. 9, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971 last accessed 14 of June 2017.
404 Indra Spiecker Genannt Döhmann and others 'A Comparative Analysis' [2016] 2(4) European data Protection Law Review 535-554. Available at https://ueaeprints.uea.ac.uk/63337/1/EDPL_4_2016_Country_Reports_section_EMR_INTERNALUSE_Rep1.pdf last accessed 13 of July 2017
405 Erdogmus N and Marcel. S. Spoofing face recognition with 3d masks. Information Forensics and Security, IEEE Transactions. Available at https://www.researchgate.net/publication/262605045_Spoofing_Face_Recognition_With_3D_Masks -last accessed 20 Of July 2017
406 See footnote 23. Xu Yi et.al. (2013).
407 Article 32 para. 1 a) of the GDPR.

obligations."[408] In simple words, pseudonimyzation is a privacy-enhancing measure that allows the conversion of the individual identifier (names or addresses) into a pseudonym.[409] Under A29 WP 216,[410] pseudonymization techniques are "merely reducing the linkability of the data set with the original identity of the data subject."

Under Recital 26, the GDPR mentions, however, that "personal data which has undergone pseudonymization, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person." Therefore, in general, pseudonymized data are still personal data. In consequence the rules of GDPR will be applied to these particular type of data. However the 'proportionality test' will be applied, in this situation, only to the additional information. In this sense, De Hert and Papakonstantinou[411] revealed the probability that pseudonymized data can be regarded as non-personal data. As a consequence, they are exempt from the rules of data protection.

In the case of FRS, in general, knowledge of the identity of people in the image is not a prerequisite. This 'makes the case for image de-identification, the removal of identifying information from images, prior to sharing of the data.' [412] However, as revealed in Chapter 3, due to the existent technological advancements, the risk of identification is still higher. As FRS technology is advancing, new techniques of anti-spoofing and anti-attacking methodologies have also emerged (e.g. 3D acquisition scanners).[413] The anti-spoofing measures are usually, techniques that may be implemented to differentiate between real biometrics and the 'synthetically' manufactured products that contain biometric features.

Sensors that deliver precise information might become in the future a viable solution against 2D photos and towards the video-attacks against FRS.

GDPR, under Article 32, has anticipated these burdens. Despite all proposed efforts, even the ones suggested by the highly advanced tech companies, FRS, the data controllers and processors, these systems face difficulty from the challenges posed by hackers.[414] In the end 'the enemy knows your system'

---

[408] Recital 28 of the GDPR.

[409]Maldoff Gabriel, 'Top 10 operational impacts of the GDPR: PART 8 – Pseudonymization' (Iapporg, 12 February 2016). Available at https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/ - last accessed 7 September 2017.

[410] Article 29 Data Protection Working Party (2014). Opinion 5/2014 on Anonymization Technique, April 10, 2014. 0829/14/EN WP216. Available at https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf -last accessed 18 August 2017.

[411]Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" Computer Law and Security Review [2016] 32 (2) 179–94.Available at http://daneshyari.com/article/preview/466369.pdf -last accessed 3 of September 2017.

[412] Andrew Senior, 'Face De-Identification' in Andrew Senior (ed), Protecting Privacy in Video Surveiilance (Ralph Gross 2009) 129. Available at http://www.pitt.edu/~jeffcohn/biblio/facede.pdf last accessed 13 of July 2017

[413] J. Galbally, S. Marcel and J. Fierez "Biometric Anti-Spoofing Methods: A Survey in Face Recognition " CAM under Project S2009/TIC-1485, in part by the Ministry of Economy and Competitiveness through the Bio-Shield Project under Grant TEC2012-34881. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6990726 –last accessed 15 August 2017.

[414] Ibid.

principle may be applied. The principle is rooted on the fact that 'the simpler and fewer are things needed to be kept secret in order to ensure the security of a given system, the easier is to maintain the security.'[415] In this respect, the GDPR approach is a flexible one adapted to the "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."[416] Therefore, the technical and organizational measures are provided and should be adopted in an alternative way.

4.6.3 Data breach notification.

The GDPR will implement a name and shame tool. This requirement of data breach notification is articulated under Article 33 and 34 of GDPR. In Article 33, notification of the supervisory authority is regulated whereas under Article 34 of GDPR the communication of the data breach to the data subject is mentioned.

The personal data breach is defined under Article 4(12) such as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

According to Recital 85 ***"****a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."*[417]

In case of data-breach notification, the GDPR is undertaking a risk-based method. Thus, relatively benign breaches do not necessarily need to be notified to the supervisory authorities or data subjects. The risks that are enacted through the data breaches are separated into three classifications.

Firstly, if **no risk** 'to the rights and freedoms' of individuals has concluded, the notifications are not necessary. In this case, however, the data controller bears the duty to document the event.[418]

Secondly, if after the assessment, a **likelihood of a risk** to the right and freedom of the individuals has been identified, then a notification to the supervisory authority should be sent in 72 hours.[419]

Moreover, according to Recital 85 of the GDPR "where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay."

Thirdly, when after the assessment a **high risk** to the rights and freedoms of the individuals has been identified, a notification is compulsory without any unnecessary postponement.[420]

---

[415] Ibid. See also A. Kerckhoffs, ''La cryptographie militaire,'' J. Sci. Militaires [1883], 9, pp. 5–83. Available at http://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf -last accessed 15 August 2017.
[416] Article 32 of the GDPR.
[417] Recital 85 GDPR see Also Article 32 GDPR.
[418] See article 31 of GDPR.
[419] See Article 33 (1) of GDPR.
[420] Article 34(1) of GDPR.

However, even in the case of **high risk**, there is an exoneration in regard to the notification of data subject whenever: "the controller has implemented technical and organizational measure; the controller has undertaken subsequent measures in order to enable that the high risks to the rights and freedoms of data subjects can no longer materialize; the notification will involve an disproportionate measure."[421]

For example, when data processed through the FRS are encrypted the notification is not mandatory. This layered methodology enables data controller flexibility and discretion in the notification process. In this sense, saving actions could be implemented by the controllers at any level. In practice, it seems that not so many notifications will reach the public, since ex-post measures and additional parameters can be adopted by data controllers.[422]

Although, it is debatable, in what circumstances the processing made by a controller in the case of FRS is likely to result **in risk or high risk** towards the rights and freedoms of the individuals. Even though, 'risk-based approach can help to identify the challenges to data protection and the selection of the most effective tools for mitigating these risks'[423], a matter of concern is, whether this flexibility will be likely to add a valuable contribution towards the data protection purposes.[424]

In regard to the FRS processing of personal data, it has to be assessed whether processing is implying 'risk' or 'high risks'.

On a first look, the high risk requirements for data breach notifications are fulfilled by FRS because they contain: • "New technology • Long time since initial processing (e.g. reference template that is generated will be deposited on a face database existent on the service or on other online services) • Systematic automated decision-making (profiling in the case of FRS used in retail) • Large-scale processing of sensitive data (FRS used in social network sites and commercial retail) • Systematic monitoring of public areas (commercial retail)"[425]

However, the application of the risk-based approach could be seen as difficult to implement as it relies on a robust methodology.[426]

4.5.4 Data protection impact assessment. (DPIA)

Conceptually, an impact assessment is defined as a "tool that is used for the analysis of the possible consequences of an initiative of an initial societal concern or concerns, when this initiative might present

[421] Article 34 (3) (a), (b), (c) of GDPR.

[422] Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" Computer Law and Security Review [2016] 32 (2) 179–94.Available at http://daneshyari.com/article/preview/466369.pdf -last accessed 3 of September 2017.

[423] See footnote 189. Kuner et.al. (2015).

[424] Ibid.

[425] Maldoff Gabriel, 'The Risk-Based Approach in the GDPR: Interpretation and Implications' (Iapporg, 29 March 2016) https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/ -last accessed 7 September 2017.

[426] Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN, WP 218, Adopted on 30.05.2014 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf -last accessed 14 of July 2017

dangers to these concerns with a view to support the informed decision-making, whether to deploy this initiative and not ultimately constituting a means to protect these concerns."[427]

Under Article 35 of GDPR, the notion of Data Protection Privacy Impact Assessment **(DPIA)** has been introduced. Whenever, the processing is likely to result in a high risk to the rights and freedoms of the data subjects, a DPIA has to be carry out by the data controller as an 'assessment of the impact of the envisaged processing operations', in particular when 'new technologies are involved, taking into account the scope, nature, context, and purposes of the processing.'[428] However, in the case of failure to attain these measures, a heavy sanction might be imposed. Furthermore, since the article mentions that the DPIA should be undertaken before the processing, the emphasis will be put on the anticipatory measures rather than on the reactive ones. As Kloza et. al. highlights DPIA is a 'living instrument.'[429]

DPIAs are "important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (see also article 24 GDPR)."[430]

The DPIA mechanism incorporates "a single assessment that may address a set of similar processing operations which present similar high risks."[431]

Therefore, DPIA might be implemented to assess multiple operations which are similar in the matter of risk involved.

The DPIA is mandatory whenever the processing is 'likely to result in a high risk'. Therefore, a risk-based approach is proposed in the case of DPIA as well. As discussed in the previous section, the risk-based approach is still unclear, and it might generate 'artificial complication' into the DPIA.[432] Therefore, the upcoming GDPR offers significant flexibility when determining whether the processing is likely to determine high risk and whether this 'residual risk' will necessarily generate a DPIA.

According to Article 35 (3), the GDPR mentions in the form of a non-exhaustive list, *inter alia* the obligation of assessing a DPIA in the case of[433] evaluation or scoring, where processing of personal data implies automated decision making (in the form of profiling, e.g. in case of FRS used in retail); in the case of processing of systematic monitoring (data collected without the user's awareness in public areas and

---

[427] Kloza Dariusz and others, 'Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals' [2017] (1) Brussels Laboratory for Data Protection & Privacy Impact Assessments (dpialab). Avaialble at http://virthost.vub.ac.be/LSTS/dpialab/images/dpialabcontent/dpialab_pb2017-1_final.pdf –last accessed 14 July 2017.

[428] Article 35 of GDPR.

[429] See footnote 427. Kloza et al. (2017).

[430] Art. 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679,17/EN WP248. Adopted on 4 of April 2017.

