DIGITAL IDENTITY: BETWEEN HUMAN RIGHTS AND CYBERCRIMES

Manlio d'Agostino Panebianco

Abstract [ita]: nella moderna società globalizzata, la dimensione digitale ha modificato i paradigmi degli stili di vita, in specie nel cyberspazio: oggigiorno, le relazioni interpersonali si instaurano e si intrattengono sempre più attraverso i *social-networks*, che attraverso la crescente creazione dei "profili", favoriscono una maggiore condivisione online di dati personali. purtroppo, la maggior parte dei cittadini-digitali sono poco consapevoli dei rischi a cui si espongono: dal punto di vista strettamente legale, riguarda sia le libertà ed i diritti fondamentali, ma anche la possibilità di diventare vittime degli emergenti *cybercrimes*. in questo contributo, ci si vuole focalizzare sull'identità digitale e sui crescenti reati correlati, attraverso la disamina dei principali (trattamento illecito di dati personali, furto d'identità, diffamazione, *cyber*-bullismo, violazioni informatiche, etc.), con una doppia prospettiva - italiana ed internazionale – così da poter offrire alcuni spunti di approfondimento e casistiche da analizzare.

Abstract [eng]: In a globalised society, the digital dimension changed the paradigms of lifestyle in cyberspace: relationships are more and more based on On-line-Social-Networks, which implies the creation of account-profiles, with a consequent sharing of personal-data. Since most digital-citizens are mostly unaware, from a legal perspective they are exposed to many risks, for their fundamental rights and freedoms, and even being victims of many of cyber-crimes. In this paper, the focus is on digital identity, and on the increasing issue of "identity crime", considering the most possible offences (unlawful data processing, forgery, identity theft, defamation, cyberbullying, violation of IT systems, etc.), through literature and from both international and Italian point of view, in order to give some practical hints and applications.

Keywords: Digital Identity, Impersonation, Cyberbullying, Privacy, Fundamental Rights.

1. The new social contest and the arising issues.

One of the most important joint-effect of Globalization and the widespread use of *digital technologies*[1] significantly modified relationships in economy and society, both in terms of quality and quantity. ICT also changed many paradigms in lifestyle, generating considerable positive effects, but also exposing modern citizens to new considerable risks, due to an expansion of unlawful activities and behaviours.

In fact, in the *Information Society* it is possible to identify[2] three different dimensions of the life of a natural person, which overlap and interact with each other, especially in everyday behaviour and legal effects: the first is the *real dimension*, that is the traditional one characterized by direct contact, and of the five senses; the second one is the *digital*, which is intermediated by a device, the Internet, apps and generally by all new forms of IC Technology, which sometimes can cancel distances and time, and soon it became an integral part of the social and labour sphere[3]; the third one, is so called the *virtual* to which belong all those forms of tools (aroused naturally and spontaneously from online communities)[4] but have not yet acquired legal recognition and validity (such as virtual currencies or cryptocurrencies, *e.g.* Bit-Coin)[5].

The *Information Society*, because of its nature as a social organization and lifestyle and full expression of *techne*, beyond the expected benefits has, since its inception, brought out a series of ethical issues, whose extent and complexity are proportional to the range and speed of growth and evolution. Floridi[6] affirms that, nowadays, it is necessary and urgent to develop «an information ethics that can treat the world of data, information, and knowledge, with their relevant life cycles (including creation,

1 *I.e.*, Information and Communication Technologies, ICT.
2 M. D'AGOSTINO PANEBIANCO, *Vivere nella dimensione Digitale*, Themis ed., 2019, p. 14 ss.
3 These two dimensions are complementary to each other, and both produce both social and legal effects, and it is appropriate to consider the second one as the modern and innovative evolution of the first one.
4 According to a bottom-up process.
5 In order to better clarify the meaning of this latter dimension, it seems appropriate to highlight at least three different considerations: since this last dimension is not firstly framed in a previous (legal) context, this should be considered as *uncertain* or even devoid of any legal effect; secondly, considering the speed and normal evolution of modern phenomena, any innovative solution is expected that soon will assume a recognized value, thanking to the intervention of a State or a National or Supranational Authority; then, it is important not to identify and confuse the *digital* with *virtual* dimension, creating misunderstanding especially in not specialized citizens, since it would increase the risk exposure to damages and cybercrimes conducts.
6 L. FLORIDI, *Foundations of Information Ethics*, in K.E. HIMMA, H.T. TAVANI (a cura di), *The handbook of information and computer ethics*, Wiley, 2008, p.3 ss.

elaboration, distribution, communication, storage, protection, usage, and possible destruction), as a new environment, the *infosphere*, in which humanity is and will be flourishing. An information ethics should be able to address and solve the ethical challenges arising in the *infosphere*»[7].

This social and technological perspective premise is important to frame and focus the object and purposes of this paper, which aims to address a legal examination of the arising issues. As a matter of facts, in modern devices (*i.e.*, smartphones and tablets) are stored many information about our private life (contacts, pictures, travel history, financial information, and often intimate conversations) which belong to the personal sphere and constitute a part of our *identity*; moreover, it is worth considering that these instruments are - generally and currently - *app-based*, most of these data ends up in third-parties' hands[8] (*e.g.*, clouds).

Furthermore, the *social distancing measures* adopted in response to the spread of the COVID-19 pandemic, have further highlighted how *social relationships* are no longer predominantly based on direct contacts, but are maintained in an increasingly significant way through *On-line Social Networks* (OSNs): in ICT-mediated relations, the *surfer* has a different perception of reality, with the consequence that some of those limits (which can be considered as pillars to *individual* and *social respect*) are remarkably reduced. This new condition exposes each person to the threats of those growing and increasing *cybercrimes*, with direct and indirect effects on *fundamental rights* of human person, and then with significant impacts in the legislative and regulatory field[9], and implications under both criminal and civil law. As a matter of facts, «the Internet today represents, and increasingly will be given the trends and changes in the market and in the way of shopping, the main place where we meet to do business, sometimes lawful, but also unfortunately, illegal»[10].

The previous considerations both concern *adults* and *adolescents*: indeed, referring to the classification made by Prensky[11], there is no significant difference between the first ones (defined as "*digital immigrants*" *i.e.*, people who grew up before 1985[12]) who were introduced to ICT later in life, with the consequent "problem of adaptation",

7 L. FLORIDI, *op. cit.* p.3 ss.
8 R. COOPER, *Protecting our digital identity: the argument for adopting uniform privacy laws in the united states,* in *SSRN*, https://ssrn.com, 2020, p. 1 ss.
9 C. GRANDI, *Le conseguenze penalistiche delle condotte di cyberbullismo. Un'analisi* de jure condito, in *Annali online della Didattica e della Formazione Docente*, 2017, p. 40 ss.
10 S. SORIANI, *Informatica e Contratto*, in *Corso di Informatica Giuridica*, Simone ed., 2016, p.86 ss.
11 M. PRENSKY, *Digital Natives, Digital Immigrants*, in *On the Horizon*, n.9, 2001, p. 1 ss.
12 The 1985 is identified as the beginning of "*the digital age*".

and the second ones (the so called "*digital natives*"[13]), who have been raised alongside developing technologies, but without any parental guide.

Firstly, this classification points out a gap between two generations, then that each of them has a different awareness and sensitiveness of the digital context; furthermore, since there is a lack of reference points, for either categories emerge the need to *self-learning*, not only those aspects concerning the technical functioning of the devices but, primarily, to the *social* and *legal* effects on daily life. In practice, the problem is that in the current digital age there is a lack of a "*generation of digital parents*" who can provide the necessary indications of prudence and caution, both as users and in absolving the liability *in educando*, *lato sensu*.

