What About Post-Mortem Digital Privacy and Personal Health Data Protection ?

Gauthier Chassang

What about post-mortem digital privacy and personal health data protection?

Gauthier Chassang[1,2,3]

Abstract

Recent efforts from national and international regulators such as the European Union (EU) concentrated on protecting privacy of the living individuals. But in the big data era where the global digitalisation of all the economic sectors allows world's datafication and of daily professional or intimate life, we will inevitably face more questions on what constitutes or should constitute individuals' digital privacy after the data subject passed away, the so-called "post-mortem digital privacy". The doctrine defines post-mortem privacy as "the right of a person to preserve and control what becomes of his reputation, dignity, integrity, secrets or memory after death"[4]. Questioning post-mortem privacy is particularly important where the data at stake are considered as sensitive personal data categories, which includes health-related personal data and genetic data according to the EU GDPR. First, this article explores existing major pieces of regulations in order to figure out if specific provisions exist which would grant special protection to personal health data after data subjects' death. We explore International and EU legal instruments, hard- and soft-law, including ethical recommendations, pertaining to personal health data protection, to healthcare and biomedical research (Part 1). Second, we will explore some existing post-mortem digital privacy frameworks with examples of policies voluntarily set up by important actors of the digital world, or set up at a research project's level, and with an example of national law, in France (Part 2). This exploratory work does not aim to be exhaustive but constitutes a plea to further investigate the ethical, legal and social issues and innovations in the field in the coming years.

[1] Inserm, UMR 1027, Equipe BIOETHICS, Toulouse, 31000, France.
[2] Université Toulouse III – Paul Sabatier, Université de Toulouse, Toulouse, 31000, France.
[3] Plateforme « Ethique et Biosciences » (Genotoul Societal), GIS Genotoul, Toulouse, 31000, France.
[4] Edwards, L., & Harbinja, E. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment Law Journal, 32*(1), 101–147.

Introduction

The raise of big data in health entails big hopes and big challenges. Relying on the increased digitalisation of health systems and services, and on the profusion of connected devices offered to professionals, patients and consumers, the management and uses of big volumes of personal data generates important challenges in our modern societies in terms of privacy and personal sensitive data[5] protection, two fundamental individual rights[6]. Big health data are definitely new important informational resources to support the development of precision medicine, to improve healthcare provision and public health policies, to feed scientific and technological health research. But these data necessitate a better organisation of health systems and deserve specific attention to ensure wise, lawful and ethical uses. Indeed, these data are also the targets of different lusts triggering serious ethical and legal challenges for citizens and policy-makers. Among these challenges, the so called "post-mortem privacy" could become crucial in the future if we consider the large amount of digital data produced daily in the internet of things world and its related trend of exponential growth[7]. Nevertheless, to date, this topic seems insufficiently addressed from an ethical and legal point of view. But it is good to remember that digital personal data presents a specific feature deserving particular attention, the digital data lifespan. Digital data survives biological entities. With adequate storage, digital information is virtually eternal and some authors nicely mentions our entry into the age of digital immortality or "e-mortality"[8]. Digital data, independently of its source, should constitute an immaterial patrimony for the humanity representing, at individual and population levels, the digital memory of past life events, of various socio-economical phenomena, of people's digital identities and personalities[9], from which various profiles[10] could be extracted. In other words, a raw, imperfect, but very scalable and highly reusable informational legacy for current and next generations. In parallel to the massive digitalisation of societies and its resulting constant data storm, we are in a context of a global population aging[11]. This situation will inevitably increase both natural deaths and issues related to post-mortem digital data privacy. A consequent part of these data could qualify under the scope of several legal instruments such as the European Union's (EU) General Data Protection Regulation

[5] Including health-related data, genetic and biometric data in the meaning of Article 4 and 9(1) of the EU General Data Protection Regulation.

[6] Charter of Fundamental Rights of the European Union (CFREU), OJEU C 364/9. Article 7 and 8. 18 December 2000.

[7] IDC. The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. 18 June 2019.

[8] Murata, K. and Orito Y. (2014). Privacy after Death. Proceedings of ETHICOMP 2014 (University Pierre et Marie Curie, Paris, France), pp. 1-9.

[9] Floridi, L. (2011). The informational nature of personal identity. *Minds & Machines, 21*, 549–566.

[10] E.g. of this profiling potential: Carrie Wong J. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. The Guardian. 17 March 2019.

[11] OECD plans a significant increase of very old persons in the world by 2050 with almost 10% of the total population that will be 80 years old and over (compared to 1% in 1950). OECD Labour Force and Demographic Database, 2010.