[431] Ibid.

[432] See footnote 427. Kloza et al (2017).

[433] See also Kamarinou, Dimitra and Millard, Christopher and Singh, Jatinder, Machine Learning with Personal Data (November 7, 2016). Queen Mary School of Law Legal Studies Research Paper No. 247/2016. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811 -last accessed 23 of July 2017.

without knowledge about how the data might be used, for example FRS used in commercial retail); in the case of processing of sensitive data (e.g. digital image might be regarded as sensitive data); data that are processed on a large scale[434] (FRS that are used for identification purposes and ones that are used in commercial and retail area are falling under this criteria). Nevertheless, A29 WP Opinion released in 2017, makes clear that the DPIA is necessary in the case of 'innovative use or applying technological/organizational solutions, such as face recognition for improved access control.'[435] The rationale is that, in accordance with Article 35(1), and recitals 89 and 91, these new technologies might imply the formation of new practices of data processing. In consequence the risks for the right and freedoms of the individuals is high.[436]

Moreover, according to Article 35(4), the controller shall seek advice from the data protection officer (DPO) when a DPIA is needed to be carry out. However, the responsibility of the controller is not entirely noticeable, since advice is required without any additional description from the DPO.[437]
Under recital 84 and 90 and Article 35(7) the DPIA should entail a description of the envisaged processing operations and the purposes of the processing "an assessment of the necessity and proportionality of the processing; an assessment of the risks to the rights and freedoms of data subjects; the measures envisaged address the risks; to demonstrate compliance with this Regulation." Thus again, it is for the data controller to decide the 'qualified assessors, to ensure the robustness of the DPIA and to be aware of documentation and their entire accountability for the selection of the necessary method.'[438] However, in particular, when it is not clear whether a DPIA is required, the A29 WP recommends that 'a DPIA is carried out nonetheless, since a DPIA is a useful tool to help data controllers comply with data protection law.'[439]

4.6 Profiling.

According to Hildebrand "profiling is not about data but about knowledge."[440] This sophisticated concept, or 'new type of inductive knowledge' enables the detection of the "correlations between data in

[434] Art. 29 Data Protection Working Party Opinion 03/2012 on purpose limitation. 00569/13/EN WP 203.Adopted on 2 April 2013. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf last accessed 23 August 2017.
In order to determine that, processing on a large scale has been undertaken, accounts should be taken on: "the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity.
[435] See footnote 430. Art 29 WP (2017) on DPIA.
[436] Ibid.
[437] See footnote 427.Kloza et.al (2017).
[438] Ibid.
[439] See footnote 430. Art 29 WP (2017) on DPIA.
[440]Hildebrand M, 'Profiling from data to knowledge the challenges of a crucial technology [2006] 30(9) Datenschutz und Datensinchercheit.

databases that can be used to identify and represent a human and non-human subject[…]or the applications of the profiles to individuate and represent a subject or to identify a subject as a member of a group or category."[441]
Profiling applies, even in the absence of a direct link to a particular individual. In this sense, a "profile can be connected to or applied later or the connection to an individual can be made based on the identification of an individual as having one or more attributes contained in the profile."[442] Whilst, the Directive 95/46/EC has not defined profiling, allowing the definition and regulation to be determined by Member States,[443] the new GDPR is defining profiling expressly, and it mentions profiling for 23 times.[444]

In the Article 4 (4) of GDPR profiling is defined as: ***"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements***"[445]

In the same way, Recital 71 of the GDPR articulates that profiling "consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him/her or similarly significantly affects him/her." Practically, automated decision-making will usually incorporate profiling, where these particular profiles will lead to the decision making-process.[446] In this sense, the concept of profiling is unambiguously presented under the GDPR, as a "sub-category of the automated processing, and refers to the use of personal data to evaluate certain personal aspect of natural persons to analyze and predict certain aspects of life."[447] Therefore, as highlighted by Bygrave, and as stated under article 15 of the Directive 95/46/EC, the rationale behind the principle is that "the fully automated assessments of a person's character should not form the sole basis of decisions that

Available at <https://pdfs.semanticscholar.org/c0a1/aa843e812925127dfb8f9540089e1a0a72b5.pdf> -last accessed 14 July 2017.

[441] Hildebrand, Defining Profiling: A New Type of Knowledge? in M Hildebrand and S Gutwirth (eds), Profiling the European Citizen (Springer Science 2008) 17-45.Available at https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2 –last accessed 23 of August 2017.

[442] C Roosendaal, A. P. (2013). Digital personae and profiles in law: Protecting individuals' rights in online contexts Oisterwijk: Wolf Legal Publishers (WLP). Available at https://pure.uvt.nl/ws/files/1515346/Roosendaal_digital_21-05-2013_emb_tot_22-08-2013.pdf -last accessed 17 of July 2017.

[443] See footnote 404. Indra Spiecker Genannt Döhmann and others (2016).

[444] Ibid see GDPR – Profiling in eight recitals (24, 60, 63, 70, 71, 72, 73, 91) and nine articles (4, 13, 14, 15, 21, 22, 35, 47, 70).

[445] Article 4(4) GDPR.

[446] Kamarinou Dimitra and others, 'Machine Learning with Personal Data' [2016], Queen Mary School of Law Legal Studies Research Paper No 247/2016. Available at SSRN: <https://ssrn.com/abstract=2865811> -last accessed 1 August 2017

[447] Ibid.

significantly impinge upon the person's interests."[448] The GDPR maintains this principle under Article 22 where states that the "data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[449] Thus, it might be useful to separate the profiling process into three main activities: data collection, model development (through machine learning) and decision-making. The machine learning algorithm has the role of developing the profile from the data collected, whereas in decision-making, determination and outcomes regard to the data subjects are undertaken, based on the profile made.[450]

In addition, according to Recital 63 and Article 13(2)(f) of the GDPR, "*the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases**, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject***."[451]

Therefore, in the case of profiling, data subjects have the right to obtain from the data controllers the knowledge of the logic involved and the foreseen outcomes of the processing.[452]

This provision is relevant in the case of FRS used in retail 'given that proponents of the technology emphasize its ability to automate and facilitate decision making processes.'[453]

As revealed, FRS used in the commercial retail (digital signage technologies) might predict and understand behavior in order to influence the behavior of the customers by creating different layers of market segmentation. The FRS already might learn and analyze the attitude towards the products (happiness, disgust) of the consumers. In consequence, FRS creates a complete emotional and personalized profile of the customers.[454] In this sense, FRS can deliver "brand tailored and personalized advertisements to the individual customer."[455]

On the one hand, computers might outperform humans in this sense since '"computer software cannot be depressed or otherwise experience emotional or cognitive abnormalities as humans can."[456] Thus, prima facie, the application of the Article 22 and the obligation of providing the logic involved to data subjects, in the case of automatic decision making is clear. However, authors like Savin, have emphasized

---

[448] Bygrave Lee, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' [2001] 17(1) Computer Law & Security Report.
Available at http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf - last accessed 31 July 2017.

[449] Article 22 of GDPR

[450] See footnote 446.Kamarinou et. al. (2016).

[451] Recital 63 of GDPR.

[452] See also Article 12(a) and 15 (1) of the Directive 95/46/EC, See also Brownsword Roger and others, The Oxford Handbook of Law, Regulation and Technology (1st edn, Oxford University Press 2017).

[453] See footnote 446. Kamarinou et.al. (2016).

[454] Ibid.

[455] See footnote 14.Lewinski et.al. (2016).

[456] Lewinski, P. (2015a). Automated facial coding software outperforms people in recognizing neutral faces as neutral from standardized datasets. Frontiers in Psychology, 6, 1386. Available at doi:10.3389/fpsyg.2015.01386- last accessed 28 of March 2017.

that 'if the real intention of the data processor is not to evaluate personal aspects but an auxiliary effect', article 15 of the Directive 95/46/EC[457] (actual 22 of GDPR) will not be applied.[458] On the other hand, 'what is less clear is what this means for anybody using automated decision-making.'[459] In regard to the data protection legislation, there are already concerns expressed. It has been held that the 'increasing automation of decision-making processes endangers automatic acceptance of validity of the decision reached and the concomitant reduction in the investigatory and the decisional responsibilities of the humans.'[460] The criticism that appears is that the GDPR is 'confined in its application to decisions that are fully automated.'[461] Therefore, as noticed, the application and the scope of Article 22 is confined to the decision-making processes that are fully automated. Conversely, whenever the profiling mechanism will entail human intervention in the decision-making process, article 22 will be not applicable.[462] However, humans have to 'exercise a real influence on the outcome of the particular decision-making process to lead the inapplicability of the protection of Article 22 of the GDPR.'[463]

In the case of FRS software, even though they developed significantly recently[464], it is noteworthy to be reminded that these systems are not, always, entirely automatic.[465] Human's intervention is necessary, for instance, in cases where sub-optimal conditions produce poor quality images or when images are several years old.[466] As already mentioned in Chapter 2[467] many application algorithms require operators to review the so-called candidate list and to check for the existence or the lack of matching.[468]

As argued, 'when the humans do not have a real influence on the machine that provides the decision-making in accordance with Article 22 of the GDPR and the human actors are only building the machine, providing the inputs' (e.g. in our case checks for individual's matching) the safeguards of Article 22 GDPR will be applied.[469] These activities will fall under the data collection stage. Moreover, where the 'machine

---

[457] Article 22 of GDPR

[458] Savin (2014), See footnote 480.

[459] Leenes Robert, 'Accountability and transparency in Big Data land' (DSC/t Blog - May 2016-Tilburg Institute for Law, Technology, and Society; TILT, Tilburg Law School). Available at https://www.tilburguniversity.edu/research/institutes-and-research-groups/data-science-center/blogs/data-sience-blog-ronald-leenes/ -last accessed 31 July 2017.

[460] See footnote 448.Bygrave (2001).

[461] Koops Bert-Jaap, 'On decision transparency, or how to enhance data protection after the computational turn' in Mirelle Hildebrant and Katja De vries (eds), Privacy, due process and the computational turn (Abingdon: Routledge 2013) 196-220.Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2367510 –last accessed 23 of July 2017.

[462] Ibid.

[463] See footnote 448.Bygrave (2001).