Thus, it would be a great mistake to consider these phenomena only as part of the technological progress: the close link between *Legal Informatics*[14] and so-called *privacy* represents in a paradigmatic way the interference that new technologies have with new and emerging legal problems, considering that it concerns both behavioural, conceptual and organizational aspects[15].

Individual privacy is probably a major concern, although some other issues are evidently growing related to offence-commission, that in many cases is related to an under-evaluation of criminal conduct, several times perpetrated by minors. For instance, it is possible to refer, either to "*hate speech*" and to *social nature* offences (such as *Cyberbullying),* or *economical* ones (such as *forgery* and *identity theft*)[16].

Since the *Digital Dimension* is completely globalized, then a transnational approach to all the digital phenomena is required, as expressed in a communication of the

13 *i.e.*, people who were born prior to 1985.

14 According to A. CLERICI, *Introduction*, in M. BALLERINI - M. DE PRA - B. INDOVINA - G.L. PEDRAZZIONI, *Informatica giuridica*, Egea, 2019, p. XI ss.: «Legal Informatics is the discipline that concerns the application of information technology to law: it is therefore a subject strongly linked to the technical and practical issues of information technology tools. It is a separate, but complementary, subject with respect to IT law, or the branch of law that concerns the legal rules relating to the supply and use of IT products or services»; while A.C.A. MANGIAMELI, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, Giappicchelli, 2015, p.61, focused on «the issue of intangible computer assets and appropriability and transmission regimes, as well as the processing of personal data and the need to protect the freedom and dignity of the person».

15 A. ROSSETTI, *Legal Informatics*, Moretti Honegger, 2008, p.13 ss.

16 For completeness, it is worth reporting that the European Union (in the frame of the "*Convention on Cybercrime*", the first International Treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security, signed in Budapest on 23rd November 2001) identifies - among the criminal acts committed online by using electronic communications networks and information systems, classified in three broad definitions - even online fraud, forgery, identity theft, and several computer hacking acts.

European Commission with the affirmation «no crime is as borderless as cybercrime»[17]. The main purpose of this paper is to explore those legal aspects - in the international and Italian context - and risks concerning *identity crime*[18], directly related to both *social behaviours* and *illegal conducts*, in the light of the criminal law relevance (*e.g.*, whether these behaviours are "intentionally" or "unintentionally" done), and consequent liabilities.

2. The relationship between Privacy and Data Protection.

One of the major issues is the relationship between *individual privacy*[19] and the *protection of personal data*.

"*Privacy*" should be observed and analysed from two different perspectives representing the two different components: «"*Ontological privacy*" [which] consists of the physical and technological structures that allows to be alone. [And] "*regulatory privacy*" [which] consists of rules (not just legal) to be alone: the lack of physical structures in some companies to be alone does not imply either the absence of the

17 See EUROPEAN COMMISSION, *Communication from the Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre,* Brussels, 28th March 2012.

18 According to B.J. KOOPS - R. LEENES, *Identity Theft, Identity Fraud and/or Identity-related Crime*, in *Datenschutz und Datensicherheit*, n.9, 2009, p. 556 ss., even defined *identity-related crime*, *i.e.* that concerns all punishable activities and conducts that have *identity* as a target or a principal tool.

19 According to A. MOORE, *Defining Privacy*, in *Journal of Social Philosophy*, Vol. 39 No. 3, 2008, p. 412, it seems appropriate to report a brief summary indicates the variety and breadth of the definitions that have been offered in literature: «Privacy has been defined in many ways over the last few hundred years. Warren and Brandeis, following Judge Thomas Cooley, called it "the right to be let alone." Pound and Freund have defined privacy in terms of an extension personality or personhood. Legal scholar William Prosser separated privacy cases into four distinct but related torts. "Intrusion: Intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. Private facts: Publicizing highly offensive private information about someone which is not of legitimate concern to the public. False light: Publicizing a highly offensive and false impression of another. Appropriation: Using another's name or likeness for some advantage without the other's consent." Alan Westin and others have described privacy in terms of information control. Still others have insisted that privacy consists of a form of autonomy over personal matters. William Parent argued that "[p]rivacy is the condition of not having undocumented personal knowledge about one possessed by others," while Julie Inness defined privacy as "the state of possessing control over a realm of intimate decisions, which include decisions about intimate access, intimate information, and intimate actions." More recently, Judith Wagner DeCew has proposed that the "realm of the private to be whatever types of information and activities are not, according to a reasonable person in normal circumstances, the legitimate concern of others"».

idea of privacy, nor the absence of privacy regulations»[20]. Currently, in the *Information Society*, the *right to privacy* is mainly guaranteed by Data Protection laws and regulations[21].

Specific legislation has been promulgated over the years, and is in force in most Countries around the World: *e.g.*, Argentina approved in 2000 a *Data Protection Act* and in 2011 an Intelligence Act; Canada enacted the *Personal Information Protection and Electronics Document Act*, the federal privacy law for private-sector organizations, lastly amended on 23 June 2015; Australia enacted the *Privacy Act* in 1988. According to Rodrigues[22], in India, a constitutional *right to privacy* for persons exists through a judicial reading of it into Article 21 of the Constitution of India (right to life or personal liberty).

In the USA, there is no specific Act, but as written by Cooper[23] «the First Amendment is a proponent of privacy in one's beliefs, while the Third and Fourth Amendments champion privacy within one's home and one's person, respectively»", pointing out that «the Fourth Amendment undoubtedly serves as a proponent of digital privacy by preventing third party access to devices in certain situations. The Fourth Amendment states that a person has a right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures (U.S. CONST. amend. IV)».

The European Convention of Human Rights (ECHR) incorporates at Article 8 the *right to respect for private and family life*, defining this, within the European context, as the most significant *digital identity* impacting legal provision[24]. Recently a Privacy legal-framework has been approved: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the so called GDPR). This, priorly refers to Article 8(1) of the *Charter of Fundamental Rights* of the European Union, that guarantee the *right to the protection of personal data* concerning any natural person and, also, the «right of access to data which has been collected concerning him or her, and the right to have it rectified»; and then it gives precise indication on *data processing*, stating three main principles: (i) personal data protection is a fundamental right; (ii) these rules create a complex and functional mean to respect all the other rights and freedoms of the individual *human person*; then, (iii) this Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of

20 A. ROSSETTI, *op.* cit., 2008, p.17 ss.
21 See also A. ROSSETTI, *op.* cit., p.15 ss.
22 R.E. RODRIGUES, *Revisiting the legal regulation of digital identity in the light of global implementation and local difference,* The University of Edinburgh Research Archive, https://era.ed.ac.uk, 2011, p.139 ss.
23 R. COOPER, *op. cit.*, p. 1 ss.
24 R.E. RODRIGUES, *op. cit.,* p.139 ss.

an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

From another perspective, in order to complete this frame, it seems appropriate to highlight that, for example, these values are expressed both by article 3 of the Constitution of the Italian Republic[25], and also, by Pope Paul VI when affirming the importance of the «integral human development»[26].

One of the main provisions is that any *data processing* is lawful only if *data subject*[27] withdraw a an *expressed*, *freely given* and *specific* consent[28], priorly being informed of: (i) the purposes; (ii) the categories of recipients to whom data can be disclosed; (iii) times, modalities and techniques of the processing (including, *profiling*); (iv) and all the exercisable rights[29].

A particular attention is required where the *data subject* is a *minor* (*i.e.*, child) especially in relation to the offer of information society services: indeed, article 8 of Regulation (EU) 2016/679 states that the personal-data-processing is considered lawful only if the *informed consent* is given by an over 16 years old[30], otherwise, in case the child is below the quoted age, such consent is given or authorised by the holder of parental responsibility over the child.