(GDPR)[12], as sensitive personal data and health data whose processing deserves particular protection due to privacy risks. Therefore, it is useful and timely to envisage and to discuss post-mortem privacy from an ethical and regulatory point of view. The doctrine defines post-mortem privacy as "the right of a person to preserve and control what becomes of his reputation, dignity, integrity, secrets or memory after death."[13] But is post-mortem privacy recognised and protected as such regarding digital health data? If so, how? If not, is there any kind of protection? To what extent? Do we have example of regulatory approaches touching upon post-mortem privacy? By making our focus on personal health data defined as all personal data concerning the physical or mental health of an individual, including the provision of health-care services, which reveals information about this individual's past, current and future health, this paper explores existing major pieces of privacy regulations at International and EU level, both through "hard law" and "soft law" instruments, in order to take a non-exhaustive picture of current provisions that would found post-mortem digital privacy concepts and grant special protection to personal health data after data subjects' death (Part 1). Then, we will explore specific approaches adopted first, at the level of data controllers, with examples of policies adopted by big internet actors and in the context of an international research project, and second, at national law level, with the example of the current provisions in French law. Throughout the paper we will not specifically address the issues related to forensic medicine and its related special legal framework in order to concentrates on two broader contexts namely the internet and health systems.

1. Post-mortem digital privacy and personal health-related data in International and EU law

A. No explicit recognition of an individual right to post-mortem digital privacy

Since the Universal Declaration of Human Rights[14] that recognised human dignity and privacy as fundamental individual rights at international level, the updating of privacy protection laws and regulations became a central topic for most governments[15] and international organisations in this decade (2010-2020), all realising both the rapidness of technological progress in ICTs, the potentials of digitalisation for critical sectors, and the related major ethical, legal and societal challenges and risks of such a trajectory. The EU paved the way to this global movement with the famous GDPR which became a modern

[12] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).

[13] Edwards, L., & Harbinja, E. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment Law Journal, 32*(1), 101–147.

[14] UN. Universal Declaration of Human Rights. General Assembly Resolution 217 A. 1948. Article 12.

[15] UN. Data Protection and Privacy Legislation Worldwide. "107 countries (of which 66 were developing or transition economies) have put in place legislation to secure the protection of data and privacy. In this area, Asia and Africa show a similar level of adoption, with less than 40 per cent of countries having a law in place." The level of protection ensured and the value of such rights within Constitutional law can vary from a country to another. Retrieved 7 February 2020.

privacy protection landmark worldwide. Indeed, the EU inspired other governments on the necessity to address the issue of data protection and to eventually legislate or revise their current legislation for granting citizens with enhanced protection of their personal information (e.g Brazil, Australia, Mexico etc.). Interestingly, some giants of the digital industry, which are more and more active in the fields of health and biomedical research, represented by their Chief Executive Officers, such as Mark Zuckerberg (Facebook, Twitter, Instagram) and Tim Cook (Apple), have called their government for "comprehensive privacy legislation similar to GDPR"[16]. All this could lead to an alignment of national laws, hopefully for the sake of human rights and freedoms protection, further post-mortem digital privacy considerations, and in the spirit of openness to responsible data sharing and international collaboration.

Despite these advances, to date, the only legally binding International Convention on personal data protection is the Council of Europe Convention 108+ [17,18], as revised[19] in 2018, an historic cornerstone for privacy protection since 1981. Its updating started slightly after the EU initiative. But Convention 108+ falls short of protecting post-mortem digital privacy as it excludes the topic from its scope. Indeed, the Explanatory Report of the modernised Convention clearly states that "The Convention applies to living individuals: it is not meant to apply to personal data relating to deceased persons. However, this does not prevent Parties from extending the protection to deceased persons."[20] In other words, personal data protection law confers subjective rights, personality rights, which shall be materialised for and exercised by an individual, as a natural person, living and autonomous[21] data subject, in order to protect his dignity, his personality and intimacy. Deceased persons are simply not anymore considered as data subjects entitled with such rights. They do not have legal personality any longer and are practically unable to exercise their rights. The same approach is adopted within EU law. The EU privacy protection framework is mainly composed of two specific and complementary acts[22], the famous GDPR of 2016, in force in all EU Member States since May 2018, and the e-Privacy Directive[23,24] of 2002 presently revised in the

[16] Elizabeth Shulze. The US wants to copy Europe's strict data privacy law – but only some of it. CNBC. Tech. 23 May 2019.

[17] Council of Europe. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, CM/Inf(2018)15-final. 18 May 2018.

[18] Council of Europe. Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol). 10 October 2018.

[19] Council of Europe website. Modernisation of Convention 108: https://www.coe.int/fr/web/data-protection/convention108/modernised

[20] Explanatory Report CETS 223, cited supra. Para. 30.

[21] In most jurisdictions, data subjects with no or limited legal capacity to act autonomously can exercise their privacy rights through various legal representatives identified or designated by National law. This is interesting to keep in mind.

[22] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR. 12 March 2019.

[23] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJEU L 201 , 31/07/2002, p. 0037 – 0047.