[464] Phillips Jonathon and Alice O'Toole, 'Comparison of human and computer performance across face recognition experiments' [2014] 32(1) Image and Vision Computing. Available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913011 – last accessed 31 July 2017.

[465] Dunn White and others, 'Error Rates in Users of Automatic Face Recognition Software' [2015] 10(10) PLoS ONE. Available at <https://doi.org/10.1371/journal.pone.0139827 > - last accessed 30 of July 2017

[466] Ibid.

[467] See section 2.5.

[468] Article 29 WP 80.

[469] See footnote 446. Kamarinou et al. (2016).

learning algorithm that provides the decision that stays at the basis of Article 22 GDPR is always accurate, reliable and objective, the protection of Article 22 GDPR will be applied.[470]

Nevertheless, the GDPR does not explicitly mention if the final 'decision' has to be final or an interim one, a step to final decision or whether the final outcome should specifically exclude at all human interventions.[471] In the end it is not completely clear whether the safeguards provided by Article 22 of GDPR apply in the circumstance of semi-automated decision. As mentioned already, 'it is highly likely that one or more humans will be involved in the design, training, and testing of a system incorporating in data collection and machine learning' and that application of Article 22 of GDPR will be applied. But it is not completely clear if the provision will be applied when a human intervenes into the decision.[472] Therefore, the application of the Article 22 GDPR is not completely clear and is contextual.

However, according to Article 22 GDPR, the decision has to produce 'significant' legal consequences, which in alignment with A29 WP should be a balance between the 'possible and actual impacts of profiling technologies on the rights and freedoms of data subjects and the legitimate interests of the controllers.'[473] Moreover, the obligation to provide the logic involved, guarantees only an 'ex-ante-transparency and ex-ante reflection of the data controller of the foreseeable but not wanted side-effects of processing.'[474] However, as the data processing might be complex, prediction of the envisage outcomes and the act of providing information in an eloquent manner, ex-ante, might be impossible or difficult to attain in some particular cases. The individuals often lack the necessary technological information and the opacity of the processing will likely to be an important barrier. In addition, security measures shall be adopted, not only when the data controllers are entering in the possession of personal data. Beside ex-ante measures privacy impact assessment and ex-post actions should be adopted.

Moreover, profiling itself, refers only to the automatic processing of personal data. However, the collection and the processing of the 'anonymous data required for the creation of the profile' are not a part of the concept of profiling.[475] In this sense, Article 22 of the GDPR applies only 'to data subjects' and as Savin highlights 'the protection of Article 22 against automated decision-making in relation with anonymized data does not apply.'[476] On the other hand, legal scholars such as Roosendal emphasized that profiling applies, although there will be no direct link to a particular individual. In this sense, a "profile can be connected to or applied later or the connection to an individual can be made based on the

[470] Ibid.
[471] Ibid.
[472] Ibid.
[473] Article 29 Working Party (WP29) Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted 13 May 2013. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf -last accessed 30 of July 2017
[474] Ibid.
[475] See footnote 404. Spiecker Indra ,Genannt Döhmann and others (2016).
[476] Savin, A. (2014) 'Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks.paper presented at 7th International Conference Computers, Privacy & Data Protection, Brussels, Belgium): 1-14. Available at http://research.cbs.dk/en/publications/profiling-and-automated-decision-making-in-the-present-and-new-eu-data-protection-frameworks(9c7f8f4c-b54f-4c30-bf50-77284a9fbaef).html –last accessed 23 of August 2017.

identification of an individual as having one or more attributes contained in the profile."[477] Kamarinou et. al.[478] remembers, similarly that the usage of the anonymized data, alone or in combination with other data, to single-out (e.g to make predictions towards someone interest/conduct) an individual will determine application of the Article 22 GDPR.

When it comes to FRS, according to A29 WP 193, these technologies might have the potential for profiling, although there is not real knowledge of the individual's identity. There is no doubt, that it is possible for FRS, to "track routes and habits of the individuals" (in commercial retail) for the particular purpose of "effective queue management, product placement and targeted advertising.[479]

To continue, whilst Article 22(1), generally prohibits profiling, the subsequent paragraph 2 highlights three exceptions. These exceptions allows profiling if it: "(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent."

However, in all three situations, suitable measures should be put in place to ensure the rights of the data subjects. The first situation should be regarded from a "narrow interpretation" where there is a contractual agreement and a specific legal framework. In the second situation, the consent should be informed.[480] On the other hand, obtaining 'explicit and informed' consent in the case of commercial retail shops is not an easy task. One solution that has been proposed is the introduction of "members only shop." Moreover, noticeable signs can be implemented in the shops. 'When a consumer enters a shop with a big and obvious sign out front that the AFRS is being used, the retailer could *potentially* imply such consent .[481] Alternatively, a contract as a legal basis for profiling is also difficult to be obtained.[482]

Finally, in the case of FRS used in retail, online-behavioral profiling might occur. Therefore, if AFRS can identify individuals and match a photo that they capture with a Facebook photo of an individual, the 'image' will become complete. The separate bits of information could be gathered to obtain the detailed image of the individuals: friendships, habits, tastes.[483]

Although, most of the companies that employ behavioral advertising are stating they do not engage any personal data usages and that their processing is lawful, the statement that they do not use direct identifiers of the users is not truthful at all. As demonstrated in the identification section,[484] the risks that an image, or name can be linked to MAC address are high.

---

[477] Roosendaal Arnold, Digital personae and profiles in law: Protecting individuals' rights in online contexts (1st edn, Oisterwijk: Wolf Legal Publishers (WLP) 2013). Available at https://pure.uvt.nl/ws/files/1515346/Roosendaal_digital_21-05-2013_emb_tot_22-08-2013.pdf last accessed 23 of August 2017.

[478] See footnote 446. Kamarinou et.al. (2016)

[479] Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193, See also footnote 14. Lewinski et.al. (2016)

[480] See footnote 446.Kamarinou (2016) see also footnote 404.Indra Spiecker Genannt Döhmann and others (2016).

[481] See footnote 14.Lewinski et.al. (2016).

[482] Ibid.

[483] See footnote 16.Wall Mathew (2015).

[484] See section 2.6.2.

4.6.1 Interim Conclusion

In this chapter, it has been revealed that facial images should be regarded as personal data as they relate to an identified or identifiable person. In consequence, GDPR is applicable. However, the situation is not as clear as it seems to be. Whenever the images are blurred, or they are gathered from a distance, no personal data are processed and thus the GDPR not apply.

Furthermore, by taking into account the GDPR, a separation between direct and indirect identifiers has been established. Moreover, when it comes to metadata or content of metadata, as these usually entail sensitive information, require consent of the end-users whose data are being processed by the FRS. MAC addresses are regarded as personal data and the gathering of these data should be undertaken by using anonymization techniques. Processing for direct marketing purposes might fall under the legitimate interest exceptions. However, data controllers have to perform a balancing test in this sense. When the processing involves activities such as 'extensive profiling, data-sharing, online direct marketing or behavioral advertisement, consent of data subjects is needed.'[485] In any case, withdrawal of the consent should be done in an easy manner (free of charge at any time). Security measures such as encryption, data breach notification, pseudonymization or data protection impact assessment are also proposed in the case of FRS security risks. The robustness of the technologies and the spoofing attacks, however, create doubt in regard to the viability of these security techniques. However, the GDPR has anticipated these problems and is granting a flexible approach under Article 32. In assessing the necessity of the security measures, 'the state of the art of the technology, nature, scope, context of processing, the risk and varying likelihood of risks or the severity to the rights and freedom of natural persons'' should be taken into account by the data controller and data processors. It is disputable, although, whether this margin of maneuver will be in the end beneficial for data controllers.

Flexibility is granted also by the GDPR through the adoption of the risk-based approach. It should be noted that, the risk-based approach should not be presented, always, as an alternative to the established data protection rights and principles.[486] Data protection rights and principles should be permanently granted as an implementation of the right based approach. Furthermore, article 22 of the GDPR grants protection, for the profiling risks of FRS used in commercial retail. These systems usually entail automated decision-making. However, the situation is not completely clear, as at any time humans may intervene in the decision-making and in consequence the protection granted by the Article 22 GDPR will not be applied.

CHAPTER 5.

FINAL CONCLUSION.

This thesis is aimed at giving insights into data protection risks of facial recognition systems (FRS) used in the private sector, with a focus on the use of FRS in commercial retail, FRS as means of authentication/verification (banking) and FRS used in social network sites. The central research question

[485] Ibid.
[486] See section 4.3.

aims, in addition, to explain how and to what extent the identification, security and profiling data protection risks are mitigated through the GDPR.

In this sense, in the chapter 2, state of the art of FRS art has been highlighted. First, a general description of FRS technologies, their characteristics, functionalities and their technological phases has been presented. A basic distinction is made between biometric systems used for authentication/verification and those used for identification. This distinction in functionality was necessary as these systems involve different risks. Verification/authentication is the 'determination of the validity of a biometric claim' whereas identification concerns "whether a biometric reference of a specific biometric data subject is in a biometric reference database or not."[487] Biometric features that are used in both identification and verification entail specific qualities: uniqueness, persistency and universality. In general, biometric technologies follow three phases: enrollment, comparison and decision. An FRS normally has four phases or steps that are inter-related. The first step is face detection, the second is normalization, the third is feature extraction, and the fourth and final step is recognition. Detecting the face in an image is not an easy task for computers since they must determine which pixels in the photo are part of the face. A blurred background and other inanimate elements might also generate complex issues in face detection. For the final step in the process, the effective recognition, a maximum amount of information is required. It is important for successful recognition that this maximum amount of information is retained so that the biometric template is sufficiently distinctive. Otherwise, successful recognition is not attained.

In chapter 2, a specific distinction was made among the automated facial recognition systems used in commercial stores (digital signage technologies), FRS as means of authentication/verification in banking and FRS used in social network sites.

In chapter 3, using Daniel Solove's 'taxonomy of privacy' harms as staring point, the risks of the afore-mentioned FRS technologies have been highlighted. Solove's 'taxonomy of harms' has been chosen in order to reveal different levels of acknowledgement within applications of the US and EU legal framework regarding the notion of privacy (US) and the "right to respect for private life" and data protection (EU). In addition, the taxonomy of 'privacy harms' does not refer at all to data protection and does not make any reference to the concept of risk or to the risk-based approach.