Despite, on the other hand, there is a substantial complete autonomy of minors in surfing the Internet, which arise a fundamental issue concerning the foreseen *notice-and-consent* modality, the creation of *informative asymmetry* - as reported in a Study of

25 Italian Constitution, article 3 «Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese».

26 POPE PAUL VI, *Encyclical Populorum Progressio*, Vatican, 1967, 14: «The development We speak of here cannot be restricted to economic growth alone. To be authentic, it must be well rounded; it must foster the development of each man and of the whole man [...]».

27 Pursuant to article 2.1 of General Data Protection Regulation, it is defined as «an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person».

28 Pursuant to article 4(11) of Regulation (EU) 2016/679, the consent of the data subject is defined as «any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her».

29 Pursuant to (at least) articles 5, 12 and 13.

30 Although Member States may provide by law for a lower age.

the Council of Europe[31] and the "*formal compliance fulfilment*".

Often, the verification process of the age of the surfer is based on too simple solutions[32], becoming only in appearance compliant to current rules, since minors (not always totally, aware of the actions they put in place) are often technically more prepared than their parents, who in practice have a few controls on their digital life. «Those principles, which seek to balance the "fundamental but competing values" of "privacy and the free flow of information", form the basis of most privacy legislation around the world. At their core, they require that the processing of personal information be lawful, which in practice means that either the processing is explicitly permissible under law or the individual whose personal data is being processed has - after being informed of the reason, context, and purpose of the processing - given consent»[33].

Furthermore, on OSNs and in the Internet, a large amount of information and personal-data are available: some of them authorised by expressed will of the *data subject*, although other are given by other internet surfers, or by the online activities (so called metadata, mainly deriving from "*online-interactions*" among the users, such as tags, social networks friendship requests, likes, preferences, etc.). Unfortunately, it is commonly thought that since an information is *posted* (*i.e.*, publicly available), it is as well *useable*: but it is not true.

Indeed, pursuant to GDPR[34], personal-data-processing is lawful only for specific purposes: then, the only fact that a data is on-line available, does not justify its processing for different aims (the so-called, *purpose limitation*), especially when either it exposes the data subject to risks or a violation of a freedom and/or a right; or, moreover, when this use falls-in an illegal conduct.

In response to these issues, to avoid that *only formal compliant solutions* might expose to some risks the data-subject's rights and freedoms, the European Legislator introduced the principle of *accountability*[35] in the Regulation (EU) 2016/679, recalling

31 See COUNCIL OF EUROPE, *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications,* Strasbourg, 2018.

32 It is adequate to highlight that the Italian Data Protection Authority in December 2020 notified several infringements to a social network, due to the poor attention to the protection of minors, the easy dodging of the registration ban the company applies to children under 13 years, non-transparent and unclear information provided to users, and default settings falling short of privacy requirements.

33 F.H. CATE - V. MAYER-SCHÖNBERGER, *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, 2013, p. 67-68.

34 Articles 5, 6, 7 and 12.

35 Pursuant to article 5. (2) of Regulation (EU) 2016/679 «The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)», which is a dynamic, ongoing and permanent responsibility.

the application of the *culpa in eligendo* and *culpa in vigilando* principles, for the whole duration of data-processing.

If the issue concerning data-protection in *Digital Dimension* is already widely considered, it seems that too little attention has been put in citizens' awareness of effects on their "*real* dimension"[36], especially referring to those categories (minors, adolescents, and adult-digital-immigrants) who seem to be weaker, being exposed to several unperceived risks.

3. Digital Identity: the right "to be" in the digital dimension.

Firstly, it is proper to focus on the etymological definition of "*identity*" both to lists the philosophical and legal features, and to better clarify the perimeter of application.

«The English word "*identity*" originated from the Latin root *idem*, meaning "*the same*". It is defined as: a quality or condition of being the same, oneness, an instance of sameness, sameness of persons or entities in all circumstances, individuality, personality, personal or individual existence, or the "*self-same-thing*". By definition, *identity* can thus be understood in different contexts and has different qualities like sameness, equality, recurrence, individuality, distinctiveness or existence»"[37].

Identity is an element that belongs to any natural person (both minors and adults), including in this also his/her dignity and reputation; it is thus dependant and composite of many variables and factors, all related to the *expression of freedom*, and then has to be protected, like all the other *fundamental rights*.

In literature[38], it has already been highlighted how *Privacy* and *Identity* are closely related and often overlap: both of them are related to fundamental human rights, although they are separate and distinct concepts, and protect different interests in different ways. Indeed, the *right to identity* relates both to autonomy and of a person to be recognised as a unique individual.

On the other hand, *Digital Identity* is the one mediated or experienced through the involvement and use of computer technology or digital communications, like digital media or the Internet: it has to be noticed that the *Digital Identity* is a more dynamic component of the one in the *real dimension*[39].

36 M. CONTI - R. POOVENDRAN - M. SECCHIERO, *FakeBook: Detecting Fake Profiles in Online Social Networks*, in *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Istanbul, 2012, p.1071 ss.
37 R.E. RODRIGUES, *op. cit.*, p.139 ss.
38 C. SULLIVAN, *Digital Identity: An Emergent Legal Concept*, Adelaide, 2011, p. 7 ss.
39 See T. J. SMEDINGHOFF, *Digital Identity and Access Management: Technologies and Frameworks*, in O. POLLICINO - V. LUBELLO - M. BASSINI (a cura di), *Diritto e policy dei*

From another perspective, it is useful to link to its data-processing: the *identification*. Clarke[40] defines it as the association of information *with a particular human being*. In daily life, it usually refers to a *set of personal data* that allow to exercise individual rights, and it is publicly recognized and legally protected since it is registered in a *standard scheme*. According to Farina[41], there are many meanings that can be attributed to *personal identity*, among which, it is adequate to be quoted the oldest one related to the *physical* identification of people through personal data, which allow the identification of a subject within a social context.

According to World Economic Forum[42], the set of information is a collection of individual attributes, that can be classified as: *inherent*[43], that are intrinsic to a person, and are not defined by relationships to external entities; *accumulated*[44], that are gathered or developed over time, and these may change multiple times or evolve throughout an entity's lifespan; *assigned*[45], that are attached to the person, but are not related to his/her intrinsic nature. These attributes can change and generally are reflective of relationships that the entity holds with other bodies.

The "*privacy laws*" aim to ensure a safe data-processing in order to protect *Identity* as element of natural person and his/her fundamental rights. It derives the importance of an "*identity crime*" that is a violation of individual *autonomy to be recognized*, specifically where one misuses the *transaction identity information* of another person.

In the legal context, «a person's identity as recorded in the national identity register determines his or her ability to be recognised and to transact as a unique individual under the scheme. Where an individual's transaction identity information

nuovi media, Aracne, 2016, according to whom a concept of federated digital identity with generalized spending, understood as a correspondence between a specific natural person and his access credentials to a given computer system, so as to allow them to be recognized in the multiple identification systems of cyberspace as is the case with physical identity.

40 R. CLARKE, *Human identification in information systems: Management challenges and public policy issues*, in *Information Technology & People*, 1997, p. 6 ss.

41 M. FARINA, *Le tecnologie informatiche e l'effetto moltiplicatore sull'identità personale: riflessioni (meta)giuridiche tra crisi identità e necessità di tutela dei diritti fondamentali dell'individuo*, in *Rivista elettronica di Diritto, Economia, Management*, n.1, 2020, p. 41 ss., who in particular recalls the meaning of jurisprudential creation, frames it as «un bene-valore costituito dalla proiezione sociale della personalità dell'individuo, cui si correla un interesse del soggetto ad essere rappresentato, nella vita di relazione, con la sua vera identità, e non vedere travisato il proprio patrimonio intellettuale, ideologico, etico, religioso e professionale» referring to judgment of Corte di Cassazione n. 978 of 22nd June 1996.