[24] European Commission. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and

perspective of the adoption of a new EU Regulation. This framework aims to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, to online privacy, and to ensure the free movement of personal data within the EU, including for electronic communication and public information society services. These texts are not specific to health-related matters and apply limitedly to such matters which remain a competency of EU Member States but they fix the main legal principles and testify of the spirit in which data protection should be tackled in these fields. The GDPR created new data protection mechanisms, based on decentralised protection duties relying on data controller and processors' accountability. It reinforced individual rights for Europeans, with a dose of extraterritoriality[25], through a risk-based approach considering the need to balance the individual's personal data protection and privacy as fundamental rights in democratic societies[26], and the necessity to allow legitimate personal data access, sharing, transfer and use by responsible thirds. While we must salute the pioneering effort of the EU for improving the level of protection afforded to citizens in a rapidly evolutive digital environment, post-mortem privacy has been left aside. Data protection is only conceived as regards to living data subjects, as recalls recital 27 of the GDPR stating that "this Regulation does not apply to the personal data of deceased persons". Notwithstanding, it adds that "Member States may provide for rules regarding the processing of personal data of deceased persons", opening thus a leeway for Member States regulators to go ahead in post-mortem digital privacy in national law[27]. Convention 108+ Explanatory Report and this GDPR recital are interpretative guidelines which should not be interpreted as granting a total deregulation nor a free market of deceased persons' personal data. The Council of Europe and the EU could not tackle all the issues regarding digital privacy, in particular where the topics ask for further ethical debates and consensus-building within and between States before considering any harmonised policy. But again, this does not mean that there are no post-mortem privacy issues or related specific regulatory needs, including in health. Like the protection of the human body[28] of deceased persons that is founded on the memory of the deceased person under human dignity and integrity principles, as a physical representation of the deceased person deserving respect even though the soul of the person founding personality rights attributes has gone away, aggregated personal data form a digital representation of that person which, even more than his body, survives the death of their

repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM(2017) 10 final. 2017/0003(COD). 10 January 2017.

[25] GDPR op.cit. Article 3. See also: Judgment of the Court of Justice of the European Union, Case C-507/17, 24 September 2019.

[26] By reference to the Charter of Fundamental Rights of the European Union. OJEU C 364/9. Article 7 and 8. 18 December 2000.

[27] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP 136, p.22. This opinion also recognise that in certain circumstances deceased person's data could receive some kind of protection.

[28] Of note, even if the protection of the human body integrity covers deceased persons' body as a component of privacy protection seems acquired, recent scandals oblige to maintain a careful oversight on the matter. See: Anne Jouan. Scandale du don des corps: le juteux commerce de cadavres. L'Express. 25 February 2020.

initial subject and can be utilized, notably for marketing purposes[29]. By so, this analogy tends to consider post-mortem digital data as deserving an equivalent respect, in the memory of data subjects, as "digital remains", a "collective term used to generally describe the expressions, possessions and impressions that a decedent leaves behind in digital media"[30]. These includes proprietary digital goods but also embrace other non-proprietary digital data related to the deceased person. And these latter can reveal a lot about the data subject's lifestyle, philosophy, opinions, and could be used by different private or public actors[31] having access to them for various purposes which could not have been agreed, nor envisaged, by the living data subject. Digital remains, from which individual profiles could be designed through data matching, can include any type of personal data, from usual personal email or postal address to health-related data or other sensitive data such as biometric or genetic[32] data, as far as the data can be accessed and processed. While it seems more obvious today that the family and progeny of the data subject could have a privacy interest in controlling the uses of their deceased relatives' data, a crucial question is to identify who owns the control rights over these data (and where relevant, over biosamples) and whether the claimant request is legitimate and founded to argue for special measures to be taken[33]. This triggers complex issues which are even more complex in the case of genetic data processing, taking into account the current context of precision medicine developments relying both on the availability of large databases of genomic sequences, on data sharing[34] and on cooperation between various actors. Indeed, genetic data are known for being

[29] E.g. Smith, Shannon Flynn1. 2013. "If it Looks Like Tupac, Walks Like Tupac, and Raps Like Tupac, it's Probably Tupac: Virtual Cloning and Postmortem Right-of-Publicity Implications." *Michigan State Law Review*, (5): 1719-1761. A use case of a digital clone of a deceased person, in that case, of the famous deceased rapper Tupac Shakur whose the virtual clone performed a representation during a Coachella concert in 2012. A case questioning the attribution of rights for using the digital image of celebrities which impact decedents' interests.

[30] Buitelaar, J.C. Post-mortem privacy and informational self-determination. *Ethics Inf Technol* **19,** 129–142 (2017). https://doi.org/10.1007/s10676-017-9421-9

[31] From search engines operators, websites' owners, advertising companies, data brokers, to academics, authorities or simply individuals.

[32] In this regard the famous case of Henrietta Lacks shows the importance of considering post-mortem privacy for the protection of deceased person's familial interests based, in that case, on biological samples and data uses, on the commercial interests related to scientific research discoveries, knowledge and products (i.e. immortal cell lines HeLa). First, Henrietta Lacks never consented to the procurement and use of her biological samples, what was not at that time a breach of applicable laws and ethical principles; second, her family never get compensated for the huge commercial uses of the cells which occurred after Henrietta Lacks passed away. The case triggered ethical debates about biological samples and data property and secondary uses, informational autonomy and research regulations. See: Beskow LM. Lessons from HeLa Cells: The Ethics and Policy of Biospecimens. *Annu Rev Genomics Hum Genet*. 2016;17:395–417. doi:10.1146/annurev-genom-083115-022536.