On the basis of this taxonomy and the analysis performed in chapter 2, the following risks have been addressed: identification, security and profiling.

With regard to the identification risks of the FRS used in social network sites, it has been exposed that, FRS can match, through a hyperlink, the pre-available images of the persons with the entirety of personal information, that is present on the social network profile of those persons. The uploaded photos on the social network sites may reveal sensitive information such as 'gender, birthday, political beliefs or any other status updates'[488] or specific metadata like 'the time, date or the user's physical location.'[489] In addition, a privacy research study has revealed that through the combination of the WEB 2.0 data (images)

[487] Ibid.
[488] See footnote 30. Welinder (2012).
[489] Ibid.

and the FRS available at large scale, re-identification of the social network site's users might be possible.[490] The experiment included both on-line and off-line re-identification, and has revealed sensitive information about the individuals. This experiment proved that the risks of re-identification were found to be very high, as even persons on the street that did not have social network profiles were identified. Moreover, as described under chapter 3, the FRS technologies used in commercial retail possess the ability of re-identification of the customers that 'were seen in a time slot.' A customer face is the only information needed to perform the process of identification.

The data protection risks are higher than many individuals may expect, by exposing their faces in public, other passers-by or companies in the retail business, will likely be able to recognize their faces and to affix their face to a name.

Furthermore, chapter 3 highlights the fact that, security lapses, attacks and abuses against FRS have diversified in time. As revealed by A29 WP 192 Opinion,[491]security breaches might occur during the data transit (in the case of online and mobile FRS) and during data storage in the identification and authentication/verification stages of FRS. Recent studies have demonstrated, in addition, that actual face authentication systems are capable of fooling or by-passing the FRS through external attacks and in particular, spoofing.[492]

As a supplementary protection for the image-spoofing counter-attacks, financial institutions[493] have implemented measures such as blinking authentication measures. However, the protection is not achieved, as the FRS were by-passed by presenting two simple images: one with an eye-closed and the other with an eye-opened.[494] In particular, a threat was identified in the form of the increasing capability of 'virtual reality and computer vision to be used as an adversarial tool' against FRS.[495]

As revealed under Chapter 3, designers of FRS are wrongfully assuming that the attackers do not have the necessary technical skills or the suitable materials for the attacks against FRS.[496]

Furthermore, the profiling risk of FRS is described in the last part of Chapter 3. As prescribed, along with the identification purposes, FRS used in commercial retail enable the creation of profiles and a categorization of their customers on the basis of their emotions or other socio-demographic features. The FRS used in commercial retail are designed to build a complete emotional and personalized profile of the customers[497], to create different levels of segmentation of their customers on the market and to deliver various advertisements offline. FRS are also capable of providing digital content to their customers

[490] See footnote 124. Acquisti et.al. (2014).
[491] Nevertheless, the weakness of the actual popular FRS has been highlighted under the Article 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192 available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf
[492] See footnote 23. Xu Yi et.al. (2013).
[493] See footnote 224. Vincent James (2016).
[494] See footnote 23.Xu Yi et.al. (2016).
[494] See footnote 224. Vincent James (2016).
[495] See footnote 23. Xu Yi et.al. (2013).
[496] Ibid.
[497] Ibid

online.[498] By matching the FRS with other databases or social networking sites, these retail companies will be capable of targeting individuals in accordance with their particular needs. Therefore, if FRS used in commercial retail can identify individuals and match a photo of their customer (which they capture) to a Facebook photo of an individual, their customer 'image' will become complete. The separate bits of information could be gathered to obtain a detailed image of the individual such as friendships, habits and tastes.[499]

The fourth chapter aims to identify how the identification, security and profiling data protection risks of the FRS are mitigated through the GDPR. In order to properly do so, a distinction between the 'right to respect for private and family life' and the definition of data protection in the EU legal framework was made, in the beginning of chapter 4. As revealed, in the literature and under the recent Schrems[500] case, the right of data protection has been extended and broadened over time and with the new GDPR, the right is regulated *in extenso* at the utmost level existent in the EU.

Chapter 4 discusses the concept of risk and the risk based approach from the GDPR perspective. The risk-based approach represents an important tool in assessing and managing the data protection risks of the FRS.[501] Critics of the 'risk-based approach', adopted by the GDPR, argue that it is contextual and provides insufficient and uneven protection, depending on how risky the processing is found to be. Even though, it is an important tool, the risk-based approach should not always be presented as a replacement for the well-established rights-based approach that is based on fundamental data protection rights and principles. Moreover, identification data protection risks of the FRS in the GDPR were mitigated through an assessment on whether digital facial images can be regarded as personal or sensitive data. The rational is simple: if digital facial images are found to be personal data, the protection granted by the data protection principles will be applicable. Furthermore, as facial images may fall under the special legal protection of sensitive personal data, processing of these special categories of data is in general prohibited, unless special requirements determined under Article 9(2) GDPR are fulfilled. The GDPR defines the concept of personal data under Article 4(1) as "any information relating to an identified or identifiable natural person."[502] Under a first impression, a digital facial image represents personal data that benefits from the safeguards of data protection.[503] However, the situation is not as simple as it first appears. As revealed, the images of individuals taken from a far distance or the ones that are blurred are usually unlikely to be considered personal data. Furthermore, if FRS are used only for categorization purposes (spotting the individuals emotions or their socio-demographic characteristics), the processing is

[498] See footnote 14.Lewinski et al. (2016).
[499] See footnote 16. Wall Mathew (2015).
[500] Case C-362/14 Maximillian Schrems v Data Protection Commissioner. Available at http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre= last accessed 12 of July 2017
[501] Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN, WP 218, Adopted on 30.05.2014. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf - last accessed 14 of July 2017
[502] See footnote 8. The GDPR.
[503] See footnote 95. Buckley Ben and Hunter Matt (2011).

not as of personal data. Due to these circumstances, following the GDPR approach, a separation between direct and indirect identifiers has been defined. Digital facial images might be regarded as personal data, as well, when they relate to an identifiable person. Digital images may embody particular characteristics of the individual's face. In the same manner, the digital facial images may be linked with a pre-determined individual's record or profile. In consequence, the results will likely be considered personal data. In addition, the 'proportionality' test proposed by the GDPR should be also mentioned. In considering whether a digital image processed by a facial recognition system is personal data, an "account should be taken to all means reasonably likely to be used**,** such as singling out, to identify the person directly or indirectly. However, the applicability of the GDPR does not necessitate, a high level of identification.[504]

By taking into account the available technology and technological developments in FRS, and the new conditions presented in recital 26 of the GDPR, the risk that an individual 'can be identified' or singled-out is considerably high.

In consequence, digital facial images processed through a FRS might be considered personal data and the safeguards guaranteed through data protection principles of the GDPR will be applicable. In this sense, A29 WP 193 has concluded when analyzing biometric data that, "these data may be processed only if there is a legal basis and the processing is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[505]
Digital facial images might fall, as well, under the special protection of sensitive data, as the new GDPR expressly mentions biometric data under the sensitive data definition. According to Article 9 (1) of the GDPR, processing of 'biometric data that are processed to uniquely identify a person' is prohibited. In addition, recital 51 of the GDPR is mentioning that the processing of the photographs should be considered as a special category of biometric data, when these data are **"**processed through a specific technical means allowing the unique identification and authentication of the natural person."[506] Thus, as FRS usage entails specific technical means that enable data controllers to identify and authenticate the natural persons, the processing of facial images shall fall under the special protection of the sensitive personal data. In FRS used in SNS, photographs on the internet may not be processed without a specific legal basis as consent. Moreover, in the case of FRS used in commercial retail, when personal data are processed, a freely given, specific, informed and unambiguous consent is required. It is disputable, however, the manner in which the customers might accept or opt out of the processing of personal data by the FRS in commercial retail. However, in the case of processing of sensitive data, informed and explicit consent is recommended for the FRS used in commercial retail. But, these requirements are not easily attained. It is more of the data controller and processor's responsibility to obtain the 'explicit informed consent' [507] as a basis for legal processing, since the customers might not be conscious of these

[504] European Court of Human Rights –Council of Europe, 'Handbook on European data Protection law'. Available at http://www.echr.coe.int/Pages/home.aspx?p=caselaw/otherpublications&c= -last accessed 25 of August 2017.
[505] See footnote 6. Article 29 WP 193.
[506] Recital 51 of the GDPR.
[507] Lewinski, P. (2015a). Automated facial coding software outperforms people in recognizing neutral faces as neutral from standardized datasets. Frontiers in Psychology, 6, 1386. Available at doi:10.3389/fpsyg.2015.01386- last accessed 28 of March 2017.

technologies and their usages. Consent is usually attained, in commercial retail, during the enrollment of the customers in loyalty programs.[508]

An explicit or express consent will be attained in writing with a handwritten signature and it should explicitly outline why a data controller is willing to gather and further process personal data. Alternative to consent, a solution will be the adoption in commercial retail of 'members only' shops.[509]

Consent from all end-users is required in the case of targeted advertising, processing of metadata and the content of metadata.[510] The processing of these data might include sensitive data and fall under Article 35 of GDPR.[511] In case of metadata, the provision of Article 7(3) of the GDPR, offers the assurance that the data subject shall have the right to withdraw his consent at any time' and that 'it should be easy to give and withdraw consent.'[512]

As have been found problematic, the requirement of granting consent, might not be in the end a good option at all, such as in the case of FRS that process personal or sensitive data. [513]

In this thesis, taking into account the new GDPR and the security risks of the FRS, the following data security measures have been proposed to mitigate the FRS security risks: encryption, pseudonimization, data breach notifications and data protection impact assessments. Regarding the encryption, the encrypted data will remain 'personal data' for the data controller that holds the decryption key. As a consequence, the GDPR data protection and principles will apply. But due to the robustness of the FRS, a pertinent question that must be answered is whether the encryption techniques proposed by the GDPR and A29 WP 192 can be regarded as viable technical and organizational measures. In addition to encryption in order to mitigate the security risks of the FRS, pseudonimization techniques might be adopted. The new GDPR suggests the pseudonymisation as a technique designed to minimize the data security risks towards the data subjects (recital 28 GDPR), or to reduce the 'linkability of the data with the original identity of the data subject.'[514] Pseudonymized data are still personal data under the GDPR. In consequence, data protection principles will be applied to these kinds of data as well. Similar to the encryption method, the issues with the pseudonymization techniques used in FRS, are related to the great challenges posed by hackers.[515]

---

[508] Ibid.
[509] Ibid.
[510] Ibid.
[511] Ibid.
[512] Article 7(3) of GDPR
[513] Article 29 Data Protection Working Party (2011). Opinion 5/2011 on the definition of consent, July 13, 2011. 00197/11/EN WP187. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf -last accessed 25 of August 2017.
[514] Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data, June 20, 2007. 01248/07/EN/ WP 136 available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf last accessed 4 June 2017.
[515] J. Galbally, S. Marcel and J. Fierez "Biometric Anti-Spoofing Methods: A Survey in Face Recognition " CAM under Project S2009/TIC-1485, in part by the Ministry of Economy and Competitiveness through the Bio-Shield Project under Grant TEC2012-34881. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6990726 –last accessed 15 of August 2017

Data breach notifications are provided, under the GDPR, as measures to mitigate the data security risks of FRS. In the case of data breaches, the GDPR adopts a risk-based approach, where data controllers do not necessarily need to notify supervisory authorities or data subjects about benign breaches. Therefore, notifications are required only, when a 'risk' or 'high risk' in the processing is identified by the data controller.

