Towards Symbiotic Autonomous Systems

Title:

LEGAL ASPECTS RELATED TO DIGITAL TWIN

Marina TELLER
Professor of Law, University Côte d'Azur, France

Abstract

The creation of digital replicas of individuals, based on their data, gives birth to the digital twin. This new "digital self" raises many legal difficulties. This article presents the main issues from a legal point of view. Most of the structuring concepts of the law are questioned by these special symbiotic systems: the concept of person, identity, entitlement to rights and obligations, legal capacity, liability, data processing, etc. All these notions, which are rooted in the legal tradition, are correlated to the human person and must therefore be profoundly adapted to apply to the digital twin. It is a new experience: the law must devise concepts to take account of an entity that is halfway between people and things. We see this as an opportunity to rethink the legal framework and to consider the advent of future digital human rights. This questioning aims to make the law evolve towards a better consideration of symbiotic systems.

Keywords : digital twin; legal framework; digital human rights; digital identity

This work has been supported by the French government, through the 3IA Côte d'Azur Investments in the Future project managed by the National Research Agency (ANR) with the reference number ANR-1-9-P3IA-0002

The digital twin raises some very tricky questions from a legal perspective. The legal system is based on assumptions and concepts, such as the person, identity, will, property, free will... All these concepts that structure the legal matrix are questioned by the digital twin. Indeed, the digital twin is based on two principles: imitation and technology. On this aspect, we find the visionary writings of Marshall McLuhan, some of whose formulas have become postulates that seem surprisingly adapted to the issue of the digital twin: "We shape our tools and thereafter they shape us". This fear of being shaped and controlled by tools, rather than autonomously wielding them, lies at the heart of current concerns with machine learning and artificial intelligence systems[1] and also digital twin. So, what is this digital twin? An other me? A better me? A future me? The digital twin updates the Shakespearean question in the digital world: to be or not to be... A second question is then added: to be or to have? Indeed, the digital twin refers as much to the idea of person as to the idea of possession: this twin is as much a replication of the person as it is a "putting into data of the person" with a patrimonial dimension. The twin *is* the person but the person *has* his twin.

The digital twin takes us from the age of trans-humanism to the age of "exo-humanism". This is finally an eminently legal question which allows us to rethink the question of identity, of the person and the boundary between what I possess and what I am, that is to say between being and having. It is a difficult subject that must be analysed from the angle of "surveillance capitalism"[2]: the patrimonialisation of the self is made possible by data sensors, connected objects and AI systems. However, this data-based surveillance leads to behavioural modification devices. The purpose of monitoring our online behaviours through the collection of browsing data is to "manufacture" new behaviours - to "like" this content, click on this advertisement displayed according to our preferences, buy this merchandise or subscribe to this service. According to Shoshana Zuboff, these behavioural changes mean that individuals are stripped of their autonomy and freedom to become mere agents whose actions are shaped remotely. This is another challenge for the law: how to maintain people's fundamental rights? How to keep democracy in balance and avoid a dilution of the individual in the "total capitalism" of the digital economy[3]?

The digital twin raises complex legal questions; they must first be answered because the development of the digital twin will depend on the answers provided by legal experts (Part 1). Conversely, digital twin also questions the law, which must do its "examination of conscience". Perhaps it is time to update or reconsider certain rights or legal concepts, in order to provide an answer adapted to the specific nature of digital twin and to preserve the rule of law (Part 2).

Part 1) The law questions the digital twin

Today, there are many use cases of digital twin, in the industrial, real estate or health fields. The market for digital twins is estimated[4] at 15.6 billion dollars in 2023, with an average annual growth of almost 38%. Digital twins make it possible to model reality and predict its evolution: the prospects for the health market are enormous and are shaping the future of medicine of the future. The digital twin makes it possible to understand the reproduced entity, to predict its evolution, to anticipate its potential flaws, to test its reactions with virtual simulations... This use of digital twins is in line with the desire to develop "4P medicine", for personalised, predictive, preventive and participatory.