[33] As noted in the literature through a case-law analysis in the US, "the privacy interests of the deceased prevailed over the requests and wishes of their families, and the families were denied of the deceased person's personal belongings (emails and the content of Facebook profile)." See: E Harbinja. Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives? (2013) 10:1 *SCRIPTed* 19 http://script-ed.org/?p=843

[34] E.g; with the European "1+ Million Genomes' Initiative. See: https://ec.europa.eu/digital-single-market/en/european-1-million-genomes-initiative

"uniquely identifying and familial by nature"[35,36]. This characteristic, together with the difficulties for achieving total anonymization[37], questions existing legal notion of data subject as the identified or identifiable natural person to which the personal data processed relates[38], regarding its scope and its flexibility. Indeed, because of the nature of genetic data and the potential to get incidental findings from their processing, it could be considered to interpret this notion as encompassing third persons whose privacy interests would prove to be directly engaged through the data processing, in particular the deceased data subjects' family members. It should be the same regarding health data. One could argue that the notion of data subject inscribed in both texts does not make reference to a life criterion but only refers to the existence of personal data related to an identified or identifiable individual. This, again, let us think that post-mortem privacy interests could theoretically be vested by a legitimate third envisaged in the spirit of the Convention and GDPR aims, and that, finally, the sole criteria to consider in the domain is the data lifespan, not the initial data subject lifespan, and its relationship with actual privacy interests of a living natural person, as a kind of secondary data subject. But to date, most of the States did not take the opportunity offered by these master legal pieces to further legislate on the topic by eventually specifying the notions of personal data and data subjects regarding post-mortem issues. Nevertheless, some States, like France, introduced legal provisions as to what we could call "digital legacy management", outside any legal property regime (Cf. infra, in Part 2).

At global soft-law level, in October 2019, the United Nations (UN) Organisation, through the Office of the High Commissioner for Human Rights (OHCHR) and its Special Rapporteur on Privacy, Joseph Cannataci, proposed a draft Recommendation on the protection and use of health-related data[39], recently revised[40]. The aim is to initiate or stimulate standardisation of national approaches to personal health data protection with the objective of framing their collection, exchange and use for several purposes such as for healthcare, research, insurance but also for other non-health-related purposes, while recognising a number of new rights and protective measures at international level. As the Special Rapporteur said, "health technologies, if used in a way that respects the privacy of patients, can assist health practitioners and researchers as well as those seeking healthcare, but this cannot be at the expense of people's privacy". This statement is furthermore important because, as he said, "health-related data is very sensitive and has high commercial value. There is a largely

[35] Caulfield T, McGuire AL. Policy uncertainty, sequencing, and cell lines. G3 (Bethesda). 2013;3(8):1205–1207. Published 2013 Aug 7. doi:10.1534/g3.113.007435.
[36] UNESCO. Universal Declaration on Genetic Data. 16 October 2003. Article 4.
[37] Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. Science. 2013 Jan 18;339(6117):321-4. doi: 10.1126/science.1229566.
[38] Convention 108+, Article 2 ; EU GDPR, Article 4(1).
[39] UN OHCHR. Draft Recommendation on the protection and use of health-related data. First draft for consultation. 2019. https://ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf
[40] UN OHCHR. Recommendation on the protection and use of health-related data. Annual Report to the Human Rights Council and the UN General Assembly. 5 December 2019. https://ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf

hidden industry that is already collecting, using, selling and securing health data. This has a major impact on our privacy and is of enormous concern"[41]. While this industry is mainly related to health data accessible on the internet[42] and through connected devices[43], professionals in the health care system can be approached for selling such personal data. Therefore, it is important to consider the ethical tensions and legal issues in their different contexts, these involving different actors, interests and values, namely, in the public internet sphere and within the health systems.

In addition, from a conceptual point of view, it is useful to clarify that post-mortem digital privacy attempts to empower the data subject with a right to consider conditions for post-mortem uses of the data related to his personal identity, including a right to decide about a post-mortem representativeness, through a natural person who would act in, and for, the respect of the initial data subject's will and conception of privacy. It also includes a right to get adequate protection from State and actors of the data processing, an aspect that should not be neglected. Therefore, post-mortem digital privacy seems to be a twofold concept[44]. First, it aims to legally allow for living data subjects to freely organise their digital after-life while they are alive. This regime is based on the proactive autonomous choices of the living initial data subjects regarding future data processing. Second, it aims at ensuring by default the protection of digital data after the data subjects' death, including where the initial subject did not consider the matter during their life, in consideration of the dignity due to decedent memory and of the best interest for their descendants and family. This is a delegated post-mortem privacy protection regime relying on the involvement of third persons' or entities' which have a custodianship role regarding data access and uses either granted by the initial data subject or by law.

B. Clues in favour of a limited and implicit post-mortem digital privacy protection through interpretation of current provisions applying to personal health data uses

Even though there is no direct specific provision on post-mortem privacy in the Convention 108+ and the EU GDPR, we will see that some current provisions at European and International levels seem indirectly to cover post-mortem data processing issues, or at least open new possibilities for operators and data subjects to consider post-mortem digital privacy management and particular limitations related to health and research fields.

First, we suggest to identify some interesting elements which could ground a post-mortem privacy regime based on data subject's autonomy.

