VII. DIGITALISATION AND HUMAN RIGHTS

CONSTRUCTION AND DECONSTRUCTION OF THE IMAGE IN THE DIGITAL WORLD: PROTECTION OF PERSONAL IDENTITY AND DEEPFAKE

Annagrazia Tomasi
PhD candidate
University of Salento

1. The right to one's image and the right to personal identity within the Italian and European legal order.

In the Italian legal system, the right to one's image is established in article ten of the Civil Code in its 'pathological connotation' (in fact, it is entitled "Abuse of another's image"). As a preliminary point, some necessary considerations: the Italian Civil Code is from nineteen forty-two and precedes the Republican Constitution, which was issued six years later, in nineteen forty-eight. The nineteen forty-two Civil Code gives centrality to enterprise and productivity: for these mostly historical and social reasons, the current Civil Code, accords importance to pecuniary aspects and their respective rights. Beyond this, the Code's provisions must be interpreted in light of the principles of the Constitution, which is the supreme and primary legal source.
Law, as the preeminent social science, must place the person at the center of its focus. The contemporary interpretation of the Civil Code moves in this direction, thanks to the Constitution which, among many other things, subordinates productivity to the respect for fundamental human rights. Consider, for instance, what article forty-one of the Constitution states about the private economic initiative. It establishes that the private economic initiative is free but it may not be carried out in contrast with social utility or in what causes harm to health, the environment, safety, liberty, or human dignity.
The right to one's image and the right to identity are linked into the category of fundamental personality rights with a constitutional basis as they represent distinct facets of the individual[1]. Personality rights are non-pecuniary situations, even though it is well-known that the right to image is recognized to generate economic relationships. However, these are situations indissolubly linked to the person and exercisable only by that person.
Considering these preliminary points, the right to image is primarily protected by article ten of the Italian Civil Code; this provision defines the right not in positive, but in negative, by focusing on its violation or abuse: it stipulates that if an image is exposed or published outside the cases permitted by law, or with prejudice to the person's decorum or reputation, the judicial authority, upon request of the interested party, may order the cessation of the abuse, without prejudice to the right to claim damages. In any case, the prevailing view is that the right to one's image must be subsumed within the broader category of personality rights, and this evolution reflects the conviction that the right to image constitutes one of the possible manifestations of individual personality.

[1] For a survey of personality rights, *ex multis*, cf. Rescigno, 1991; De Cupis, 1982; Zeno-Zencovich, 1995. In the Italian legal landscape, the absence of explicit statutory provisions, generated considerable difficulties in conceptualizing personality rights. Doctrine itself became divided between proponents of a monistic theory and those adhering to a pluralistic approach. At present, the prevailing theory is the monistic one, a position also affirmed in longstanding case law, as in Cass., 10 May 2001, no. 6507: "Within the sphere of personality rights, founded upon the Constitution, the right to one's image, to one's name, to honor, reputation, and privacy represent but individual aspects of the constitutional significance that the person, in his or her unity, has acquired within the constitutional system". For a more detailed account of the historical development, Mignone, 2014, in particular, regarding the 'right to be oneself' and to the centrality of the deliberative moment for the identity-related choice, p. 80

From the exegesis of art. 10 of the Italian Civil Code, which prohibits the publication of another person's image without consent (unless justified by law, such as in the case of public figures at public events)[2], it emerges that the publication of another's image is unlawful not only when it occurs without the person's consent or outside the circumstances expressly contemplated by law as capable of excluding protection of the right to privacy (chief among them the notoriety of the subject portrayed), but also when, even in the presence of such consent or circumstances, the exhibition or publication nonetheless causes prejudice to honor, reputation, or decorum.

The right to one's image, in addition to constitutional protection (by virtue of art. 2 of the Italian Constitution) and codified regulation, is also safeguarded by Law no. 633 of 22 April 1941 (the so-called Copyright Act), which prohibits (subject to exceptions) the reproduction or commercial exploitation of a person's likeness without his or her consent. To these provisions must be added those of the so-called Privacy Code, which, by protecting any element evocative of personal identity, extends its protective scope to the reproduction and dissemination of an individual's image.