Another measure proposed to mitigate the data security risk is the data protection impact assessment (DPIA). In the GDPR, this measure should be taken as an anticipatory tool, whenever, the processing is likely to result in a high risk to the rights and freedoms of the data subjects**.**[516]

With regard to FRS, the DPIA is an important measure. Article 35 (3) of the GDPR mentions, in the form of a non-exhaustive list, inter alia*,* the obligation of assessing a DPIA in the case of[517]: evaluation or scoring, where processing of personal data implies automated decision-making (in the form of profiling, e.g. in case of FRS used in commercial retail); in the case of processing of systematic monitoring (data collected without the user's awareness in public areas and without knowledge about how the data might be used, e.g. FRS used in commercial retail); in the case of processing of sensitive data (e.g. digital image might be regarded as sensitive data) and data processed on a large scale[518] (FRS that are used for identification purposes and the ones that are used in commercial retail area fall under this criteria).

Finally, as described in Chapter 4**,** the concept of profiling is presented under the GDPR, as a "sub-category of the automated processing, and refers to the use of personal data to evaluate certain personal aspects of natural persons to analyze and predict certain aspects of life."[519] In the GDPR, profiling is prohibited whenever the decision-making is a result of a solely automated decision-making process. This provision is relevant in case of FRS used in retail or 'machine learning, given that proponents of the technology emphasize its ability to automate and facilitate decision-making processes.'[520] Conversely, whenever the profiling mechanism entails human intervention, in the decision-making process, article 22 will be not applicable. As depicted in Chapter 4, in the case of FRS used in commercial retail, humans intervene in the interpretation of the image, in analyzing the candidate lists or in examination of the matching. These activities, since they might fall under data collection and machine learning, are protected by Article 22 GDPR. However, it is disputable whether the automated decision-making process should be a final or interim one. What happens if a human intervenes during the FRS process in stages other than data collection or machine learning?

---

[516] Article 35 of GDPR.

[517] See footnote 446. Kamarinou et.al. (2016).

[518] Art. 29 Data Protection Working Party Opinion 03/2012 on purpose limitation. 00569/13/EN WP 203.Adopted on 2 April 2013. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf last accessed 23 August 2017.
In order to determine that, processing on a large scale has been undertaken, accounts should be taken on: "the number of data subjects concerned, either as a specific number or as a proportion of the relevant population; the volume of data and/or the range of different data items being processed; the duration, or permanence, of the data processing activity; d. the geographical extent of the processing activity.

[519] Ibid.

[520]See footnote 446. Kamarinou et.al (2016).

Nonetheless, profiling is not prohibited, if the decision-making based solely on automated processing is necessary in situations such as entering into a contract between the data controller and data subject or is based on the data subject's explicit consent.[521] In order to mitigate the risks of circumventing the protection granted by Article 22(1) GDPR, the data controller is obliged to implement "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[522]

Concluding remarks

On the basis of the analysis, it is almost impossible to use FRS without the processing of personal or sensitive data. As revealed in Chapter 4, there is a high probability that digital facial images fall under the personal or sensitive data category, as defined by the GDPR. In this sense, GDPR offers a sufficient legal protection, since the identification risks of the FRS are mitigated by the data protection principles underlined in Chapter 4 of this thesis. However, a data subject's consent as a legal basis for the data processing in case of FRS can pose problems in practice. In order to alleviate this problem, in this sense, one solution can be adopted in the form of 'noticeable signs', (where the data subject's consent is supposed to be implied when the data subjects are entering in the shops) which may be introduced by retailers, or 'member's shop only' services in case of FRS used in commercial retail. But, even though granted with the right of denial of the processing of their personal data, the consequences of refusal have the potential to keep the users out of the systems and to be helpless. As the burden of proof regarding the data subject's consent is on the data controller, an explicit consent obtained in 'writing' is can be regarded as a viable solution in the case of FRS used in commercial retail. In addition, FRS systems data security risks can be mitigated through the following measures: encryption, pseudonimization, data breach notifications and data protection impact assessment. An issue that may appear in mitigating these risks can be the robustness of the FRS and the increase in hacking and spoofing capabilities of the attackers. These measures should be adopted in light of the on-going shifting data security threat landscape. GDPR is conferring a sufficient legal protection, since it is adopting a flexible approach adapted to the "the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons."[523] Therefore, the technical and organizational measures are provided and should be adopted by the data controller, in an alternative way, by taking into account the above mentioned criteria.

[521] Article 22(2) GDPR.
[522] Article 22(3) GDPR.
[523] Article 32 of the GDPR.

The risk-based approach has been proven to be an important tool in the GDPR in assessing and mitigating the risks. For an appropriate adoption of Article 32 GDPR, the implementation of the suitable measures and over-simplification of the risk concept (to ensure a level of security appropriate to the risk) is important to be adopted by data controllers and data processors. It might be argued that, 'the risk based approach' is narrow and offers a limited protection. But this approach is beneficial in the case of data breach notifications, where the risk-based approach can eliminate benign breaches. In consequence, a fundamental maneuverability is granted, as well as for data controllers, since saving actions, might be taken at any level of data breaches. In consequence, the number of data breach notifications will be reduced significantly.

GDPR guarantees, too, maneuverability for data controllers in assessing the 'risk', in case of DPIA. Thus again, it is for the data controller to decide the 'qualified assessors, to ensure the robustness of the DPIA and to be aware of documentation and their entire accountability for the selection of the necessary method.'[524]

However, in particular, when it is 'not clear whether a DPIA is required, the A29 WP recommends that a DPIA is carried out nonetheless, since a DPIA is a useful tool to help data controllers comply with data protection law.'[525]

In addition, the GDPR is offering a relatively sufficient protection to data subjects in relation to profiling risks that arise from FRS technologies' data processing activities. A useful recommendation is the inclusion of 'semi-automated decision-making' in the Article 22 GDPR profiling definition. It is not completely clear if the provision will be applied when a human intervenes into the decision-making process. Therefore, the application of the Article 22 GDPR is not completely clear and is contextual.

Moreover, another recommendation will be that, besides the obligation of a data controller to provide the logic involved in decision-making, the GDPR is also proposing for data controllers the adoption of data-protection impact assessment or other ex-post measures.

Taking into account the analysis in this thesis, identification, profiling and security risks of FRS are considerable, and it is impossible for the FRS in commercial retail, banking or used in social networking sites to function without processing personal data. This state of affairs will force the compliance with the data protection principles, security and profiling guidelines of the new GDPR.

[524] See footnote 427. Kloza et al. (2017).

[525] Art. 29 Data Protection Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP248. Adopted on 4 of April 2017.

BIBLIOGRAPHY

i) Legislation

- Art. 29 Data Protection Working Party (2012a). Opinion 2/2012 on facial recognition in online and mobile devices March 22, 2012. 00727/12/EN WP192.
- Art. 29 Data Protection Working Party Opinion 03/2012 on purpose limitation. 00569/13/EN WP 203.Adopted on 2 April 2013.
- Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data, June 20, 2007. 01248/07/EN/ WP 136
- Article 29 Data Protection Working Party (2011). Opinion 5/2011 on the definition of consent, July 13, 2011. 00197/11/EN WP187.
- Article 29 Data Protection Working Party (2012b). Opinion 3/2012 on developments in biometric technologies, April 27, 2012. 00720/12/EN WP193.
- Article 29 Data Protection Working Party (2014). Opinion 5/2014 on Anonymization Technique, April 10, 2014. 0829/14/EN WP216.
- Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN, WP 218, Adopted on 30.05.2014.
- Article 29 Data Protection Working Party, Working document on biometrics, August 1, 2013. 00720/12/EN WP80.
- Article 29 Data Protection Working Party (2014). Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, April 9, 2014. 844/14/EN WP 217.
- Article 29 Data Protection Working Party. Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) 4 April 2017. 17/EN WP 247.
- Council of Europe, ETS no. 005, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, 4 November 1950.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002).
- Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 191/1/1.
- EU Charter of Human Rights, O.J. C 364, 18 December 2000.
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ,COM/2017/010 final - 2017/03 (COD).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 191/1/1.
- Universal Declaration of Human Rights, G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948).

ii) Research papers/Journal Articles

- Agagu TT and Akinnuwesi B., 'Automated Students' Attendance Taking in Tertiary Institution using Facial Recognition Algorithm' [2012] 19(2) Journal of Computer Science and Its Application. Available

at https://www.researchgate.net/publication/236003526_Automated_Students'_Attendance_Taking_in_Tertiary_Institution_using_Facial_Recognition_Algorithm -last accessed 2 September 2017.