42 World Economic Forum, *A Blueprint for Digital Identity*, Cologny, 2016.

43 age, height, date of birth, fingerprints, etc.

44 health records, preferences and behaviours, etc.

45 national identifier number, telephone number, e mail address, etc.

is misused by another person, the individual's ability to be recognised and to transact is fundamentally affected»[46].

With the Internet advent and the increasing development of the digital dimension in any fields of life, society and economy, these *references to an individual's identity* have been registered in e-database (instead of paper registers, like in the past), and even the *Identity Documents* changed in favour to the adoption of "electronic cards" or a "series of confidential credentials" (in place of paper documents) that allow to be used even in *e-relationships* (*e.g.*, e-commerce, G2C, B2C, etc.)[47]. Due to both this change and to technological progress, even the set of information increased in quantity and quality: in many cases, depending to national legislation, *biometric data*[48] have added to handwritten signature and facial photograph. Undoubtedly this enforced the *identification process* (*i.e.*, the verification of the identity, initially authenticated at the initial time of registration), meanwhile exposing to some threats, related to security in data processing[49].

Nevertheless, it is worth noting that one of the most relevant ways in which the law impacts on *digital identity* is through the establishment and regulation of national identity schemes, establishing a minimum set of attributes. Since only few Countries enacted them (*e.g.*, UK, with Identity Documents Act of 2010; and India, with Registration of Citizens and Issue of National Identity Cards Rules of 2003), the current result is a fragmented scenario[50]: thus, due to global exchanges and the need to allow an *interoperability* among different identity management systems, a supranational agreement on the adoption international standards is required[51].

46 C. SULLIVAN, *op. cit.*, p. 7 ss.
47 These statements are even more true, in the light of the *social-distancing* experiences required by the management of the COVID-19 pandemic: for example, the Italian Government in order to allow a certain business continuity, pushed on the use of Digital Identity (SPID) and e-signature, see Article 27 of the Decree-Law 16 July 2020, n. 76 converted into Law 11 September 2020 n. 120.
48 *E.g.*, Pursuant to article 4(14) of Regulation (EU) 2016/679, a biometric data is a «personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data».
49 As a matter of facts, many national Data Protection Authorities and legislators went to the direction of adopting the so called "*strong authentication*" methodologies, in order to protect the person fundamental rights, during any personal data processing, especially those more exposed to risks. *E.g.*, see The Italian Data Protection Authority Provisions: n. 258/2014; n.502/2017; n.429/2018; n.215/2019.
50 R.E. RODRIGUES, *op. cit.*, p.139 ss.
51 A.I. SEGOVIA DOMINGO - Á. M. ENRÍQUEZ, *Digital Identity: the current state of affairs*, in *BBVA Research Working Paper*, Madrid, 2018, p. 25 ss.

On the other hand, in the last decades, "*On-line Social Networks*" became the most used media for people to share information, and although the quality and quantity of information transferred and posted depends on the nature of the OSNs, varying significantly from each other, basically each of OSNs require the creation of an account, the so called "profile"[52], which can be assimilated to a *digital identity*. Indeed, thanking to *interoperability*, it is possible to join or access to any other OSNs or internet service, avoiding to create a new account, but using the "*favourite*" one. «Given the vast amount of personal information that is shared among friends in an OSNs, protecting the privacy of individual user has emerged as an important problem. In recent years, several privacy threats that exploit either personal data of a user or unintended vulnerabilities of OSNs have been reported»[53].

Besides, with the growth of the Internet has as well increased the use of *anonymity*[54] and *pseudonymity*[55] in cyberspace. As reported in literature[56], the causes are different: *on line anonymity* (in any forms, both totally or partial) allows people to maintain their privacy by using *screen identities*, and there is some reason to suppose that technology can contribute to the "*deindividuation*" of its users, contributing to express those hidden component (aggressiveness, hostility, disinhibition, etc.) of the behaviour of normal people.

Moreover, the wide use of *pseudonymity* also reveals an *unawareness* of the resulting implications, both from a strictly criminal point of view, and with the risk of acting on the verge of "abuse"[57], especially in minors.

4. Is a Fake Profile only a pseudonym?

52 It is worth noticing how this term recalls the meaning of "profiling" described (as "sensitive") at article 4(4) of GDPR: «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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements».

53 M. CONTI, et al., *op. cit.*, p.1071 ss.

54 that can be defined as *being* or *acting* without a name or with an unknown name.

55 *i.e.*, use of a "false" name, even to adopting a "*personae*" quite different from their *real world identities*.

56 M.E. KABAY, *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy*, in *Annual Conference of the European Institute for Computer Anti-virus Research* (EICAR), Munich, 1998, p.6 ss.

57 in most cases, this very common and widespread practice among internet surfers is not aimed at the commission of an illegal act, *i.e.* it is not possible to verify ex ante neither the will and / or premeditation.

Nowadays, it is very common that a person creates a *fake profile* with different goals: first and foremost, just to remain anonymous but, also in some other case, aiming to impersonate another *real person* in the *digital dimension*.

In this last circumstance, the reasons can be the most varied: from establishing online relationships with the friends of the "target" (*victim*), in order to get to know them or to spy them; acquiring more information and data about him/her, by interacting with his/her friends; or, finally, destroying the *victim's reputation*, adopting malicious behaviours.

Legal Informatics' literature classifies *fake profiles* depending whether they were based on *dynamic* or *static* behavioural data on social network. The first one refers to «a social network profile of a person who maintains a false identity in the internet to pretend as someone else. It is found out by Krombholz et al.[58] the fake user behaviour is different from the legitimate users. Therefore, the amount and the type of information that a fake user pass into their profile have a clear discrepancy from the legitimate user»[59]. The second one concerns a *profile clone* (thus, is an abusive clone account), where the offender, collecting personal data of the victim from OSNs or simply in the Internet - or even worse stealing or capturing (by using one of the *cyber-attacks* and/or some *Machine Learning* techniques, based on neural networks) - creates a new account, containing specular information. To complete this framework, it is adequate to report that literature highlights two variants of "*identity threat attacks on OSNs*": *single-OSNs* and *cross-sites-OSNs*. «In the first case, the victim already has a profile in the OSNs where the adversary will create the clone profile. In *cross-site OSNs*, the victim does not have a profile in the same OSNs where the attack is run, but the profile of the victim exists in other OSNs»[60].

The result is that the *Internet surfer* could turn into an *offender*, violating the freedom and rights of the victim. Indeed, the use of *fake profiles* concerns many different legal aspects to be exploited, thus it is worth analysing some specific issues. Since it is mainly based on using someone-else personal-data without his/her consent, this *behaviour* falls in - at least - in the sphere of a *misuse* in data-processing[61].

58 K. KROMBHOLZ - ET AL., *Fake identities in social media: A case study on the sustainability of the Facebook business model*, in *Journal of Service Science Research*, n. 4(2), 2012, p.175 ss.
59 S. ADIKARI - K. DUTTA, *Identifying fake profiles in Linkedin*, in *Proceeding of the 19th Pacific Asia Conference on Information Systems*, Chengdu, 2014, p. 279 ss.
60 M. CONTI et. al., *op. cit.*, p.1071 ss.
61 Indeed, it might not always be considered as an unlawful data processing (in absence of the subjective and objective features), in any cases this behaviour exposes to get close to be *borderline*.

On the other hand - as better detailed and clarified in the following - it can configure a proper *criminal conduct* or a *predicate offence*[62].

Therefore, for instance, it is appropriate to recall *forgery*, since this conduct can be characterized by two different methodologies: (i) creating a new false "*document*" or, (ii) altering an existing one[63].