In conclusion, legal scholarship underscores that the right to one's image is intrinsically connected to personal autonomy and dignity, highlighting the importance of safeguarding the image as an expression of personality and of everyone's private sphere.

According to art. 14 GDPR, for a case of de-referencing of allegedly inaccurate content, the Court of Justice (Grand Chamber) ruled that a person's image constitutes one of the chief attributes of his or her personality as it reveals the person's unique characteristics and distinguishes the person from others and that the right to the protection of one's image is thus one of the essential components of personal development and mainly presupposes that person's control over the use of that image, including the right to refuse publication of it[3]. In fact, an individual's image is one of the principal attributes of their personality, as it reflects their originality, enables them to be distinguished from others, and conveys personal, and at times even intimate, information. The right of a person to the protection of their image constitutes one of the conditions for their personal development and entails, in particular, the power to exercise control over their own image and, consequently, the ability to prevent its dissemination. Moreover, the Court affirmed: "it should be noted that the publication of photographs as a non-verbal means of communication is likely to have a stronger impact on internet users than text publications. Photographs are, as such, an important means of attracting internet users' attention and may encourage an interest in accessing the articles they illustrate"[4] and underscores that images, as a form of non-verbal communication, are undeniably more capable of attracting the attention of Internet users than textual publications and they are often open to a wide variety of interpretations.

With regard to the right to personal identity (likewise to be classified among the rights of personality) its scope may be properly understood only if distinguished from the right to identification, which requires certain clarifications concerning the right to a name. This right is specifically regulated and accordingly protected under artt. 6–9 of the Italian Civil Code, where the exclusivity of the use of one's own name and pseudonym is safeguarded. Conversely, the improper use of another's name is prohibited, as it may cause prejudice to the person concerned and give rise to a claim for damages[5].

---

[2] Stanzione, 2009, p. 599, affirms that he individual's consent thus legitimizes the dissemination of his or her image (by any means, including television or cinematographic media) and such consent (that according to general principles, may be either express or implied) while on the one hand it renders dissemination lawful, on the other it circumscribes its scope by defining and specifying the modes and contexts of its circulation.

[3] Court of the European Union, Grand Chamber (2022) Judgment of 8 December 2022, Case C-460/20.

[4] *Ibidem.*

[5] This in addition to the two legal actions available for the protection of one's name, the so-called action of complaint, defined as a typical action for condemnation grounded in the contestation of and unlawful use of another's name, and the so-called action of usurpation, linked to the exclusivity of the use of one's own name, defined as an action aimed at obtaining the prohibition of its use by others and subject to the concurrence of two requirements, namely the unlawful use by third parties and the harm, even if only potential, resulting or capable of resulting therefrom.

The name assumes an emblematic value for the identification of the person, at the very least because it represents the most immediate and synthetic means of recognition[6].
However, what is the 'identification' of the individual must be distinguished from his or her 'personal identity', which encompasses the protection of several aspects of personality (such as name, honor, reputation, image, privacy, etc.).
From a legal perspective, personal identity has thus been reconstructed[7] as the right not to have one's individual personality misrepresented and, above all, as the interest, generally considered worthy of legal protection, that each person be represented, in social relations, in accordance with his or her true identity, as this is recognized in the relevant social reality, whether general or particular. Specifically, it was the 'Veronesi case', as decided by the Supreme Court of Cassation in 1985, that brought the notion of personal identity into the legal stage as a "synthetic formula to distinguish the subject globally in the multiplicity of their specific characteristics and manifestations". The ruling defined the judgment stemming from the fact that some phrases spoken by the oncologist in an interview were later reused by a cigarette manufacturer in an 'advertorial' context to promote their products. During the first judgment, the infringed legal position had been identified as the right to a name, *ex* art. 7 of the Civil Code. However, the Court of Cassation, in overturning the lower courts' approach, developed an articulated definition of the right to personal identity in its reasoning, along with a thorough evaluation of its normative foundation and its relationships with other personality rights. Following this famous pronouncement, the configurability and systematization of personal identity as a relevant subjective legal position for the legal system has no longer been in question.
It may therefore be concluded that in the Italian law, 'image' is generally understood as the visual representation of a person's likeness that is, the graphic reproduction of their features. In this sense, the Italian Supreme Court last year[8] said that the image of a person must be protected in itself as a highly distinctive element that makes the individual unique, original, and as such recognizable. On the other hand, we have personal identity that includes the protection of various aspects of personality, such as one's name, honor, reputation, image, privacy, etc. Consequently, on a legal level, the framework for personal identity is the right not to see one's individual personality misrepresented in general or specific social reality.
The delicate subject of personal image and identity, and their violation or abuse, becomes even more complex and demands greater protection in the digital world.