However, the innovative potential of digital twin should not overshadow the importance of the legal framework. Indeed, the development of digital twin involves removing certain legal obstacles and clarifying the applicable law. Digital twin is based on contextualised data which are thus transformed into information. At the heart of digital twin are therefore data, algorithms and AI systems. The legal framework of these concepts is therefore the key to the development of digital twin. Thus, from a legal point of view, digital twin raises questions regarding data, medical liability, algorithmic integrity and intellectual property. This list is far from being exhaustive.

The digital twin and the data

Up to now, there is no legal corpus dedicated to digital twin. However, the provisions applicable to data do apply, in particular the General Data Protection Regulation (GDPR)[5]. Digital twin does not present any particular specificity in this field and as soon as personal data is processed, the obligations provided for by the GDPR apply: Article 5 (Chapter 2) sets out a general framework which lays down several obligations (obligation of transparency, obligation of loyalty, obligation to store the data within a reasonable time, obligation to keep the data up to date, etc.). Articles 6 and 7 provide for the basic requirement of the consent of the data subject to the processing of data but also, as a consequence, the possibility of withdrawing such consent at any time. This consent is essential because, as Article 9 recalls, the processing of health data is, in principle, prohibited unless the patient consents. Article 17 of the GDPR also provides for a right of oblivion and the individual will be able to lodge complaints or legal remedies if he or she considers that his or her rights have been violated (in accordance with Chapter 8).

The difficulty here is how to articulate the rights of a person with respect to his or her data with those of another person related to him or her (for example, in medical matters, a spouse with a chronic contagious disease: can the digital twin capture this information relating to a third person but which has an impact on the human twin?) In addition, other rules can be added to the GDPR, particularly in medical matters: if digital twin is considered a "medical device", the legal framework may be even stricter. For example, in France, the legal regime for the hosting of health data obliges web hosts to obtain certification.

The digital twin and medical liability

The scope of liability is under great pressure from the players in the digital world. Connected objects, robots, autonomous devices are upsetting the classic rules of civil and criminal liability. It is necessary to adapt a legal framework that has been thought up to now for people with will and independence because liability is generally the counterpart of a right or a duty. Up to now, it has been assumed that machines were not able to act by themselves, but they have bridged the gap and become autonomous in the new virtual world. Must we change our models and allow machines to embody us in a sustainable way and in a legal framework ruling virtual communities?[6] Is the profile the person? Can the real person be held responsible for damage caused by his or her digital twin? The reflection is old and can feed into already developed examinations about the liability of robots. Who is responsible: the programmer, the manufacturer, the owner of the robot or the machine? But the digital twin still raises some very specific questions. The cyber-connected patient becomes an actor in his own health, or even an expert in his pathologies, to the point where he sometimes questions the diagnosis and therapeutic solutions proposed by the doctor[7]. The challenge will be to maintain the sacred relationship between the doctor and the patient: the European Parliament reminded us, as early as 2017, that human contact is one of the fundamental aspects of personal care[8]. The French legislator is proposing to establish in law a principle of "human guarantee", in order to guarantee human supervision of any use of digital technology in health care. Another question arises: how can the doctor's decision-making autonomy be strengthened? Who will be the real decision-maker: the digital twin or the doctor? To avoid the doctor becoming a mere executor of the machine's prescriptions, it is important to sanctify the doctor's decision-making role. This presupposes upstream work on the "explicability" of AI systems so that algorithms, in medical matters, are not black boxes for doctors at least.