For the purposes of this analysis, it is useful to premise that all world legislations consider any action that changes the truth contained by a document as the crime of forgery, although in order to give a legal definition, it is worth referring to *Forgery and Counterfeit Act 1981* of United Kingdom. Indeed, differently to other national legislations, UK deals with forgery in a way that was mostly different to some extent, introducing a wider concept: «as for the subject matter of forgery, a person is guilty if he makes a false instrument or alters in any of its aspect. […] This intention seems to have been thwarted by definition of instrument including "any document". A document may be an "instrument" within the meaning of FCA 1981 even if it is not an instrument in the narrow sense. This is clear not only from Section 8 (1) (a) but also from Section 8 (1) (d). A device on or in which information is recorded or stored is not necessary an instrument in the narrow sense»[64].

Thus, in this context, *forgery* should be considered either a "*stand-alone*" crime or a *predicate offence*, that lead to create a fake profile. Moreover, in most serious cases, a *fake profile* falls into the crime of *identity theft*.

5. Identity theft: a single offence or a multi-offensive crime?

Identity theft can be described as an illegal acquisition of a living or deceased person, which nowadays mainly applying the cyber-techniques of *impersonation*, that «involves a person pretending to have the identity of another genuine person, this might be through simply using a stolen document of someone that looks similar, but may also be combined with counterfeit or forged evidence (e.g. photo substitution on a person's genuine passport with the impostor's image)»[65].

62 For example, *Identity threat attacks on OSNs* belongs to the category of *social engineering cyber-attacks*, and it is common to those other illegal conducts, such as *impersonation* in Cyberbullying, and identity theft.
63 It concerns with *alteration* or *tampering* of a document and/or obtaining it by practicing deception, or from a person not in control of his senses.
64 Q.H. DAHASH, *The Concept of Forgery Crime Under United Kingdom Law*, in *Journal of Juridical and Political Science*, 6, 2017, p. 161 ss.
65 FATF, *Guidance on Digital Identity*, Paris, 2020, p. 40 ss.

Furthermore, as demonstrated by some investigations, it is appropriate to refer to *synthetic identities*[66] that have the purpose of not revealing (therefore, *hiding*) the real-identity of the offender.

«*Synthetic identities* are developed by criminals by combining real (usually, stolen) and fake information to create a new (synthetic) identity, which can be used to open fraudulent accounts and make fraudulent purchases. Unlike impersonation, the criminal is pretending to be someone who does not exist in the real world rather than impersonating an existing identity. For example, criminal groups can engage in identity theft, generating large numbers of synthetic digital IDs that are based in part on a real-individuals' identity attributes and other data that have been stolen from online transactions or by hacking Internet databases, and in part on entirely fake information. The synthetic IDs can be used to obtain credit cards or online loans and withdraw funds, with the account abandoned shortly thereafter»[67].

In doctrine and among the various authors the debate is still open, and there is no commonly accepted definition[68], also due to the different national legislations, for which it is often possible to make a distinction between *identity theft* and the crime of *identity fraud* (as any kind of deception to any database identity information, configuring a fraudulent behaviour)[69]. In order to better clarify and qualify the conduct, *e.g.* referring to Italian Criminal Code, it is proper to quote to article 640, identifying the following conduct «anyone, with artifices or deception, by inducing someone in error, procures for himself or others an unjust profit with others damage».

On the other hand, according to many legislations, *identity theft* is a criminal offence itself: *e.g.*, in the Italian Criminal Code it is contained at article 494. It should be noted that the Italian jurisprudence[70] has admitted that the crime could be

66 the creation of a "*new false virtual identity*", which is different compared to the impersonation, since it does not concern any "*real* third person".
67 FATF, *op.cit.*, p. 40 ss.
68 B.J. KOOPS, R. LEENES, *op. cit.*, p. 556 ss.
69 C. SULLIVAN, *op. cit.*, p. 7 ss.
70 *E.g.,* see Judgments of the Penal section of Italian Corte di Cassazione: n.46674/2007; n.18826/2013; n. 25774/2014. For an appropriate depth analysis see A. AMAOLO, *Della falsità personale: la sostituzione di persona ex art. 494 C.P.,* in *RatioIuris*, n.2, 2016; and also, M. PAPPONE, *In tema di sostituzione di persona sul web – Cass. Pen. 25774/2014*, in *Giurisprudenza Penale*, 2014 (online) who argued that technological evolution and, in particular, the era of web 2.0, require not only the Legislator to adapt the current regulatory framework, but also the jurisprudence to keep pace with the new protection requirements that follow. In this context, the offense of personal replacement on the web is placed (pursuant to art. 494 Italian Criminal Code), to be considered as a subsidiary criminal hypothesis, included in Chapter IV, Title VII, called "personal falseness", placed to protect the public faith. The jurisprudence of legitimacy has begun, in recent years, to deal with the hypothesis in question also committed via the internet,

committed through the Internet, such as creating a fake profile on OSNs and/or, damaging the reputation of the offended person (victim), *e.g.* recalling *Cyberbullying*. Moreover, it is appropriate to notice that it can configure - even - other crimes and also it can be a *predicate offence* aimed to do commit others.

Focusing only on some elements that characterize the conduct, and comparing them with each other, it is possible to highlight the *induction in error*[71], by illegitimately attributing himself a different *identity*, no matter whether it refers to another real person, or it is "imaginary". Moreover, another important aspect concerns the goal: either the conduct might procure an advantage (for the offender or for others) or, it might cause damage to a third party (victim).

Finally, it is possible to assume that *identity theft* is part of the larger issue of *identity fraud*, highlighting that the first one «is fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent»[72], while the second one «is fraud committed with identity as a target or principal tool»[73].

configuring the crime of substitution of a person in the conduct of the one who creates and uses an e-mail "account", falsely attributing the identity of a different subject, misleading the users of the internet against whom the false personal details have been declined and with the aim of causing damage to the subject whose personal details have been illegally spent (Criminal Court, Section V, 8 November - 14 December 2007, n. 46674). According to the Court, therefore, the crime of substitution of person occurs not only when one illegitimately substitutes one's own person for another person, but also when «si attribuisce ad altri un falso nome, un falso stato ovvero una qualità cui la legge attribuisce effetti giuridici, dovendosi intendere per "nome" non solo il nome di battesimo ma anche tutti i contrassegni d'identità», so including, among them, also the so-called *nicknames*. Therefore, it can be concluded that the object of criminal protection is the interest regarding public faith, as «questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali; siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome». On the other hand, as regards the subjective element, it is represented by the specific intent consisting in the purpose of procuring an advantage for oneself or others, or of causing damage to others. On this point, however, there is a certain unanimity of rulings, such as the one examined, in recognizing in the case of person replacement also the *non-pecuniary* advantage: among the advantages that can be deduced from the attribution of a different identity, in fact, there is both the possibility of having relationships with other people and the satisfaction of one's own vanity (non-patrimonial advantage).

71 independently whether is an individual citizen or it concerns with public faith.

72 B.J. KOOPS - R. LEENES, *op. cit.*, p. 556 ss.

73 B.J. KOOPS - R. LEENES, *op. cit.*, p. 556 ss.

Since *Identity Theft* compromise the so defined[74] individuals' *Personally Identifiable Information*[75] (PII), it could also be classified as an *unlawful data processing*, since it misses the required *informed consent*[76]. Confirming this, it is worth quoting a case sanctioned by the Italian Data Protection Authority in 2017[77], in which five Money-Transfer-Companies attributed hundreds of financial operations to more than a thousand completely unaware people, illegally using their data[78].

Last, but certainly not least, it should be highlighted how it is frequent that it is a predicate crime of fraud, indeed «*identity thieves* may use identifying information to open new credit card accounts, take out loans, or steal funds from existing checking, savings, or investment accounts. The consequent effects on the victim are significant and long lasting, since it can take years of hard work and hundreds or thousands of dollars in out-of-pocket expense to remove all vestiges of identity-theft from a victim's record, and in the interim, a victim may be unable to obtain a job, purchase a car, or qualify for a mortgage»[79].