2. The digital revolution and its impact on the individual as user.

Between technology and law, there has always been a particularly close relationship[9]. The "digital revolution" has made it necessary to afford broader and more pervasive protection of an

[6] For this undeniable function of social identification, its foundation is to be found at times in a public interest, at times in a private one.
[7] Raffiotta, Baroni, 2022, p. 166. Already Prosser, 1960, in the attempt to construct a systematic account of the right to privacy, said that the right to respect for the person is infringed even where false facts are attributed to the individual, thereby producing a distortion of his or her personality. The author identifies four principal categories (Prosser's Privacy Torts) of conduct that may be regarded as infringing upon privacy: intrusion upon the plaintiff's seclusion or solitude, or into his private affairs (the intrusion upon seclusion), publicity (the public disclosure of private facts) which places the plaintiff in a false light in the public eye (the false light); appropriation, for the defendant's advantage, of the plaintiff's name or likeness (the appropriation of name or likeness).
[8] Cass., 21 August 2024, no. 23018.
[9] Among others, cf. Pascuzzi, 2020. The A. addresses the entirety of technological innovations and the evolution that has affected the law in light of new technologies. With regard to the impact of the new digital services of the information society on modes of communication, connection, consumption, and economic activity, particular attention is given to Regulation (EU) 2022/2065 of 19 October 2022 on the single market for digital services (the so-called Digital Services Act), as well as to the need to resolve the contradictory ambivalence of the online environment, originally conceived as a "free" space resistant to regulation and characterized by the absence of intermediation, yet

individual's image. Such protection must, indeed, be guaranteed online, since the non-consensual dissemination of images (whether authentic or artificial) on the internet constitutes a serious violation of the right to one's image.
Currently, the most prevalent virtual places for social interaction are digital platforms. Their profound innovative impact lies in the pervasive tendency towards their sharing. With the advent of social networks, communicative practices have undergone such a transformation that initially emerged as a simple means of interaction among users has evolved into a widely used form of virtual environment. The keystone of social networks is the profile, that for us, for the legal speech, is the digital identity. Profiles are generally created through standardized procedures requiring the provision of personal data such as name, age, photograph, etc.; the accuracy and veracity of the information inserted into these profiles often cannot be verified.
As I said before, the construction of one's profile directly concerns the dimension of identity: users create representations of themselves by combining different kinds of personal information. Through their profile, individuals articulate and construct their social identity, or rather, their multiple identities. If personal identity in the digital era acquires new features and evolves into digital identity, then, as has already been affirmed[10], digital identity may be understood as the personality of a subject as projected online and the ways in which it is expressed, as the results of an online search concerning an individual and the data thereby disclosed, the self-image that is created and shared on the internet, and the presentation of a person within the 'online environment'. So, when an individual's identity is transferred into the digital sphere, all the data, information, and characteristics that make that individual unique are likewise transposed. The possibility of creating and subsequently utilizing fictitious identities, and the possibility of appropriating another's identity, reveals how dynamics already well known are amplified and occur with greater frequency in the online space.
The risks associated with privacy and with the impairment or distortion of one's digital identity give rise to a wide range of consequences, from moral and reputational harm to pecuniary damage. Furthermore, numerous studies have highlighted that patterns of information-sharing on social networks do not always reflect an awareness of the extent to which such data may be disseminated: this phenomenon has been described as the 'privacy paradox', that is, the disjunction between what users claim to know about the privacy settings of their accounts and their reactions when confronted with unforeseen consequences arising from privacy violations[11].