[41] UN OHCHR. UN expert warns of enormous privacy concerns over health data as he unveils international protection standards. 2019.
[42] Madhumita Murgia and Max Harlow. How top health websites are sharing sensitive data with advertisers. Financial Times. Epub. 13 November 2019.
[43] Ed Pilkington. Google's secret cache of medical data includes names and full details of millions – whistleblower. The Guardian. Epub. December 2019.
[44] Jean Herveg. Une vie privée après la mort ? Le cas des données relatives au patient. Journal des Tribunaux. Ed. Larcier. N°6189. 3 Septembre 2005. P.489-499. In this paper, a similar analysis is performed and distinguishes between "subjective" protection and "objective" protection regimes in post-mortem privacy.

While data subject's consent could not be the legal basis chosen by the controller to process the personal data[45], it is part of EU data ethics and best practices to obtain additional, explicit consent to the secondary use of the data, including in specific sectors such as scientific research[46]. In any case, a prior fair and clear information shall be provided to the data subject about personal data storage duration before destruction, envisaged uses of the data in that period, anonymisation policy and intention to transfer the data to third entities, in a way that allows for transparency, at an early stage, and sufficient understanding of potential risks related to data subject's rights and freedoms. Such a transparency requirement should normally cover post-mortem processing issues, provided that the actors had set up appropriate policy. Identification and information about personal data processing limitation criteria after data subject's death seem particularly useful for transparency purposes. In this regard, the UN draft Recommendations of 2019 formulated a special rule entering within the scope of our investigation (provision which has been then modified in the version of December 2019). This provision was based on the same assumption than the one formulated within the Convention 108+ and the EU GDPR which recognise that "it is not always possible to determine beforehand the purposes of different research projects at the time of the collection of data", and by then, that "data subjects should be able to express consent for certain areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards", what opens to future limited data uses, including post-mortem. But, in its initial draft recommendations, the UN went further, inspired by the UK Human Tissue Act. Indeed, the draft continued by stating that "data subjects may also give prior consent to the future use of their health-related data for scientific research purposes after their death. In the absence of such consent, any health-related data retained must be anonymised after the death of the data subject."[47] This was a direct recommendation for post-mortem privacy right of living data subjects. Nevertheless, the corresponding article[48] of the December 2019 version of the UN Recommendation does not anymore mention this provision. But the topic has been addressed and it is safe to interpret the latest version of this recommendation as including possibilities for the living data subject to open, limit or reject possibilities for future personal data uses with different, yet undefined, research purposes, in the respect of his autonomous informed decision. Possible broad areas of scientific research in which the data are likely to be used should be defined and communicated to data subject. The Recommendation usefully refer, for instance, to the use of the World Health Organization's International Classification of Diseases. Data subjects should also be provided with "comprehensible information that is reasonably precise" about "the means and capacity to extract novel forms of health-related data as well as uncertainties to what might be extractable in the future."[49] The UN Recommendation of December 2019 also mentions ethical compliance of

[45] EU GDPR. Supra. Article 6.
[46] European Commission. Ethics and data protection. 14 November 2018. p.11.
[47] UN OHCHR. Draft Recommendation, 2019, cf. supra. Article 15.6.
[48] UN OHCHR. Recommendation, December 2019, cf. supra. Article 21.9.
[49] UN OHCHR. Recommendation, December 2019, cf. supra. Article 21.7(b).

the data processing projects and the necessity to perform independent review of health-related data access requests for research uses[50]. As specified by the European Commission in the field of research, if the data are intended to be used in "multiple projects or for multiple purposes, or if it is not possible fully to identify the purpose of the data processing at the time of data collection, it may be appropriate to use a consent management application. Various service providers now offer ethically robust, secure informed consent platforms that can help you to manage, document and evidence your consent processes"[51]. Dynamic consent[52] technologies could be helpful to preserve a link with the living data subject and the forms could include a dedicated section on post-mortem digital privacy with a possibility for data subjects to name a person for exercising representation in data management after his death. But dynamic consent could lead, inter alia, to "click fatigue" or over-engagement and designating a representative for research matters could not be a good solution if we consider existing legal and ethical safeguards in place in that sector.

The recent right to be forgotten[53,54,55], as a complement to the right to erasure regarding the digital environment, as well as the right to restriction of processing[56] established under the GDPR are also of interest when considering post-mortem privacy regulatory approaches and related limitations in the field of health and biomedical research based on individual autonomy. Indeed, these rights empower the living data subjects in the control of their digital life by allowing them to decide about their digital death and to request the data controller to erase their personal data under certain conditions. The controller will have to warn other data controllers or processors to whom the concerned data have been communicated about the data subject's instructions and their consequences. They will need to respect data subject's choice and act accordingly under the instructions of the controller. The GDPR plans several limits to that right, notably where the controller can oppose a legitimate interest in keeping the data without anonymisation or where the data are necessary for compliance with a legal obligation or for reasons of public interest[57].