6. Impersonation in Cyberbullying: a social crime in which the offenders and the victims are minors.

Cyberbullying is the natural evolution in the *digital* dimension of the one perpetrated in the *real* one, not replacing but alongside and integrating: in this conduct, a significant component is *impersonation*, hence the interest for the purposes of this analysis.

As a matter of facts, while *bullying* can be defined as any behaviour by an individual minor or group deliberately hurtful, repeated over time that can have a

74 Definition given by THE FINANCIAL ACTION TASK FORCE (FATF), the global money laundering and terrorist financing watchdog, which is an inter-governmental body that sets international standards that aim to prevent these illegal activities and the harm they cause to society.
75 That is, any information that by itself or in combination with other information can identify a specific individual; which is in coherence and compliance to the definition of *data subject,* pursuant to article 2.1 of GDPR.
76 Pursuant to at least articles 5, 12 and 13 of GDPR.
77 See Italian DATA PROTECTION AUTHORITY, provisions nn.39, 40, 41, 47, 48 of 2nd February 2017.
78 For completeness, the investigation carried out, revealed that the names to which the transfers were made, were never the real senders, and in some cases, the forms were "signed" by either *non-existent* or *deceased people*, then configuring the (alleged) crime of *identity theft*.
79 See R. GELLMAN, *Privacy Benefits and Costs From a U.S. Perspective*, in G. ROSI (a cura di), *Da costo a risorsa - La tutela dei dati personali nelle attività produttive*, Rome, 2004, p. 29 ss.

serious long-term impact on the person affected (victim), the phenomenon of *cyberbullying*, marks a particular mode of perpetration of some "*prevaricatory*" behaviours typical of bullying, whose projection in *cyberspace* increases dramatically the offensive potential[80].

In fact, as pointed out by some authors referring to *cyberstalking* (to which these considerations are common), the "*cyber*" component should be considered as an «an additional weapon in the artillery of the offender»[81], since in *infosphere* both anonymity and pseudonymity are currently the norm[82]. Willard[83] outlined some modalities to which *CyberBullying* can be put in place[84]: (i) *flaming*, as well known as online fights, which imply the use of electronic messages (instant-messaging, email, etc.) with hostile and vulgar language; (ii) *slandering*, is a modality that implies online disparagement, for example, sending cruel images or rumours about others to spoil their reputations or social relationships; (iii) *defamation*, is the spreading of secrets or embarrassing information about someone; (iv) *exclusion*, are several action which deliberately aim to exclude someone from an "online group"; (v) *cyber-harassment*, is the repeated sending of messages that include threats of injury or that are very intimidating. Last, but certainly not least, (vi) *impersonation* that is perpetuated by either an infiltration into victim's account, or creating fake profiles, in order to reduce (or destroy) the victim's reputation and relationships, through the sending of messages, and causing trouble for or endanger the victim.

In this context, it seems important to report a *sociological perspective* to better clarify the link between the offender's behaviour and the consequent legal liabilities: «Bullying already existed much earlier before the Internet and cell phones appeared. Young and adolescent students, and also more and more children, have used the new technologies to bully others, basically because these media provide them with this facility (or that is what they believe) to attack but remain anonymous (anonymity), which other cyberbullying aspects facilitate: not seeing the victim, nor his or her pain and suffering caused by bullying conduct. So, it is much easier for them to keep a

80 C. GRANDI, *op. cit.,* p. 40 ss.
81 L.P. SHERIDAN - T. GRANT, *Is cyberstalking different?*, in *Psychology, Crime & Law,* n.13, 2007, p.627 ss.
82 L. DE FAZIO - C. SGARBI, *New research perspectives about stalking: the phenomenon of cyberstalking*, in *Rassegna Italiana di Criminologia*, 2012, p.147.
83 N. WILLARD, *Educator's Guide to Cyberbullying and Cyberthreats*, http://cyberbully.org, 2005; N.WILLARD, *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*, Research Press, 2007.
84 E. CALVETE - I. ORUE - A. ESTÉVEZ - L. VILLARDÓN - P. PADILLA, *Cyberbullying in adolescents: Modalities and aggressors' profile*, in *Computers in Human Behavior* 26, 2010, p.1128 ss.

moral distance from their victims. This means feeling less regret and having fewer scruples when harming someone else»[85].

From a legal perspective, on the other hand, some elements[86] should be present to detect the criminal conduct: wilfulness, premeditation, repetition, absence of a legitimate purpose, persistence. *Cyberbullying* is a crime in many legislations and, for example, in Italy was introduced in two different steps: firstly, in direct consequence of the acquiring of awareness of the spread of the so called "*hate speech*" and of the *stalking* phenomenon[87], lead the legislator to introduce the Italian Criminal Code, article 612bis on *persecutory acts*; then, by Italian Law n.71 of May 29th 2017, approving as a sort of specific *framework criminal law on Cyberbullying*, in which at article 1(2) gives a broad definition[88], recalling several and different criminal conducts listed in the Italian Criminal Code[89].

For the purposes of this paper, it is appropriate to focus on the features of *impersonation in Cyberbullying*, the related criminal conducts; and, thus identifying three different stages: (i) *computer hacking* (perpetrated in many ways, belonging to several cybercrimes) as predicate offence to commit (ii) *identity theft*[90], and, (iii) *defamation*.

The relationship between the *digital behaviour* and the *criminal hypothesis* can be illustrated by shortly[91] listing some of the most common methods revealed both by literature and by investigations: *fake profiling* and *exclusion* in chat room and OSNs[92];

85 A. Ovejero - S. Yubero - E. Larrañaga - M. De La V. Moral, *Cyberbullying: Definitions and Facts from a Psychosocial Perspective*, in R. Navarro - S. Yubero - E. Larrañaga (a cura di), *Cyberbullying Across the Globe*, Cham, 2016, p. 2 ss.
86 B.H. Spitzberg - G. Hoobler, *Cyberstalking and the technologies of interpersonal terrorism*, *New Media & Society* 4, 2002, p. 67 ss.
87 L. De Fazio - C. Sgarbi, *op. cit.*, p.147 ss.
88 The definition of Cyberbullying given by Italian Law n.71/2017 is: «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o piu' componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».
89 Article 612-bis (persecutory acts); article 610 (private violence); article 581 and 582 (aggression); article 612 (psychic aggression through threat); article 660 (harassment); article 629 (extortion); article 595 (defamation); article 494 (impersonation).
90 Please, refer to the previous considerations, in particular to the given definitions of "*impersonation*" and "*synthetic identities*".
91 It has to be noticed that it is quite impossible (and as well useless) to list all of kinds of cyber-attacks techniques, since as any phenomenon is dynamic and in continuous daily evolution.
92 *e.g.*, such as Facebook, Twitter, Myspace, Instagram, etc.

spamming and *mail-bombing*[93]; *cybers-mearing* and *flaming*[94]; *password-cracking techniques* and *hacking accounts*[95].

Therefore, it is possible to create a link between these latter cyber-attack-techniques with the most relevant offences: since each national legislation is different, to the aims of this paper, it is adequate to yet refer to the Italian legal framework.

Whether the conduct is perpetrated through the violation of IT systems, *abusive access to an IT or telematic system* (article 615-ter of the Criminal Code) could be invoked; if said infringement occurs with the use of confidential credentials, it can be configured an *illegal possession and disclosure of access to IT or telematic systems* (pursuant to article 615-quater of the Criminal Code). While if the "*receptioning*" technique[96] is adopted, could also be configured *the violation, subtraction and suppression of correspondence/mail* (provided by article 616 of the Criminal Code).