3. The de-construction of one's image in the digital world.

From the foregoing considerations, it emerges that an individual's image, once it enters the digital sphere, is constructed upon the deconstruction of the real image.
When we move on to online, digital, personal protection, the legal approach is the European one. This approach, particularly concerning the right to privacy and personal data, and the regulation of AI adopts a user-centric model.
In sum, we have two different situations: if, in fact, the technologies of the digital age have made it possible to construct another reality, that is a virtual space characterized, for example, by social networks 'populated' by users, offering great new opportunities and advantages (including, e.g., the possibility of creating one's own avatar in the Metaverse)[12], on the other hand, it often happens

simultaneously in pressing need of guarantees of security and the protection of fundamental rights, cf. Grisi, Tommasi (eds.), 2024.
[10] Pesci, 2023, p. 124.
[11] Barnes, 2006. An interesting survey conducted among users registered on some of the most widely used social networks worldwide has shown that the main problem does not lie in the lack of available privacy settings, but in its settings. In fact, a significant number of users are not even aware of the existence of privacy control mechanisms on social networking platforms; Acquisti, Gross, 2007, pp. 35-37.
[12] The most accredited definition is that propounded by Matthew Ball, who defines the metaverse in the following terms: "The Metaverse is a massively scaled and interoperable network of real-time rendered 3D virtual worlds and

that a person's image enters the web without their consent or happens that an image, having ended up online of one's own volition, is then used by third parties in a distorted way.
Already in the 2015, with the Declaration of Internet Rights, was affirmed that "the Internet has decisively contributed to redefining the public and private spheres, to structuring relationships among individuals and between individuals and institutions. It has erased boundaries and created new forms of producing and utilizing knowledge". This recognition already made clear that identity acquires new characteristics in the digital era, and for this reason, when the right to privacy (that constitutes a fundamental right of the person under art. 8 of the Charter of Fundamental Rights of the European Union, and that its principal framework of protection is today provided by Regulation (EU) no. 679 of 27 April 2016) comes into consideration is thus to be understood as extending well beyond the traditional right to secrecy, thereby emphasizing the importance of constructing and safeguarding digital identity.
The words of a renowned Italian jurist appear timelier than ever. In fact, in 2009, Stefano Rodotà said that we are in the era in which we had to admit that we are what Google says we are; and when he said "within that vast catalogue of the world and in the countless other databases that relentlessly preserve personal information, our identity is constructed in forms that increasingly escape the control of the very individual concerned"[13], the risks inherent in this new construction (namely the digital one) of one's image become clearly apparent, and the consequence is the loss of control over the identity itself.

4. Generative Artificial Intelligence and the distortive effects of deepfakes.

Now there is an increasing use of the 'high-risk technology', which is the generative Artificial Intelligence[14]. In particular, the Regulation (EU) no. 2024/1689 (the AI Act) is the first-ever comprehensive legal framework on AI worldwide. This Act addresses the risks of AI and puts Europe in a position of leadership with the aim of fostering trustworthy AI in Europe.
The AI Act defines four levels of risk for AI systems: unacceptable risk, high risk, limited risk, and minimal risk. Use cases of AI that may entail serious risks to health, safety, or fundamental rights (as in the present case) are classified as high-risk. Consequently, such systems must be subject to strict obligations before they can be placed on the market.
While it is true that Regulation (EU) of the last year, no. 2024/1689, laying down harmonized rules on artificial intelligence, imposes specific and additional safeguards (the European regulation requires transparency obligations for providers and deployers of these AI systems), also due to the fact that these generative Artificial Intelligences are able to generate text, images, and other content, but at the same time the development and training of such models require access to vast amounts of text, images, videos and other data that may be protected by copyright and other related rights: the threat is that loopholes and exclusions of liability may be created behind the veil of the development and training of these AI systems, supposedly in the name of common progress.
Accordingly, owing to the potential of Artificial Intelligence, digital technologies assume the role of "facilitating agents of manipulative practices"[15], systematically exploiting cognitive and affective vulnerabilities of individuals *by design*[16]. One of the most emblematic instances of this phenomenon