The digital twin and algorithmic integrity

The quality of the data will guarantee the quality of the digital twin's virtual image, reflecting the real person. Or, data integrity is a major and challenging issue. The A.I. community has recently begun working on methods to detect and mitigate bias in the training data sets of supervised automatic learning systems. Indeed, it has been demonstrated that the computerised and automated processing of big data raises risks of bias[9] and discrimination of all kinds (racial, gender, professional, etc.). The quality of the data is therefore an essential subject: it must be fair, "inclusive", i.e. representative of various trends, and reliable over time. It is therefore a question of moving from big data “to smart data”. The concepts of ‘transparency’ and ‘explainability’ are presented as tools to achieve this goal. Such approaches, however, involve significant limitations, especially in professional contexts such as medicine, law, or financial advice. Instead, systems should be designed to be contestable, meaning that those subject to algorithmic decisions can engage with and challenge them[10]. Both laws and norms should encourage contestability of automated decisions,

but systems designers still must take explicit steps to promote effective questioning and challenges.

The digital twin and ownership issues

From a general property perspective, the digital twin poses a difficulty: how to share rights between the real person behind the data and the creators of the digital twin? Theoretically, it is possible that, tomorrow, these data will be commercialised and there are currently no specific regulations on how they should be exchanged. It is therefore important to know who is the owner of the data and whether there is a right of control over the knowledge that will then be extracted from it. It is therefore a twofold question, that of the ownership of the data and then that of the appropriation of the results. If a digital twin is extracted from our uses, must we be informed? The same question applies to the sharing of a digital twin.

Conflicts of rights can even be considered: for example, after a divorce, can a former spouse request to have access to delete data related to him or her? As we produce more and more data as part of our digital lives, the question now arises as to what happens to this data after we die. Is it possible for a relative or heir to take over the digital identity of the deceased? Can we inherit from a digital twin? In the absence of any specific rule, we can draw inspiration from the law set up by social network platforms, which allows heirs to request the deletion of the deceased's accounts. With regard to the PDT, this right must be provided for from the outset, when the contract is formed.

The development of these digital twins also raises questions from an industrial property point of view. Indeed, can a digital twin be patented? As a reminder, the algorithm embedded in a program is not, as such, protected by copyright, in the same way as the ideas underlying the creation. The application of intellectual property rights becomes possible again, provided that the algorithm is incorporated in an invention which is itself patentable[11]. The legal framework is quite complex and distinguishes between databases, software, reverse engineering and work-data. More precisely, one could imagine the case of a discovery resulting from the modelling of a digital twin. One could then imagine legally protecting this invention, provided that the conditions for patentability are met: the invention must be new and it must be susceptible of industrial applications.

Part 2) The digital twin questions the law

The digital twin puts the legal categories in tension. Thus, it is a fantastic opportunity to refresh legal concepts and challenge our thinking habits in several ways.

The digital twin questions our relationship to reality and to the person.

The most important action of a sovereign state is to grant citizenship and establish civil statuses. However, digital technologies have blurred borders and increased anonymity. What becomes of a person in a digital world? The person is reconstituted as a collection of digital traces, scattered data points collected as they navigate various networks. The individual becomes nothing more than a profile, defined externally. New statistical information collected using data mining, and new statistical capabilities, such as profiling, are unprecedented threats to individual freedoms[12] and also opportunities to build our digital twin.

The digital twin causes a "derealisation" of human experiences. The digitisation and pixelisation of the person disrupts our traditional conception of the person, which is no longer defined by his or her civil status but by the correlation of his or her data. So where does the virtual begin and where does the person stop? Between the two, a kind of digital unconsciousness appears halfway between the person and the thing.

The digital twin involves thinking about the notion of **digital identity**[13] and blurs the boundary between people and things. Perhaps the digital twin corresponds to this notion of "centre of interest" proposed by Gérard Farjat, which is halfway between people and things, in a grey area of the law[14]. Neither quite a person nor quite a thing, the digital twin recognised as a "centre of interests" could then benefit from certain rights and obligations attributed to both.

The digital twin questions free will, consent and willpower

The creation of the digital twin changes our relationship to lived experience: the digital twin makes it possible to replace real experimentation and self-experimentation with simulation and statistical prediction. Prevention has become the absolute priority, with global monitoring. Specifically, chance and uncertainty, which are a normal part of everyday life, have been replaced with ex ante systems that automate the relationships between individuals.