[50] UN OHCHR. Recommendation, December 2019, cf. supra. Article 21.2 and 21.3.
[51] Op.cit. p.12.
[52] Kaye, J., Whitley, E., Lund, D. *et al.* Dynamic consent: a patient interface for twenty-first century research networks. Eur J Hum Genet Vol. 23, 141–146 (2015). https://doi.org/10.1038/ejhg.2014.71
[53] EU GDPR. Supra. Article 17.
[54] De Terwangne, C. Droit à l'oubli, droit à l'effacement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique. Dans : Enjeux européens et mondiaux de la protection des données personnelles. Chapitre 3. 245-275. (Création information communication). Ed. Larcier. 2015.
[55] De Terwangne, C. The right to be forgotten and informational autonomy in the digital environment. In: The ethics of memory in a digital age: interrogating the right to be forgotten. 82-101. Palgrave MacMillan. 2014.
[56] EU GDPR. Supra. Article 18.
[57] In particular in processing for archiving purposes in the public interest, historical, scientific research or statistical purpose according Article 89 of the GDPR and other applicable rules such as those related to the EU Clinical Trial Regulation. Examples of legitimate interests or public interest purposes could be characterized where the personal data are necessary to allow social security services and health insurance functioning or healthcare establishments administration, healthcare practices implementation, health products or technology assessments and activities related to the "–vigilances", such as pharmacovigilance, are necessary to protect the vital interest of the data subject or of a third, without possibility to achieve these objectives without using the concerned personal data.

Compromise is part of privacy[58]. This is particularly true in health and scientific research where solidarity is crucial. Personal data processing after death can greatly benefit to other patients receiving health services whose design and procedures have been conceived and will be improved by using, at least partly, personal health data, in order to generate new biomedical knowledge, new healthcare services, procedures or medical products. But whatever the limitations, these rights entail the roots of post-mortem privacy as we defined because their effects could permanently affect the data, including after data subjects' death, in a way that will preserve their very own conception of privacy for the whole data lifespan. It is good to remind that big challenges remain for ensuring full data erasure, particularly on the internet, and that the European Court of Justice restricted the application of the right to be forgotten regarding its territorial scope[59], based on proportionality. In my personal opinion, this EU judicial decision diminishes the initial GDPR ambition to grant to internet users the possibility to obtain full and efficient privacy protection worldwide even though the data subjects' requests are legally legitimate. This limitation indirectly results in a digital personal data permanency on the internet. This judgement should raise awareness of internet users about the side-effects of internet use and it should serve to increase the attention brought to post-mortem privacy issues in order to limit risks to bypass data subjects' will, based on territorial limitations of law enforcement.

The new right to data portability also entails potentials regarding post-mortem privacy management and related regulatory approaches. In short, where data portability applies[60], the data subject can ask data controllers, during their life, to obtain the data in a machine-readable format allowing reuses from the data subject (vertical portability) or to transmit the data to another controller, without hindrance from the initial controller (horizontal portability). He could, for example, decide to provide personal data coming from a connected health-related device or apps to a research data repository that will store and manage access to the data on the long run, including after data subject's death, in the respect of his choices. Based on data portability, post-mortem privacy could be organised by the data subject before death. It is a way to regain control over the data provided to thirds and to eventually repurpose them in a way data subjects deem respectful of their privacy and personality. This could contribute to stop potentially abusive data lock-in practices from profit or non-profit organisations and eventually serve scientific research if data subjects would decide to provide the data to open-controlled data repositories established for research purposes. However, it is not sure that both data subjects and repositories would be in favour of such a possibility outside traditional health data pipelines. In any case, it is interesting to further explore these potentials for envisaging developments at national level post-mortem privacy management issues in the spirit of the GDPR.

[58] In any cases, transparency of the measures taken to respect data subject's wishes must be ensured by initial data controller.

[59] ECJ. Google LLC c/ CNIL. Case C-507/17. 24 September 2019.

[60] Chassang, G. , Southerington, T. , Tzortzatou, O. , Boeckhout, M. , & Slokenberga, S. Data Portability in Health Research and Biobanking: European Data Protection Law Review, Volume 4, Issue 3 (2018) pp. 296 – 307.

Elements presented above are consistent with the trajectory of international regulatory documents adopted by the Council of Europe including data protection issues. The famous Council of Europe Oviedo Convention[61] of 1997, known as the Convention on Human Rights and Biomedicine, and its Additional Protocols, are considered by some as the unique international binding *lex specialia* ruling research activities in the biomedical field. These texts regulate individual's rights and autonomy as research participants, researchers' duties of transparency, security, confidentiality, and highlight ethical and deontological principles applied to specific research fields. The Convention echoes the underlying ideas of post-mortem digital privacy protection namely the respect of deceased individual autonomous choices and the protection afforded by third entities mandated to ensure a delegated protection of deceased persons' privacy. Also, the Convention specifically address measures for the protection of the dignity of human beings and does not explicitly exclude post-mortem digital privacy issues. Without dealing with the topic, it regulates the possibility to access to the human bodily materials from deceased persons, in the direct therapeutic benefit of a living person[62], and the possibility to store biological samples for further uses with different purposes, in conformity with appropriate information and consent procedures[63], a logic that is similar to the one used in data protection regulations at International and EU levels. The Additional Protocol on Biomedical Research adds that participants must be informed "of any foreseen potential further uses, including commercial uses, of the research results, data or biological materials"[64] in order for them to express their consent or potential wishes as to limitations. This empowers living data subjects to envisage the future uses of these materials and could easily include post-mortem privacy issues. Interestingly, the Protocol deals with the protection applied to a person unable to consent (e.g. unconscious patient) and the remits of her representatives which could act on her behalf in decision-making[65]. It also regulates a number of specific situations[66] but not post-mortem digital privacy issues.