environments which can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments", cf. Ball, 2022.
[13] Rodotà, 2009.
[14] On the subject of generative artificial intelligence, among others, Maras, Alexandrou, 2018; Alpa (ed.), 2020; Perlingieri, Giova, Prisco, 2020; Santosuosso, 2020; Uricchio, Riccio, Ruffolo, 2020; Sartor, 2022; Camardi (ed.), 2023; Melchiorre, Monaca (eds.), 2023; Sturino, 2023; Azzali, Ellecosta, 2023; Finocchiaro, 2024; Flora, Maggi, 2024; Pignataro, 2024.
[15] Panattoni, 2024, p. 525
[16] On high-risk AI systems and the requirements established in Regulation (EU) 2024/1689, Viterbo, 2024, pp. 188–199; it is Mignone, 2024 who speaks of a 'manipulated', indeed even 'non-existent', consent.

is arguably the case of Cambridge Analytica, in which, as is widely known, large-scale manipulative strategies were implemented while simultaneously being 'tailored' to the specific profiles of individual users, with the objective of influencing voting preferences in the United States elections. Artificial Intelligence, when applied within the online environment, may thus constitute an effective instrument for the realization of such practices, not solely through the profiling of users but also, for example, through the direct generation of 'artificial' content. It is at this juncture that the phenomenon of deepfakes emerges.

Given that the term 'deepfake' in itself is not necessarily negative[17], but in common and media use 'deepfake' has acquired predominantly negative connotations, being associated with deceptive manipulations, disinformation, distortive effects, falsification of reality, and infringements of personal image and identity.

In the 2021 report (Trackling deepfakes in European policy) published by the European Parliament, deepfakes are defined as manipulated or synthetic audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done, produced using artificial intelligence techniques, including machine learning and deep learning. This view is here shared.

To provide a more complete picture, and to underscore the risks inherent in the phenomenon, it is worth the criminal law perspective, which shows that numerous offences may be committed through the use of deepfakes. Alongside offences against individual personality, one must also recall property and economically motivated offences, which encompass various forms of counterfeiting of voice, images, or video, with the aim of misappropriating corporate information or personal data, or of inducing the victim of a deepfake attack to perform certain acts, primarily acts of disposition of property, as well as deepnude and deepfake pornography, and even identity theft. At present, the existing legislative framework does not afford sufficient protection in criminal law terms, given the rapid mutability of the phenomenon under consideration. Beyond this observation, which illustrates both the complexity and the significance of the issue, attention must be drawn to the nexus between the phenomenon of deepfakes and identity theft. Indeed, the creation of any deepfake product necessarily involves the artificial deprivation of an individual of his or her identity (in the sense previously described).

That's how came out the pathological phenomenon of deepfake: the starting material consists of real faces, real bodies, and real voices of people, transformed, however, into 'digital fakes', thereby infringing the right to personal identity. Another central issue in relation to possible countermeasures against disinformation, including that disseminated through deepfakes, is the principle of transparency. Indeed, the third paragraph of art. 52 of the proposed Artificial Intelligence Regulation sets forth an obligation of transparency, insofar as it requires the creator of a deepfake to disclose that the content is not authentic; the critical point concern with this requirement lies in its practical enforceability[18]. And now the problem is highly topical because deepfake technologies, initially very expensive and not widespread, are now extremely prevalent, as they are accessible to everyone using a common smartphone. The Italian Data Protection Authority states that deepfakes constitute a particularly serious form of identity theft, and that individuals appearing in a deepfake without their knowledge not only suffer a loss of control over their image but are also deprived of control over their ideas and thoughts, which can be distorted based, e.g., on a generated video.