- Alessandro Acquisti and others, 'Face Recognition and Privacy in the Age of Augmented Reality' [2014] 6(2) Journal of Privacy and Confidentiality 1-20
- Andrew Senior, Face De-Identification in Andrew Senior (ed), Protecting Privacy in Video Surveiilance (Ralph Gross 2009) 129 available at http://www.pitt.edu/~jeffcohn/biblio/facede.pdf last accessed 13 of July 2017 .
- Batagelj and others, 'Computer Vision and Digital Signage' [2008] Tenth International Conference on Multimodal Interfaces. Available at http://eprints.fri.uni-lj.si/1162/1/computer.vision.and.digital.signage.pdf last accessed 1 August 2017.
- Borut Batagelj and others, 'Computer Vision and Digital Signage' [2008] Tenth International Conference on Multimodal Interfaces. Available at http://eprints.fri.uni-lj.si/1162/1/computer.vision.and.digital.signage.pdf last accessed 1 August 2017.
- Buckley Ben and Hunter Matt, 'Say cheese! Privacy and facial recognition' [2011] 27 Computer Law & Security Review, 637–640. Available at http://www.its.ohiou.edu/bernt/ITS351/say%20cheese%20privacy%20and%20facial%20recognition.pdf – last accessed 25 of August 2017.
- Bygrave Lee, 'Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling' [2001] 17(1) Computer Law & Security Report. Available at http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf - last accessed 31 July 2017.
- Bygrave Lee, 'Privacy and Data protection in an international perspective [2010] 56(1) Scandinavian Studies in Law 165-200. Available at https://pdfs.semanticscholar.org/695f/434a1111f254c2c3104811f4851324b1de35.pdf -last accessed 23 of August 2017
- Calo M, 'The Boundaries of Privacy Harm ' [2011] 86(1) Indiana Law Journal p. 1132-1161.Available at http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf -last accessed 23 of August 2017
- Cavoukian Ann, 'Privacy and Biometrics for Authentication Purposes: A Discussion of Untraceable Biometrics and Biometric Encryption.' in Kumar, Ajay, Zhang, David (ed), Ethics and Policy of Biometrics-Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, Hong Kong (Springer Berlin Heidelberg2010) 16. Available at http://www.springer.com/gp/book/9783642125942 -last accessed 30 of July
- Chellapa Rama and others, 'Face recognition by computers and humans' [2010] 43(2) IEEE Computer Society. Available at http://ieeexplore.ieee.org/document/5410708/ -last accessed 23 of August 2017.
- Chibba Michelle and Alex Stoianov, 'On Uniqueness of Facial Recognition Templates' [2014] 1(1) NTIA US Department of Commerce Privacy Multi-stakeholder Process: Facial Recognition Technology. Available at https://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf -last accessed 23 of August 2017.
- Cootes, T., & Taylor, C. (2000). Statistical models of appearance for computer vision. Technical report, University of Manchester, Wolfson Image Analysis Unit, Imaging Science and Biomedical Engineering. University of Manchester :U.K. Available at http://www.face-rec.org/algorithms/AAM/app_models.pdf - last accessed 17 of July 2017.
- De Hert Paul and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" Computer Law and Security Review [2016] 32 (2) 179–94.Available at http://daneshyari.com/article/preview/466369.pdf -last accessed 3 of September 2017.
- De Luis Garcia Rodrigo et al, 'Biometric Identification Systems' [2003] 83(12) Elsevier Signal Processing. Available at http://dx.doi.org/10.1016/j.sigpro.2003.08.001 - last accessed 16 February 2017.
- De Marisico Maria and others, Face Recognition in Adverse Conditions (1 edn, IGI Global 2014) 361. Available at https://www.di.ubi.pt/~hugomcp/doc/IGI_Face.pdf -last accessed 28 of July 2017.
- Duc Nguyen and Buy Minh, 'Your face is not your password' [2009] 1(1) Security Vulnerability Research Team Bach Khoa Internetwork Security (Bkis) Ha Noi University of Technology – VietNam. Available

at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.8363&rep=rep1&type=pdf -last accessed 30 July 2017.

- Erdogmus N and Marcel S., Spoofing face recognition with 3d masks. Information Forensics and Security, IEEE Transactions *on*, 9(7):1084–1097, 2014. Available at https://www.researchgate.net/publication/262605045_Spoofing_Face_Recognition_With_3D_Masks - last accessed 20 Of July 2017
- Farinella GM and others, 'Face Re-Identification for Digital Signage Applications' [2014] Springer Image Processing Laboratory, Department of Mathematics and Computer Science University of Catania. Available at http://iplab.dmi.unict.it/download/VAAM2014/FinalPaper.pdf -last accessed 1 August 2017
- Farrel Henry, 'Constructing the International Foundations of E-Commerce—The EU-US Safe Harbor Arrangement' [2003] 57(1) International Organization <DOI: 10+10170S0020818303572022> accessed 17 August 2017. Available http://www.henryfarrell.net/IO.pdf -last accessed 23 of August
- Fuster Gloria Gonzalez and Gellert R.,'The fundamental right of data protection in the European Union: in search of an uncharted right' [2012] 26(1) International Review of Law, Computers & Technology 73-82. Available at http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.646798 -last accessed 23 of August 2017.
- Gellert R., 'Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing'' [2017] 1(1) Trends and Communities of legal informatics: IRIS2017 - Proceedings of the 20th International Legal Informatics Symposium Schweighofer, E, Kummer, F & Sorge, C (eds) Austrian Computer Society 527-532. Available at https://www.researchgate.net/publication/314839054_Why_the_GDPR_risk-based_approach_is_about_compliance_risk_and_why_it's_not_a_bad_thing -last accessed 25 of August 2017.
- Gellert R.,'We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection' [2016] 4(2) European Data Protection Law Review (EDPL) 481-492. Available at https://www.researchgate.net/publication/312652929_We_Have_Always_Managed_Risks_in_Data_Protection_Law_Understanding_the_Similarities_and_Differences_Between_the_Rights-Based_and_the_Risk-Based_Approaches_to_Data_Protection - last accessed 10 of July 2017.
- Gerard Spindel and Phillip Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' [2016] 7(1) JIPITEC- Journal of Intellectual Property Information technology and E-commerce Law. Available at http://www.jipitec.eu/issues/jipitec-7-2-2016/4440/spindler_schmechel_gdpr_encryption_jipitec_7_2_2016_163.pdf -last accessed 12 of July 2017.
- Hildebrand, Defining Profiling: A New Type of Knowledge? in M. Hildebrand and S Gutwirth (eds), Profiling the European Citizen (Springer Science 2008) 17-45. Available at https://link.springer.com/chapter/10.1007%2F978-1-4020-6914-7_2 –last accessed 23 of August 2017.
- Hildebrand, 'Profiling from data to knowledge the challenges of a crucial technology [2006] 30(9) Datenschutz und Datensinchercheit. Available at <https://pdfs.semanticscholar.org/c0a1/aa843e812925127dfb8f9540089e1a0a72b5.pdf> -last accessed 14 July 2017.
- Hon,Kosta,Millard,Stefanatou, Tilburg Law School Legal Studies Research Paper Series No. 07/2014, p. 9, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405971 last accessed 14 of June 2017
- Iglezakis, I. 'EU Data protection legislation and case-law with regard to biometric application'. (Aristotle University of Thessaloniki, 18 June 2013). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2281108 – last accessed 18 February 2017
- Indra Spiecker Genannt Döhmann and others 'A Comparative Analysis' [2016] 2(4) European data Protection Law Review 535-554. Available at https://ueaeprints.uea.ac.uk/63337/1/EDPL_4_2016_Country_Reports_section_EMR_INTERNALUSE_Rep1.pdf last accessed 13 of July 2017

- Introna Lucas D. and Nissenbaum, Helen, Facial Recognition Technology: A Survey of Policy and Implementation Issues (July, 22 2009). Center for Catastrophe Preparedness and Response, New York University. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1437730
- J. Galbally, S. Marcel and J. Fierez "Biometric Anti-Spoofing Methods: A Survey in Face Recognition " CAM under Project S2009/TIC-1485, in part by the Ministry of Economy and Competitiveness through the Bio-Shield Project under Grant TEC2012-34881 available at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6990726
- Jain Anil and Kumar Ajay, Biometric Recognition: An Overview. in Emilio Mordini and Dimitrios Tzovaras (eds), Second Generation Biometrics: The Ethical, Legal and Social Context(Springer Netherlands- The International Library of Ethics, Law and Technology' 2012) 49- 79. Available at https://link.springer.com/chapter/10.1007%2F978-94-007-3892-8_3 -last accessed 21 April 2017.
- Jain Anil and others, '50 years of biometric research: Accomplishments, challenges, and opportunities' [2016] 79(1) Pattern recognition letters- Elsevier 80-105. Available at https://www.researchgate.net/publication/290509735_50_Years_of_Biometric_Research_Accomplishments_Challenges_and_Opportunities -last accessed 23 of August 2017.
- Kamarinou Dimitra and others, 'Machine Learning with Personal Data' [2016], Queen Mary School of Law Legal Studies Research Paper No 247/2016 . Available at SSRN: <https://ssrn.com/abstract=2865811> - last accessed 1 August 2017
- Kerckhoffs, ''La cryptographie militaire,'' J. Sci. Militaires, vol. 9, pp. 5–83, Jan./Feb. 1883. Available: http://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf -last accessed 15 August 2017.
- Keyurkumar Patel and others, 'Secure Smartphone Unlock: Robust Face Spoof Detection on Mobile' [2015] 15(15) MSU Technical Report MSU-CSE-15-15, Oct 21, 2015 1-13. Available at https://pdfs.semanticscholar.org/bfd2/505fbc432cd0def950b7d099fd4797b562e1.pdf -last accessed 23 of August 2017.
- Kindt Els, 'Biometric application and the data protection legislation- the legal review and the proportionality test' [2007] 31(3) Datenschutz und Datensicherheit 166-170. Available at http://www.fidis-project.eu/fileadmin/fidis/publications/2007/DuD3_2007_166.pdf - last accessed 30 of July 2017.
- Kindt Els, Doctoral thesis 'The processing of Biometric Data- A Comparative Legal Analysis with a focus on the Proportionality Principle and recommendations for a Legal framework ', Katholieke Univerisiteit Leuven 2012 available at https://lirias.kuleuven.be/bitstream/123456789/345184/1/PH_D_text_PartI%2BPartII_17.04-Pservice.pdf last accessed 10 of July 2017
- Kloza Dariusz and others, 'Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals' [2017] (1) Brussels Laboratory for Data Protection & Privacy Impact Assessments (dpialab). Avaialble at http://virthost.vub.ac.be/LSTS/dpialab/images/dpialabcontent/dpialab_pb2017-1_final.pdf –last accessed 14 July 2017.
- Kokott Juliane and Christoph Sobotta, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, International Data Privacy Law, Vol. 3, No. 4 (2013). Available at http://oxfordindex.oup.com/view/10.1093/idpl/ipt017 -last accessed 23 of August 2017.
- Koops Bert-Jaap and others, 'A Typology of Privacy' [2016] 38(1) University of Pennsylvania Journal International law. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2754043 -last accessed 22 March 2017
- Koops Bert-Jaap, 'On decision transparency, or how to enhance data protection after the computational turn' in Mirelle Hildebrant and Katja De vries (eds), Privacy, due process and the computational turn (Abingdon: Routledge 2013) 196-220. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2367510 –last accessed 23 of July 2017.