The digital twin also reflects a society marked by aversion to risk and chance: the place of chance is regressing, which is not without consequences for the expectations of individuals. The digital twin is an achievement as much as a promise. However, it may be important to maintain the place of chance in algorithmic processing, as Alexei

Grindbaum proposes[15]. Indeed, it is not a question of knowing how to make artificial intelligence benevolent. It is a question of ensuring that it does not replace man as a moral agent : by integrating chance into the algorithmic code, we reintroduce the random when a moral choice arises. Only recourse to chance, and this from its conception, by design, can free the machine from the responsibility that one wants to make it bear. For example, to translate a neutral pronoun into a gendered form, the random translation into "she" or "him" avoids giving priority to one or the other.

The digital twin raises the question of the advent of the fundamental rights of the digital person

The fundamental question is whether the time has not come to enshrine the fundamental rights of the digital person. These rights would make it possible to take account of the radical change resulting from the digitalisation of the world.

The question is not whether deep tech presents opportunities, nor is it a matter of understanding its true nature or establishing whether these technologies should be regulated by adding such and such a rule to such and such a code. We also need not ask if we need more ethical considerations to make up for algorithmic biases. We believe that the danger lies elsewhere, because we are seeing technological systems take the place of legal systems, because they are fulfilling the same roles, but faster and even more effectively. The question today is whether the law, in its role as a social regulator, will be replaced by digital structures. It is from this viewpoint that we will try to think differently about the law by creating meta-rights to protect the rule of law and its legal norms[16].

One might say that existing legal systems already have mechanisms in place to control how algorithms are used, and more generally, to supervise operators who use automated processing techniques for personal data. The General Data Protection Regulation mechanism is an effective frame of reference for regulating data in a context that opposes data transmitters and data processors[17]. This is an important contribution, but we believe that the heart of the matter lies elsewhere and goes well beyond the individual relationship between the data transmitter and the data user. Basically, the GDPR focuses on the person, guaranteeing the protection of personal freedoms. This framework helps to implement mechanisms that depend on people’s will to exercise these freedoms, involving consent, the right to be forgotten, data access, and portability. The way these data are processed raises further questions about protecting the public interest, beyond singular examples, due to the way data processing shapes society. It is not merely enough to consent to the automatic processing of your personal data, we need to ensure that the massive collection of data does not become a new tool for social conditioning, influencing the way person votes or behaves. That is the difficult part. The GDPR affirms liberties that suppose people will want to keep track of how their data is used. It is only logical. But what about the unconscious effects, that is to say, all those situations where the perception of an individual is shaped by massive data, processed on an industrial scale, whose ultimate

effects they can hardly be aware of? Are our democracies robust enough to face this problem, when we are already living in the era of big data[18]?
Finally, and above all, the power of algorithms is displacing people's control of their own behavior (internet consumption habits, web browsing, owning your browser history, etc.). Legal mechanisms that focus on the individual will have trouble referring acts when they have been separated from the person. That is why thinking in terms of personal freedoms may not be enough, and why we need to find another way to think about this legal framework.

We believe that the implications of deep tech such as the digital twin require that we stretch our legal imagination if we are to rise to this challenge. First, we will need to bring concepts from deep tech into the legal world and test how they fit into the legal framework (i.e. What is their legal meaning? What effects do they have? What obligations do they give rise to?). The same goes for the notions of robustness, calculability, provability, consensus, correlation, interoperability, etc.

Next, we will need to review the letter of the law as it currently stands. Some are calling for the establishment of new fundamental rights, called "meta-rights"[19] : the right to be forgotten[20], the right to disobey, or the right to be informed. The ability to forget and be forgotten, to disobey, or to be informed about the reasons for our actions are all seen today as essential for a solid legal system; in other words, a legal system that is effective when faced with algorithmic governmentality and the new norms that it creates. One author suggests that the laws of robotics should be rewritten for the age of big data, mixing public and private law and creating "algorithmic accountability" obligations, inspired by auditing rules and the recognition of externalities[21]. Others have proposed a bill of rights for social media platform users[22], or the creation of a responsibility-by-design mechanism to introduce responsibility natively, at the heart of deep tech systems[23].