[17] In fact, e.g., the technologies offer opportunities to cinematographic artists, educators, advertisers and technology companies to create more engaging and personalized digital experiences; in the medical field, there are therapeutic applications in development, and the technology may even give a voice to the mute; there are also many innocent applications, such as beauty filters in camera apps, and other entertaining applications for live video footage.

[18] Cazzaniga, 2023, p. 185.

5. The right of every person to be represented in a truthful and non-distorted manner. Remedies within the legal framework.

The distorted phenomenon of deepfakes, which profoundly and by its very nature undermines the right of every individual to be represented in a truthful and non-distorted manner, demonstrates how the law is often unable to regulate before society is transformed by the digital revolution.
Deepfake technology is a fast-moving target and even if it is impossible to predict precisely which way the technology will develop in the years to come, as legal scholars, however, it is necessary to acknowledge this reality (this 'visual manipulation') and to seek 'appropriate remedies'[19].
Therefore, what are the 'appropriate remedies' in open contrast to the rampant deepfake phenomenon?
Certainly, traditional remedies hold validity in the digital world. *In primis* the reparation for harm concerning personality rights is deemed compensable, specifically when three conditions are met: the constitutional relevance of the harmed interest, the gravity of the offense which must exceed the tolerability, and the seriousness of the prejudice.
But current remedies are still far from adequately protecting individuals. Surely, there is the remedy to prohibit the continuation of certain conduct, but is it effective? We often face platforms that respond to requests for help with bots and almost never protect the individual, rendering extra-judicial remedies largely ineffective. While judicial recourse can stop harmful conduct and claim damages, but it's impossible to fully restore the original, *ex ante* situation.
The recommendations given by the Italian Data Protection Authority, i.e. to avoid sharing personal images on social media and learn to recognize a deepfake, cannot be effective: now, for example, Google's Veo 3 now is able to generate videos so precise that is very hard to recognize that they are fake and on the first point it's impossible for citizens not uploading personal images on social media because they already done it for years without knowledge of the risks. Furthermore, we cannot ignore the fact that social platforms are also primary sources of information. Thus, beyond the harm to the individual directly impacted by a deepfake, there's a broader public interest at stake.
While, last June, has appeared a tightening of rules on social platforms regarding consent for using personal content to train AI, in an opt-out mechanism: this demonstrates how high risks continue to intensify, while the available remedies remain inadequate and underdeveloped.
Following a thorough analysis of this issue, several final 'recommendations' can be made as follows: first, cooperation between States and platforms should be intensified, transparency should be considered the key element in the regulation of online disinformation, while the criteria for the removal of manipulated content must be consistently defined to avoid the risk of over-removal, and finally, legislative measures and platform-imposed restrictions should be complemented by initiatives promoting education[20].
Without prejudice to the fact that the analysis of subjective legal positions must necessarily be undertaken, as emphasized by authoritative scholarship[21], in the light of the legal order as a whole, in my opinion, maybe, the only effective remedy is not primarily private enforcement but public enforcement. This last one is manifested in the following terms: by imposing stricter penalties on platforms that fail to control these pathological phenomena and improving AI regulation, by regulating and sanctioning more the big platforms and the generative apps, source of deepfake, that produce not only injury to the right of image and identity, but also serious risks to the entire society.

[19] Perlingieri, 2011, p. 4
[20] In this sense, Waldemarsson, 2020, pp. 21-22.
[21] Perlingieri, 1972, p. 12

References

Acquisti, A., Gross, R., 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook', in Golle P., Danezis G. (eds.) (2007), *Workshop on Privacy Enhancing Technologies*, Springer;

Alpa, G. (ed.) (2020) *Diritto e intelligenza artificiale*, Pisa: Pacini Editore;

Azzali, V., Ellecosta, N. (2023) 'La questione deepfake in Italia: una panoramica', *MediaLaws,* 2023/3;

Ball, M. (2022) 'The Metaverse: And How It Will Revolutionize Everything', New York: Liveright Publishing Corporation;