- Kuner Cristopher and others , Risk management in data protection, International Data Privacy Law, Vol. 5, No. 2, (2015), 95. Available at https://academic.oup.com/idpl/article/5/2/95/645238/Risk-management-in-data-protection -last accessed 23 of August 2015.
- Leenes Robert, 'Accountability and transparency in Big Data land' (DSC/t Blog - May 2016-Tilburg Institute for Law, Technology, and Society; TILT, Tilburg Law School). Available at https://www.tilburguniversity.edu/research/institutes-and-research-groups/data-science-center/blogs/data-sience-blog-ronald-leenes/ -last accessed 31 July 2017
- Lewinski Peter and others, 'Face and Emotion Recognition on Commercial Property under EU Data Protection Law' [September 2016] 33(9) Psychology & Marketing, Wiley Periodicals 729-746. Available at http://onlinelibrary.wiley.com/doi/10.1002/mar.20913/abstract last accessed 30 of July 2017.
- Lewinski, P. (2015a). Automated facial coding software outperforms people in recognizing neutral faces as neutral from standardized datasets. Frontiers in Psychology, 6, 1386. Available at doi:10.3389/fpsyg.2015.01386- last accessed 28 of March 2017
- Lundevall-Unger P and Tranvik T, 'IP Addresses – Just a Number?' (2011) 19 International Journal of Law and Information Technology 53 Available at https://academic.oup.com/ijlit/article-abstract/19/1/53/706223/IP-Addresses-Just-a-Number?redirectedFrom=fulltext –last accessed 23 of August 2017.
- Luzak, J. (2013). Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies. European Review of Private Law, 1, 221–246. Available at https://www.kluwerlawonline.com/abstract.php?area=Journals&id=ERPL2013007 –last accessed 23 of August 2017.
- Mike Hintze, 'Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency' [2017] Hintze Law PLLC; University of Washington School of Law 1-available at https://fpf.org/wp-content/uploads/2016/11/M-Hintze-GDPR-Through-the-De-Identification-Lens-31-Oct-2016-002.pdf
- Millar Stephen, 'Privacy Impact Assessment (PIA) - BioConnect: combining facial recognition and MAC address tracking for authorising access to Wi-Fi' [2016] Queen's University Belfast. Available at http://pure.qub.ac.uk/portal/files/123692281/StuartMillar_13616005_PIA.pdf%20p.3 - last accessed 1 August 2017.
- Monteleone Shara, 'Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?' [2012] 3(3) European Journal of Law and Technology. Available at http://ejlt.org/article/view/168/257 - last accessed 19 January 2017.
- Montjoye, "Computational Privacy: Towards Privacy Conscientious Use of Metadata", Massachusetts Institute of Technology 2015 available at https://dam-prod.media.mit.edu/x/files/thesis/2015/yva-phd.pdf -last accessed 15 of August 2017
- Movius L and Krup N, 'US and EU Privacy Policy: Comparison of Regulatory Approaches [2009] (3) International Journal of Communication 169-187. Available at http://ijoc.org/index.php/ijoc/article/viewFile/405/305..- last accessed 15 of August 2017.
- Patil Shailaja and PJ Deore, 'Face Recognition: A Survey' [2013] 1(1) Informatics Engineering, an International Journal (IEIJ) 31-41. Available at https://pdfs.semanticscholar.org/9166/643aabcd5261299fbcd7c949246d71ec0b3e.pdf -last accessed 25 of August 2017.
- Pato Joseph and Lynet Myllet, Biometric Recognition: Challenges and Opportunities (1st ed. National Academy of Science 2010) 4.Available at https://dataprivacylab.org/TIP/2011sept/Biometric.pdf -last accessed 25 of August 2017.
- Phillips Jonathon and Alice O'Toole, 'Comparison of human and computer performance across face recognition experiments' [2014] 32(1) Image and Vision Computing. Available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913011 – last accessed 31 July 2017.
- Phillips P.J. et al., "FRVT 2006 and ICE 2006 Large Scale Results," IEEE Trans. Pattern Analysis and Machine Intelligence, forthcoming; DOI 10.1109/TPAMI.2009. Available at http://pages.cs.wisc.edu/~dyer/cs534/papers/face-recog-2010.pdf- last accessed 30 of July 2017.

- Rodotà S. (2009) Data Protection as a Fundamental Right. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht. Available at https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_3 -last accessed 23 of August 2017.
- Rodrigues and others (2016). Data protection and privacy issues concerning facial image processing in public spaces. Athens Journal of Technology and Engineering, 3 (1), 39-52. Available at https://www.athensjournals.gr/technology/2016-3-1-3-Rodrigues.pdf
- Roosendaal Arnold, Digital personae and profiles in law: Protecting individuals' rights in online contexts (1st edn, Oisterwijk: Wolf Legal Publishers (WLP) 2013). Available at https://pure.uvt.nl/ws/files/1515346/Roosendaal_digital_21-05-2013_emb_tot_22-08-2013.pdf last accessed 23 of August 2017
- S. Lu and A. Jain, 'Ethnicity identification from face images' in Proceedings SPIE Defense and Security Symposium, Orlando, April 2004. Available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.2036 –last accessed 23 of July 2017.
- Savin, A. (2014) Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks. Paper presented at 7th International Conference Computers, Privacy & Data Protection, Brussels, Belgium. Available at http://openarchive.cbs.dk/bitstream/handle/10398/8914/Savin.pdf?sequence=1 –last accessed 23 of August 2017.
- Shi, J., Samal, A., & Marx, D. (2006). How effective are landmarks and their geometry for face recognition? Computer Vision and Image Understanding, 102(2), 117–133. Available at http://dl.acm.org/citation.cfm?id=1143473 last accessed 23 of August 2017.
- Slovic Paul and Elke U. Weber, Perception of Risk Posed by Extreme Events Center for Decision Sciences, (CDS) Working Paper Columbia University, (2002), 4. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2293086 –last accessed 23 August 2017.
- Slovic Paul.,'Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield.'In M H Bazerman, D M Messick, A E Tenbrunsel, & K A Wade-Benzoni (Eds), Environment, ethics, and behavior (pp 277-313) San Francisco: New Lexington' [1999] 19(4) 689-701. Available at https://www.ncbi.nlm.nih.gov/pubmed/10765431 -last accessed 25 of August 2017.
- Solove Daniel, 'A TAXONOMY OF PRIVACY' [2006] 154(3) University of Pennsylvania Law Review. Available at https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf –last accessed 24 of August 2017
- Trzaskowski, J., Savin, A., Lundqvist, B., & Lindskoug, P. (2015). Introduction to EU Internet Law. Copenhagen: Ex Tuto Publishing. Available at http://research.cbs.dk/en/publications/introduction-to-eu-internet-law(f3be5ade-8036-4c1a-a27d-510ee97d46de)/export.html -last accessed 23 of August 2017.
- Van der Sloot B. (2017) Legal Fundamentalism: Is Data Protection Really a Fundamental Right? in: Leenes R., van Brakel R., Gutwirth S., De Hert P. (eds) Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series, vol. 36. Springer. Available at https://link.springer.com/chapter/10.1007/978-3-319-50796-5_1 -last accessed 26 of August 2017.
- Viola, P and Jones, M., 2004. Robust Real-time Face Detection. International Journal of Computer Vision 57(2), 137–154. Available at http://www.vision.caltech.edu/html-files/EE148-2005-Spring/pprs/viola04ijcv.pdf -last accessed 23 of August 2017.
- Welinder Yanna, 'A FACE TELLS MORE THAN A THOUSAND POSTS: DEVELOPING FACE RECOGNITION PRIVACY IN SOCIAL NETWORKS' [2012] 6(1) Harvard Journal of Law & Technology 166-192.Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108 –last accessed 25 of August 2017.
- Wisnieski Pamela and others, 'Facebook Apps and Tagging: The Trade-off Between Personal Privacy and Engaging with Friends' [2015] 66(9) JOURNAL OF THE ASSOCIATION FOR INFORMATION SCIENCE AND TECHNOLOGY 1883-1896. Available at http://onlinelibrary.wiley.com/doi/10.1002/asi.23299/abstract -last accessed 23 of August 2017.
- Woodward John, Horn Christopher, Gatune Julius "Biometrics. A look at facial recognition" Virginia State crime Commission, RAND Documented briefing. Available at https://www.rand.org/pubs/documented_briefings/DB396.html -last accessed 23 of August 2017.