Marina TELLER

References

1. Kluttz D, Kohli N, & Mulligan D. Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions. In K. Werbach (Ed.), *After the Digital Tornado: Networks, Algorithms, Humanity*. Cambridge: Cambridge University Press. 2020;137-152.
2. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs. 2019
3. Srnicek, N., *Capitalisme de plateforme : L'hégémonie de l'économie numérique*, Lux Canada. 2018
4. Digital Twin Market by Technology, Type (Product, Process, and System), Application (predictive maintenance, and others), Industry (Aerospace & Defense, Automotive & Transportation, Healthcare, and others), and Geography - Global Forecast to 2026
5. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
6. Bourcier D, *De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique ?,* Droit et Société. 2001; 847-871
7. Conseil d'État, *Révision de la loi de bioéthique : quelles solutions pour demain* ?. juin 2018 page 205
8. *Résolution du Parlement européen contenant des recommandations à la commission concernant des règles de droit civil sur la robotique*. 16/2/2017 ; n°32
9. Crawford K, «The hidden biases in big data », *Harvard Business Review*. 2013
10. http://blogs.hbr .org/2013/04/the-hidden-biases-in-big-data
11. Kluttz D, Kohli N, & Mulligan D, Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions. In K. Werbach (Ed.), *After the Digital Tornado: Networks, Algorithms, Humanity*. Cambridge University Press. 2020; 137-152
12. DIRECTIVE 2009/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2009 on the legal protection of computer programs
13. See: Rouvroy A, "La 'digitalisation de la vie même': enjeux épistémologiques et politiques de la mémoire digitale", *in* Un enjeu de société, *Documentaliste-Sciences de l'Information*, 2010, Vol. 47, p. 34. Greater use of remote monitoring and behavior prediction technologies is closing the gap between the inspectors and the inspected. In place of the easily identifiable individual inspections that took place in traditional companies, we are seeing new kinds of public or private oversight and surveillance that are largely invisible, fundamentally preventative, and therefore difficult to fight on an individual level.
14. Sullivan, C. "Digital Identity – A New Legal Concept". In *Digital Identity: An Emergent Legal Concept*. The University of Adelaide Press. 2011 ; p.19-40 doi:10.1017/UPO9780980723007.004
15. See : Farjat G, « Entre les personnes et les choses, les centres d'intérêts (prolégomènes pour une recherche) », *RTD civ.* 2002 ; p. 221.
16. Grinbaum A, *Les robots et le mal*. Desclée de Brouwer, 2019
17. See : Teller M, "L'avènement de la deep law », *in Mélanges Alain Couret*, Dalloz. 2020
18. Data processing operators are obligated to follow new data principles: the purpose principle, proportionality and pertinence principle, the principle of limited storage times, and the principle of security and confidentiality.
19. Cardon D, *A quoi rêvent les algorithmes. Nos vies à l'heure des big data*, Seuil, 2015 ; Murray, D., & Fussey, P. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review.* 2019; *52*(1), 31-60. doi:10.1017/S0021223718000304
20. Rouvroy A, Berns T, "Le nouveau pouvoir statistique. Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps 'numériques'…", *Multitudes*, 2010, No. 40, p. 88
21. Fabbrini, F & Celeste, E, The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal.* 2020;*21*(S1), 55-65. doi:10.1017/glj.2020.14
22. Balkin J, "The Three Laws of Robotics in the Age of Big Data", *Ohio St. L.J.*, 2017, vol. 78, p. 1217
23. Andrews L, *I know who you are and I saw what you did: social networks and the death of privacy,* Free Press, 2011, p. 189

24. Pasquale F, “Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society”, Ohio St. L.J, 2017, Vol. 78, p. 1243