Moreover, depending on the *IT techniques* adopted to commit the quoted offences (for example, in the case of "*synthetic identities*"), the Court could also evaluate the provisions of *Italian Personal Data Protection Code*[97] at article 167-bis (concerning the *unlawful communication and diffusion of personal data subject to large scale processing*) and at article 167-ter (*fraudulent acquisition of personal data subject to large scale processing*).

Since *impersonation* could be considered as a form of *identity theft*, it configures the crime provided by article 494 of the Criminal Code, as well as an *unlawful data processing* (article 167 of the *Italian Personal Data Protection Code*).

Last, but certainly not least, the Court in examining the available elements should consider whether *defamation*[98] has been committed, in the light of the offences listed in the definition of *Cyberbullying*. For what this latter offence concerns, for completeness it seems adequate to add some further considerations: according to a research

93 *e.g.*, through the sending of threatening messages, viruses, etc.
94 *e.g.*, posting defamatory materials on the Internet, etc.
95 These depend even on the capabilities of the offender; from a technical perspective it can be achieved with different kind of attacks, such as dictionary, brute force, rainbow table, phishing, social engineering, malware, offline cracking, shoulder surfing, spidering, guess, Wi-Fi sniffing, etc.
96 *i.e.* illegal receipt of electronic messages and/or access to the victim's email box, which nowadays, it evolved in its complexity and width, and it has been absorbed in the definition of "*man in the middle*" one. For an appropriate depth study about this new cyber-technique see S. EBERZ – M. STROHMEIER – M. WILHELM – I. MARTINOVIC, *A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols*, in S. FORESTI - M. YUNG - F. MARTINELLI (a cura di), *ESORICS 2012*, Springer, 2012, p. 235 ss.
97 ex Legislative Decree 30th June 2003, n.196.
98 Thus, identifying it as aimed at offending the *reputation* of a third person. In Italy indeed, *defamation* is contained in article 595 of the Criminal Code, defined as «injuring the reputation of an absent person via communication with others».

commissioned by the OSCE[99], three-quarters of the participating States maintain general criminal defamation laws. While in several common law countries (*e.g.*, the UK, Ireland, Cyprus) criminal defamation laws had largely fallen into disuse, and in the United States has no criminal defamation laws at the federal level, but such laws continue to exist at the state level. In many Countries, the current debate regards the proposals to contemplate strengthening of elements of defamation laws in an effort to combat online "*hate speech*", *cyberbullying* and related phenomena.

Nevertheless, a final consideration about it, is required: especially nowadays, in the *age of the internet*, due to the wide possibilities to spread information around the globe and to *publicly storage* information and data online for years, the damage to *reputation* is strictly linked and related to the *right to privacy*, and the respect of individual natural person's fundamental rights and freedoms[100].

In response to this issue, the European Legislator introduced the "*right to be forgotten*", *i.e.* obtaining the erasure of personal data concerning him/her, without any undue delay[101].

---

99 S. GRIFFEN - B. TRIONFI, *Defamation and Insult Laws in the OSCE Region: A Comparative Study*, OSCE Paris, 2017, p7 ss.

100 A. SPAIC - C. NOLASCO - M. NOVOVIC, *Decriminalization of defamation - The Balkans case a temporary remedy or a long term solution?*, in *International Journal of Law, Crime and Justice* 47, 2016, p. 21 ss.

101 GDPR, Article *17, "Right to erasure*" provides the right to obtain the cancellation of personal data, without delay, provided that specific conditions are met, such as: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). For an appropriate depth study about this right, see M. ZANICHELLI, *Il diritto all'oblio tra privacy e identità digitale*, in *Informatica e diritto*, XLII annata, Vol. XXV, 2016, n. 1, pp. 9-28; and also G.M. RICCIO – A. PEDUTO – F. IRACI GAMBAZZA – L. BRIGUGLIO – E. SARTINI – C. OCCHIPINTI – I. GUTIÉRREZ – D. NATALE, *The PoSeID-on Blockchainbased platform meets the "right to be forgotten"*, in *MediaLaws*, n. 2, 2020, p. 194 ss. In particular, it is adequate to highlight that «before GDPR, the main European jurisdictions developed an interpretation and application of the right to be forgotten, that has confirmed the existence of this right, although through an interpretative process shaped on a case-by-case analysis» (p. 197), and observing and analyzing the sentences and the jurisprudence, it emerges that there has been an interpretative evolution in its application: « this right has changed from its debut in the legal discourse. In fact, at the beginning of its application by the national courts, it was considered to belong exclusively to public figures and not to private citizens. In fact, only public figures were interested by the mass-media analysis, while private persons were outside this process

7. Conclusions.

In the *Information Society* the definition of "*identity*" evolved, due the wider use of the Internet and its devices, on the one hand, led to its *digitization*; on the other, the significant use of *analytics*, proportionally it has increased the possibility of creating specific *profiles* for each user[102], effectively generating specific identities in relation to a single context[103].

Even the legal perimeter is different, being enforced the relationship between individual freedoms the fundamental rights and the way to use ICT devices: in fact, nowadays, the *right to privacy* goes in parallel with the *personal data processing protection regulation*.

It is evident that ICT facilitates interrelationships, but decreasing the perception of direct contact (in the absence of *physical proximity*), and increases the risk of unwanted forms of contact (in which *anonymity* is a fundamental element to the abuse) and of several forms of *identity crime* commission.

Since *Identity* is a useful vehicle to express *individual personality* and a means to keep social relationships, a great importance to *Digital-Awareness*[104] and *Cyber-Hygiene*[105] is required.

In light of the seriousness of these abuses of "*identification*" in *cyberspace*, a solution has to be addressed, considering the real causes and reasons: «at the heart of much of the debate over the advisability and possibility of imposing limits on behaviour in cyberspace is the question of identity. Some of the most egregious abuse of cyberspace seems reasonably to be attributable in part to the ease of concealing identity; using no name or false names, malefactors can often escape almost all of the consequences of their actions»[106].

---

and were only spectators of this news. The spreading of Internet and the facilitation of collecting and indexing information has determined that also private persons may be covered by this right. In fact, these persons may be "googled" as well and their personal information may be easily found through a search on the major search engines [...] the right incorporated in Art. 17 is not absolute, but can be exercised only in specific situations, which are listed in the first paragraph of the article itself». (p. 200 ss).

102 *E.g.*, for marketing and CRM activities.

103 Cfr. also S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 1997, p. 583 ss.

104 increasing an internal immunity to exogenous *cyber issues*, even though a change in people behaviour and cultural aspects.

105 Mitigations to the causes of many cybersecurity "*incidents*", *lato sensu.*

106 M.E. KABAY, *op. cit.*, p.6 ss.

Meanwhile, *digital citizens* should be educated to use these devices and tools in an ethical and lawful way, with an increasingly *awareness* and *prudent manner*, being adequately informed of those arising inevitable risks. Only through a process of cultural growth can a person take all necessary precautions to protect him/herself from any form of violation (potentially, becoming either an *offender*, or a *victim*).

It is important that each person perceives the same sense of responsibility in acting, both in the *real* dimension and in the *digital* one, otherwise the negative effects of the use of new technologies would fall directly on *fundamental rights and freedoms*.

In this sense, it is appropriate to recall the words of Pope Benedict XVI: «Human freedom is authentic only when it responds to the fascination of technology with decisions that are the fruit of moral responsibility. Hence the pressing need for formation in an ethically responsible use of technology. Moving beyond the fascination that technology exerts, we must reappropriate the true meaning of freedom, which is not an intoxication with total autonomy, but a response to the call of being, beginning with our own personal being»[107].