- Xu Yi and others, 'Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos' [2016] The University of North Carolina at Chapel Hill. Available at https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_xu.pdf -last accessed 15 of August 2017.

iii) Books

- Christopher Hood et al, 'Risk Management' in The Royal Society (ed), Risk: Analysis, Perception and Management - A Report of a Royal Society Study Group (The Royal Society 1992).
- De Marisico Maria and others, Face Recognition in Adverse Conditions (1 edn, IGI Global 2014) 361. Available at https://www.di.ubi.pt/~hugomcp/doc/IGI_Face.pdf -last accessed 28 of July 2017.
- De SJ and Daniel Le Metayer, Privacy Risk Analysis (Morgan & Claypool Publishers 2016) 7. Available at http://www.morganclaypool.com/doi/pdf/10.2200/S00724ED1V01Y201607SPT017 -last accessed 26 of August 2017.
- European Court of Human Rights –Council of Europe, 'Handbook on European data Protection law'. Available at http://www.echr.coe.int/Pages/home.aspx?p=caselaw/otherpublications&c= -last accessed 25 of August 2017.
- Fuster Gloria Gonzalez, The Emergence of Personal Data Protection as a Fundamental Right of the EU (Springer: Law Governance and technology Series 2014) 21.Available at http://www.springer.com/gp/book/9783319050225 -last accessed 26 of August 2017.
- Hildebrandt M and Serge Gurtwirth, 'Profiling the European Citizen, Springer (2008). Available at http://www.springer.com/gp/book/9781402069130 -last accessed 26 of August 2017.
- Kindt Els, Privacy and Data Protection Issues of Biometric Applications A comparative legal analysis (1st edn. Springer, Governance and Technology Series 12, 2013) 14. Available at http://www.springer.com/gp/book/9789400775213 -last accessed 30 of July 2017.
- Lynskey O, The Foundations of EU Data Protection Law (Oxford University Press 2015). Available at https://global.oup.com/academic/product/the-foundations-of-eu-data-protection-law-9780198718239?cc=nl&lang=en& -last accessed 26 of July 2017.
- Solove Daniel, Understanding Privacy (1 edn, Cambridge: Harvard University Press 2008).Available at http://www.hup.harvard.edu/catalog.php?isbn=9780674035072 –last accessed 26 of August 2017.
- Vacca John, Biometric Technologies and Verification Systems (1st edn, Elsevier 2007). Available at https://booksite.elsevier.com/samplechapters/9780750679671/Sample_Chapters/01~Front_Matter.pdf - last accessed 30 of July 2017.

IV) On-line sites/Blogs/Reports

- Allison Grande, 'Amazon's Execution Key To Dodging 'Selfie Pay' Woes' (Law 360, may 2016). Available at https://www.law360.com/articles/773543/amazon-s-execution-key-to-dodging-selfie-pay-woes - last accessed 3 August 2017.
- Forbes, 'Forbes.com' (*Why Did Apple Acquire Facial Recognition Company RealFace?*, 22 February 2017). Available at https://www.forbes.com/sites/quora/2017/02/22/why-did-apple-acquire-facial-recognition-company-realface/#3e51d528500b –last accessed 15 August 2017.
- Arthur Charles, 'The Guardian' (Facebook in new privacy row over facial recognition feature, 8 June 2011). Available at https://www.theguardian.com/technology/2011/jun/08/facebook-privacy-facial-recognition - last accessed 15 February 2017.

- Biometric Update Research-Mobile Biometric Market Analysis. Available at http://www.biometricupdate.com/wp-content/uploads/2015/10/287127021-Mobile-Biometrics-Market-Analysis-5.pdf - last accessed 22 February 2017
- CSC press release, 'New CSC Research Reveals Where Shoppers and Retailers Stand on Next Generation In-store Technology-Big Data & Customer Analytics – a key driver for UK Retailers' (CSC, 10 September 2015) . Aavailable at http://www.csc.com/uk/press_releases/133753-new_csc_research_reveals_where_shoppers_and_retailers_stand_on_next_generation_in_store_technology –last accessed 19 January 2017.
- David Goldman, *In the Future, Can You Remain Anonymous?*, CNN MONEY (Jan. 13, 2012). Available at http://money.cnn.com/2012/01/13/technology/face_recognition/indexhtm?iid=EL – last accessed 31 of July 201
- Exeler J and others, 'Digital Signs that react to Audience Emotion. 2nd Workshop on Pervasive Advertising, [2009] 38-44. Available at https://pdfs.semanticscholar.org/ad2f/73a6f3735d4651c1199aa595385e2c65effc.pdf -last accessed 29 of July 2017
- Griffin Andrew, 'Facebook facial recognition algorithms can recognize people even if they hide faces' (Independent UK, 24 June 201. Available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-facial-recognition-algorithms-can-recognise-people-even-if-they-hide-their-face-10342195.html - last accessed 5 January 2017
- Jay P Rosemary, 'Data protection and Privacy in 31 jurisdiction wordwide' (Hunton and Williams, 2015). Available at https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf -last accessed 3 August 2017.
- Justin Mitchell, *Making Photo Tagging Easier*, THE FACEBOOK BLOG (June 30, 2011).
- Iplens, 'Personal data processing for marketing purpose under the new GDPR: consent v legitimate interest and Recital 47 – first thoughts' (IPlens, 12 July 2017). Available at https://iplens.org/2016/07/12/personal-data-processing-for-marketing-purpose-under-the-new-gdpr-consent-v-legitimate-interest-and-recital-47-first-thoughts/ - last accessed 7 September 2017.
- Kashmir Hill, You are secretly tracked with facial recognition even in church June 2015, Fusion net Available at http://fusion.net/story/154199/facial-recognition-no-rules/ -last accessed March 2017.
- Maldoff Gabriel, 'Top 10 operational impacts of the GDPR: PART 8 – Pseudonymization' (Iapporg, 12 February 2016). Available at https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/ -last accessed 7 September 2017.
- Maldoff Gabriel, 'The Risk-Based Approach in the GDPR: Interpretation and Implications' (Iapporg, 29 March 2016). Available at https://iapp.org/resources/article/the-risk-based-approach-in-the-gdpr-interpretation-and-implications/ -last accessed 7 September 2017.
- Marios Savvides, 'Introduction to Biometric Technologies and Applications, Carnegie Mellon CityLab. Available at https://users.ece.cmu.edu/~jzhu/class/18200/F06/L10A_Savvides_Biometrics.pdf - last accessed 25 of May 2017.
- Newman Lily Hay, 'Hackers Trick Facial-Recognition Logins With Photos From Facebook (What Else?)' (Wiredcom, 19 August 2016). Available at https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/ - last accessed 15 August 2017
- NOVETTA WHITEPAPER, "Opportunities in Analyzing and Processing Online Face Images", August 2016. Available at http://www.novetta.com/wp-content/uploads/2016/09/NovettaBiometrics_OnlineFaceProcessing_WP-W_9112016.pdf
- npr.org, 'High-End Stores Use Facial Recognition Tools To Spot VIPs' (npr.org, 21 July 2013). Available at http://www.npr.org/sections/alltechconsidered/2013/07/21/203273764/high-end-stores-use-facial-recognition-tools-to-spot-vips - last accessed 20 January 2017.
- Palmer Maija, 'Regulators probe Facebook's facial recognition' (Financial Times, 9 June 2011). Available https://www.ft.com/content/ffe3edb4-92c8-11e0-bd88-00144feab49a - last accessed 5 December 2016

- S Path, 'General Data Protection Regulation- Anonymization and Pseudonimization And I sit here without identity: faceless. My head aches' [2016] 1(1)PricewaterhouseCoopers Legal LLP (London). Available at https://www.pwc.lu/en/general-data-protection/docs/pwc-anonymisation-and-pseudonymisation.pdf –last accessed 6 September 2017.
- Phillips P.J. et al., "FRVT 2006 and ICE 2006 Large Scale Results," IEEE Trans. Pattern Analysis and Machine Intelligence, forthcoming. Available at DOI 10.1109/TPAMI.2009.59. -last accessed 30 of July 2017.
- Rawlson King, 'Facial recognition' (BiometricUpdate, 10 January 2016). Available at http://www.biometricupdate.com/201501/history-of-biometrics - last accessed 23 February 2017.
- Rice Simon, 'How shops can use your phone to track your every move and video display screens can target you using facial recognition' (Information Commissioner's Office (21 January 2016). Available at https://iconewsblog.wordpress.com/2016/01/21/how-shops-can-use-your-phone-to-track-your-every-move/ - last accessed 24 February 2017.
- Richardson Deidre, 'Mastercard's new "selfie authentication" takes advantage of photo feature popularity' (*Inferse.com*, 5 July 2015). Available at http://www.inferse.com/34105/mastercards-selfie-authentication-takes-advantage-photo-feature-popularity/ - last accessed 20 February 2017. See also "Lloyds says Hello to the facial recognition banking". Available at https://www.ft.com/content/923fec7c-205c-11e7-b7d3-163f5a7f229c last accessed 28 of March 2017.
- Russel Daniel 'Interactive Digital Signage: An ebay Pop up with Face Recognition in London' (Digital Signage Summit Event, 15 December 2016). Available at http://digitalsignagesummit.org/blog/2016/12/15/interactive-digital-signage-an-ebay-pop-up-with-face-recognition-in-london/ - last accessed 21 February 2017.
- Stacy Gray, 'Privacy Principles for Facial Recognition Technology' (Future of Privacy Forum, December. Available at https://fpf.org/2015/12/09/facial-recognition-and-privacy/ -last accessed 25 of August 2017.
- Tractica, 'Facial Recognition Devices and Licenses Will Reach 122 Million Annually by 2024' (Tractica.com, 26 June 2015). Available at https://www.tractica.com/newsroom/press-releases/facial-recognition-devices-and-licenses-will-reach-122-million-annually-by-2024/ - last accessed 16 February 2017.
- VicarVision, VicarVision Retail Analytics website (2016). Available at http://www.vicaranalytics.com/ -last accessed 18 of January 2016.
- Victoria Woolastone, 'Pay with a WINK! Amazon patents system that uses selfies and blinking to pay online', DailyMail available at http://www.dailymail.co.uk/sciencetech/article-3492903/Pay-WINK-Amazon-patents-uses-selfies-blinking-pay-online.html last accessed 25 March 2017.
- Vincent James, MasterCard unveils 'selfie' security checks, says heartbeat authentication could follow", The Verge, 23 February 2016. Available at http://www.theverge.com/2016/2/23/11098540/mastercard-facial-recognition-heartbeat-security -last accessed 25 March 2017.
- Wall Mathew, Is Facial recognition tech a real threat to privacy? , BBC news,June 2015, Available at http://www.bbc.com/news/technology-33199275 last accessed 25 of July 2017.

V) Case-law

- Rynes (Judgment) [2014] EU
- Case C-362/14 Maximillian Schrems v Data Protection Commissioner available at http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre= last accessed 12 of July 2017 -ECJ C-212/13 (11 December 2014)