A number of focused and complementary international soft-law instruments much respected in the health field, namely the World Medical Association's Declarations of Helsinki[67] and of Taipei[68], and the Council of Europe Recommendation on biobanking-based

[61] Council of Europe. Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo Convention). CETS n°164. Oviedo. 4 April 1997.
[62] Explanatory Report to the Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine. 4 April 1997. Point 118.
[63] Oviedo Convention, cf. supra. Article 22.
[64] Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research, CETS n°195, Strasbourg, 25 January 2005. Article 13(2)(vii).
[65] Op.cit. Article 15.
[66] Op.cit. Chapter VI.
[67] WMA. Declaration of Helsinki – Ethical Principles For Medical Research Involving Human Subjects. 64th WMA General Assembly, Fortaleza, Brazil, October 2013.
[68] WMA. Declaration of Taipei on Ethical Considerations Regarding Health Databases And Biobanks. Revised by the 67th WMA General Assembly, Taipei, Taiwan, October 2016.

research[69] of 2016 reiterates the respect of the data subject's expressed will regarding the use of their samples and data[70], with no temporal nor territorial limitations. They also organise, within their scope, delegated post-mortem privacy measures. Nevertheless, none of them address a right for the data subject to name a representative who will be the contact for dealing with post-mortem digital privacy matters.

More generally, going further into a post-mortem digital privacy based on individual's autonomy in health systems and biomedical research should be made with caution in order not to be counterproductive. While clarifications are needed on the rules in most EU member States laws, current ethical and legal safeguards seems favouring an extended privacy protection, regardless of data subject's status, alive or dead, based on solidarity, professional duties and mandatory checks of data uses' projects. The situation could be different within e-health and on the internet where the actors are not so bound compared to health systems and biomedical research settings. Indeed, as the European Group on Ethics of Science and New Technologies (EGE) notes about a current paradigm shift, if new technologies have "opened the way for citizens to engage in health projects, actions and initiatives which reflect strong solidarity-based objectives", the EGE is "concerned that these developments change the balance of emphasis as to who should provide solidarity and according to which criteria. We should be mindful of potential shifts in shared understandings of solidarity, from a state managed process to one organised and driven by citizens."[71]

Second, we can identify some interesting elements which could base a post-mortem digital privacy regime based on a delegated decision-making and on accountability.

Delegated post-mortem digital privacy can be understood as the possibility offered to an individual to be represented by a trustworthy third natural or legal person in decision-making about privacy management after that individual passed away. This can be achieved in several ways.

First, by identifying the type of person able to act as a representative for these matters and by identifying his remits. These aspects are not covered by European or International data protection laws, except where the individual is unable to consent, is a child or is considered as part of a vulnerable population. In such cases, legal representatives (e.g. parents) are in charge of providing necessary authorisations on behalf of the data subject for allowing personal data processing, including for healthcare purposes or for participation in a biomedical research. But again, these references are not specific to post-mortem privacy. They only demonstrate that such representativeness can be considered in defence of third's privacy interests in health matters.

[69] Council of Europe. Recommendation CM/Rec(2016)6 of the Committee of Ministers to member States on research on biological materials of human origin. 11 May 2016.
[70] E.g. Article 14 of Rec/CM 2016.
[71] EGE. Opinion n°29. Ethics of New Health Technologies and Citizen Participation. 13 October 2015. P.63.

Second, by ensuring that the law provides necessary duties to data controllers and processors for considering post-mortem privacy issues within their activities. There are some obligations of interest regarding post-mortem digital privacy issues to which data controllers and processors using personal health data are already submitted. Among them, the data storage limitation principle usually is a general principle in European and international data protection laws. This principle requires that no personal data may be stored longer than necessary for reaching the processing purpose for which they have been collected. Exceptions are accepted regarding certain processing. As Article 5(e) GDPR specifies, "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject". Such a provision underlines the prominent role of data controllers for taking measures of protection, in particular for ensuring legally compliant storage of and access to the data. Both aspects require technical and organisational measure to respect data subjects' rights and essential principles such as data minimisation, through pseudonymisation, encryption or anonymisation. In addition, Article 25 GDPR obliges, in a form of a general principle, to adopt an approach of data protection-by-design and by default. One could argue that such a general requirement shall sooner or later include a duty to consider post-mortem privacy and data protection after data subject's death at an early stage, including where there is no specific legislation at national level, just for coping, by design, with the GDPR principles of data minimisation, storage limitation, transparency or accountability for example. This would be a virtuous exercise for data controllers and processors to consider specific technical and organisational measures, policies or code of conducts, and to envisage the content of the information to be provided to the data subject before starting the processing, related consent options, and to build policies for post-mortem data access and storage in compliance with applicable laws and standards. Of course, this extensive interpretation could be counter-argued by the fact that nothing explicitly imposes such a questioning in the GDPR. That's also correct. But, in the fields of healthcare and biomedical research, GDPR scope is limited, national laws prevail and could be more precise on these aspects in such areas (cf. Article 89 GDPR). The GDPR is not an island and it must be read in conjunction with other binding acts and recommendations at international level (see above) which could also, in the future, tackle more specifically post-mortem digital privacy.