Finally, on a legal perspective, it seems appropriate to agree that «the research on these criminal hypotheses, which are constantly growing today, must therefore be further deepened, in order not only to assess the prevalence and the multiple qualifying aspects, but also to enhance the coping and protection tools of the victims, with a view to personal protection and control and conscious management of the means of communication available»[108].

Bibliography and Sources

AA.VV., *Identità ed eredità digitali*, Aracne, 2016

ADIKARI S. - DUTTA K., *Identifying fake profiles in Linkedin*, in *Proceeding of the 19th Pacific Asia Conference on Information Systems*, Chengdu, 2014

AMAOLO A., *Della falsità personale: la sostituzione di persona ex art. 494 C.P.,* in *RatioIuris*, n.2, 2016

BASSINI M., *Internet e libertà di espressione*, Aracne, 2019

CALVETE E. - ORUE I.- ESTÉVEZ A.- VILLARDÓN L.- PADILLA P., *Cyberbullying in adolescents: Modalities and aggressors' profile*, in *Computers in Human Behavior*, 2010

CATE F.H.- MAYER-SCHÖNBERGER V., *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, 2013

CLARKE R., *Human identification in information systems: Management challenges and public policy issues*, in *Information Technology & People*, 1997

107 POPE BENEDICT XVI, *Encyclical Letter Caritas in Veritate,* Vatican, 29th June 2009, n.70.

108 L. DE FAZIO - C. SGARBI, *op. cit.*, p.147 ss.

CLERICI A., *Introduction*, in BALLERINI M. - DE PRA M.- INDOVINA B. – PEDRAZZIONI G.L., *Informatica giuridica*, Egea, 2019
CONTI M.- POOVENDRAN R.- SECCHIERO M., *FakeBook: Detecting Fake Profiles in On-line Social Networks*, in *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Istanbul, 2012
COOPER R., *Protecting our digital identity: the argument for adopting uniform privacy laws in the united states,* in *SSRN*, https://ssrn.com, 2020
COUNCIL OF EUROPE, *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications,* Strasbourg, 2018.
D'AGOSTINO PANEBIANCO M., *Vivere nella dimensione Digitale*, Themis ed., 2019
DAHASH Q.H., *The Concept of Forgery Crime Under United Kingdom Law*, in *Journal of Juridical and Political Science*, 6, 2017
DE FAZIO L. - SGARBI C., *New research perspectives about stalking: the phenomenon of cyberstalking*, in *Rassegna Italiana di Criminologia*, 2012
EBERZ S. – STROHMEIER M.– WILHELM M.– MARTINOVIC I., *A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols*, in FORESTI S. - YUNG M. - MARTINELLI F. (a cura di), *ESORICS 2012*, Springer, 2012
EUROPEAN COMMISSION, *Communication from the Commission to the Council and the European Parliament, Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre,* Brussels, 28th March 2012.
FARINA M., *Le tecnologie informatiche e l'effetto moltiplicatore sull'identità personale: riflessioni (meta)giuridiche tra crisi identità e necessità di tutela dei diritti fondamentali dell'individuo*, in *Rivista elettronica di Diritto, Economia, Management*, n.1, 2020
FATF, *Guidance on Digital Identity*, Paris, 2020
FLORIDI L., *Foundations of Information Ethics*, in HIMMA K.E., TAVANI H.T. (a cura di), *The handbook of information and computer ethics*, Wiley, 2008
GELLMAN R., *Privacy Benefits and Costs From a U.S. Perspective*, in ROSI G. (a cura di), *Da costo a risorsa - La tutela dei dati personali nelle attività produttive*, Rome, 2004
GRANDI C., *Le conseguenze penalistiche delle condotte di cyberbullismo. Un'analisi de jure* condito, in *Annali online della Didattica e della Formazione Docente*, 2017
GRIFFEN S. - TRIONFI B., *Defamation and Insult Laws in the OSCE Region: A Comparative Study*, OSCE Paris, 2017
KABAY M.E., *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy*, in *Annual Conference of the European Institute for Computer Anti-virus Research* (EICAR), Munich, 1998
KOOPS B.J.- LEENES R., *Identity Theft, Identity Fraud and/or Identity-related Crime*, in *Datenschutz und Datensicherheit*, n.9, 2009
KROMBHOLZ K. - ET AL., *Fake identities in social media: A case study on the sustainability of the Facebook business model*, in *Journal of Service Science Research*, n. 4(2), 2012
MANGIAMELI A.C.A., *Informatica giuridica. Appunti e materiali ad uso di lezioni*, Giappicchelli, 2015
MOORE A., *Defining Privacy*, in *Journal of Social Philosophy*, Vol. 39 No. 3, 2008
OVEJERO A. - YUBERO S.- LARRAÑAGA E.- DE LA V. MORAL M., *Cyberbullying: Definitions and Facts from a Psychosocial Perspective*, in NAVARRO R.- YUBERO S.- LARRAÑAGA E. (a cura di), *Cyberbullying Across the Globe*, Cham, 2016

PAPPONE M., *In tema di sostituzione di persona sul web – Cass. Pen. 25774/2014*, in *Giurisprudenza Penale*, 2014
POLLICINO O. - ROMEO G. - *The Internet and Constitutional Law*, Routledge, 2016
POPE BENEDICT XVI, *Encyclical Letter Caritas in Veritate,* Vatican, 29th June 2009
POPE PAUL VI, *Encyclical Populorum Progressio*, Vatican, 1967
PRENSKY M., *Digital Natives, Digital Immigrants*, in *On the Horizon*, n.9, MCB University Press 2001
RICCIO G.M. - PEDUTO A. - IRACI GAMBAZZA F. - BRIGUGLIO L. - SARTINI E. - OCCHIPINTI C. - GUTIÉRREZ I. - NATALE D., *The PoSeID-on Blockchainbased platform meets the "right to be forgotten"*, in *MediaLaws*, n. 2, 2020
RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 1997
RODRIGUES R.E., *Revisiting the legal regulation of digital identity in the light of global implementation and local difference,* The University of Edinburgh Research Archive, https://era.ed.ac.uk, 2011
ROSSETTI A., *Legal Informatics*, Moretti Honegger, 2008
RUOTOLO G.M., *International law: profili di diritto internazionale pubblico della rete*, Cacucci, 2012
SEGOVIA DOMINGO A.I. - ENRÍQUEZ Á. M., *Digital Identity: the current state of affairs*, in *BBVA Research Working Paper*, Madrid, 2018
SHERIDAN L.P. - GRANT T., *Is cyberstalking different?*, in *Psychology, Crime & Law*, n.13, 2007
SMEDINGHOFF T. J., *Digital Identity and Access Management: Technologies and Frameworks*, in POLLICINO O. - LUBELLO V.- BASSINI M. (a cura di), *Diritto e policy dei nuovi media*, Aracne, 2016
SORIANI S., *Informatica e Contratto*, in *Corso di Informatica Giuridica*, Simone ed., 2016
SPAIC A. - NOLASCO C. - NOVOVIC M., *Decriminalization of defamation - The Balkans case a temporary remedy or a long term solution?*, in *International Journal of Law, Crime and Justice*, n.47, 2016
SPITZBERG B.H. - HOOBLER G., *Cyberstalking and the technologies of interpersonal terrorism*, *New Media & Society* 4, 2002
SULLIVAN C., *Digital Identity: An Emergent Legal Concept*, University of Adelaide Press, 2011
WILLARD N., *Educator's Guide to Cyberbullying and Cyberthreats*, http://cyberbully.org, 2005
WILLARD N., *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*, Research Press, 2007
WORLD ECONOMIC FORUM, *A Blueprint for Digital Identity*, Cologny, 2016
ZANICHELLI M., *Il diritto all'oblio tra privacy e identità digitale*, in *Informatica e diritto*, XLII annata, Vol. XXV, 2016