Barnes, S. B. (2006) 'A privacy paradox: Social networking in the United States', *First Monday*, 11 (9);

Camardi, C. (ed.) (2023) *La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche – Ca' Foscari Venezia, 25-26 novembre 2021*, Milano: Wolters Kluwer;

Cazzaniga, M. (2023) 'Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai deepfakes', *MediaLaws*, 2023/1;

De Cupis, A. (1982) 'I diritti della personalità', *Trattato Cicu e Messineo*, IV;

Finocchiaro, G. (2024) *Diritto dell'intelligenza artificiale*, Bologna: Zanichelli;

Flora, M., Maggi, L. (2024) *Intelligenza artificiale generativa opportunità e sfide legali*, Pisa: Pacini Giuridica;

Grisi, G., Tommasi, S. (eds.) (2024) *Mercato digitale e tutela dei consumatori. Prove di futuro*, Torino: G. Giappichelli Editore;

Maras, M.H., Alexandrou, A. (2018) 'Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos', *The Internet Journal of Evidence & Proof*, 23;

Melchiorre, D.M., Monaca A. (2023) (eds.), *Innovations and Economic and Social Changes due to Artificial Intelligence: The State of the Art*, Springer;

Mignone, C. (2014) *Identità della persona e potere di disposizione*, Napoli: Edizioni Scientifiche Italiane;

Mignone, C. (2024), '«Giornata perfetta». La patrimonializzazione dei dati personali tra inconvenienti della retorica ed esigenze della pratica', Persona e Mercato, 2024/1;

Panattoni, B. (2024) 'Condizionamenti e manipolazioni nell'era digitale. Il divieto europeo di pratiche di Intelligenza Artificiale "manipolative" ', *Diritto Penale e Processo*, 2024/4;

Pascuzzi, G. (2020) *Il diritto dell'era digitale*, 5. edn., Bologna: Il Mulino;

Perlingieri, P. (1972) *La personalità umana nell'ordinamento giuridico*, Napoli: Edizioni Scientifiche Italiane;

Perlingieri, P. (2011) 'Il giusto rimedio nel diritto civile', *Giusto processo civile*;

Perlingieri, P., Giova, S., Prisco, I. (eds.) (2020) *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli: Edizioni Scientifiche Italiane;

Pesci, G. (2023) 'L'identità nella società dell'informazione', in *Ciberspazio e diritto*, 2023/2;

Pignataro, G. (2024) *Etica, buona fede e governo dell'intelligenza artificiale generativa*, Napoli: Edizioni Scientifiche Italiane;

Prosser, W.L. (1960) 'Privacy', *California Law Review*, 48;

Raffiotta, E.C., Baroni, M. (2022) 'Intelligenza artificiale, strumenti di identificazione e tutela dell'identità', *BioLaw Journal – Rivista di BioDiritto*, 2022/1;

Rescigno, P. (1991) 'Personalità (diritti della)', *Enciclopedia giuridica*, XXIV;

Rodotà, S. (2009) 'L'identità al tempo di Google', *laRepubblica*, 14 december 2009;

Santosuosso, A. (2020) *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Milano: Mondadori Università;

Sartor, G. (2022) *L'intelligenza artificiale e il diritto*, Torino: Giappichelli;

Stanzione, P. (2009) 'Sub art. 10 c.c.', *Commentario al codice civile*';

Sturino, F.S. (2023) *Deepfake technology and individual rights, Social Theory and Practice,* 49, no. 1 (January 2023);

Uricchio, A.F., Riccio G., Ruffolo, U. (eds.) (2020) *Intelligenza artificiale tra etica e diritti*, Bari: Cacucci editore;

Viterbo, F.G. (2024) Intuitus personae *e negozi "su misura"*, Napoli: Edizioni Scientifiche Italiane;

Waldemarsson, C. (2020) 'Disinformation, deepfakes and democracy. The european response to election interference in the digital age', Alliance of Democracies;

Zeno-Zencovich, V. (1995) 'Personalità (diritti della)', *Digesto civile*, XIII.