Third, by having third independent entities able to decide, to make collegial decisions or to provide opinion about post-mortem sensitive data uses according to ethical criteria and applicable laws. As we have seen, if individual autonomy is not addressed at International nor EU levels, the whole regulatory framework applicable to scientific research activities refers to Ethics Committees. This includes the Convention of Oviedo, its Additional Protocols, and the complementary international soft-law instruments above-cited. All of them request that research projects using data or human biological samples must be reviewed by ethics

committees in order to ensure independent examination of their scientific merit, assessment of the importance of their aims, and pluridisciplinary review of their ethical acceptability. In addition, Article 19 of the Declaration of Taipei adds the role of independent ethics Committees reviews at the time of the setting up of the databases and biobanks, including when they relate to deceased persons, as specified in its Article 4. The UN Recommendation usefully refers to bodies in charge of controlling genetic data access, namely databases and biobanks, as long-term custodians of individuals' privacy. This also allows to further consider the role of such important third entities (databases or biobanks) in the delegated post-mortem privacy protection concerning controls of health-related data access and data minimisation[72]. It is now common that biobanks and health databases include collegial entities reviewing projects, including from ethical and legal perspectives[73], before granting access to the resources they hold. The UN also affirms in what we could qualify as a principle of "health data repositories' purpose impermeability" that requests for forensic medicine purposes should be rejected[74]. Exceptions are planned where there is no alternative and provided that the requester access is granted by a court order. The recent Council of Europe Recommendation[75] of 2019 on the protection of health-related data does not change the state-of-art regarding post-mortem digital privacy issues. Nevertheless, it adds a number of interesting specifications regarding such sensitive data processing which should be considered through the prism of post-mortem digital privacy, such as the provisions regarding mobile devices[76], or concerning the communication of health-related data for purposes other than providing or administrating healthcare and which explicitly mention that insurance companies and employers "cannot be regarded as recipients authorised to have access to the health-related data of individuals" except in limited circumstances[77]. All these provisions have interpretative potentials for considering post-mortem digital privacy regulatory approaches.

Shared responsibilities regimes between data controllers and processors regarding personal data processing have been fixed at European level, in particular in the EU GDPR. The UN Recommendation adds another recommendation regarding health-related data and open data practices which should also be acknowledged in the perspective of post-mortem digital privacy as it clarifies responsibility sharing in case of damage resulting from open data uses (e.g. re-identification practices). Indeed the Recommendation states that "where health-related data is released as Open Data and a health-related data breach arises from that release, the party that processes the health-related data, and the party that releases it as

[72] UN OHCHR. Recommendation, December 2019, cf. supra. Articles 21.11, 21.12, 21.13.
[73] Mahsa Shabani. Governance of Genomic Data Access for Research Purposes. PhD Thesis. Doctoral School of Biomedical Sciences. KU Leuven. Supervisor: Prof. Pascal Borry. April 2017.
[74] UN OHCHR. Recommendation, December 2019, cf. supra. Article 7.8.
[75] Council of Europe. Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data. Adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies. 27 March 2019.
[76] Op.cit. Chapter VI.
[77] Op.cit. Article 9.2 and 9.3.

Open Data (where they are not the same) shall both be liable to data subjects harmed by such release."[78]

Finally, Convention 108+, like the EU GDPR, encourages self-regulation from data controllers and processors. This is something to consider as it could lead to sector-specific or company-specific regulatory approaches in post-mortem digital privacy. While these various policies could contradict each other, they could also lead to more awareness on issues of post-mortem digital privacy and innovative approaches that regulators and supervisory authorities should scrutinise and if relevant, take inspiration.

2. Examples of post-mortem digital privacy regulatory approaches covering personal health-related data

A. Example of self-regulations based on the autonomous choices of living data subjects

We will illustrate post-mortem digital privacy self-regulation through some examples related to internet service providers and to some research projects.

In a context of health consumerism, many publicly available services propose users access to health-related services, products, support or advice online. For companies, provided or collected data can have a commercial value to develop their offers and improve their marketing strategies or for business with third interested operators. This concerns health data processed through connected e-health devices which are now largely available to consumers, same regarding health-related social networks or direct-to-consumer genetic testing services for example. Online personal health data can take many forms and be managed differently according to applicable national legislations to which the controller and processors are submitted. It is not scarce that such digital health data are unavailable to external medical professionals or researchers, due to data "lock-in" practices of private operators, including when they acquired data subject's consent to data sharing and including after the data subject's death. This "appropriation" can be criticised, in particular where private interests are against uses which could potentially help developing public health innovations, knowledge and policies of public interest. Maybe post-mortem digital privacy measures rooted in the rights we described earlier could enhance such data availability? Whatever, on the internet, transparency is key and citizens' empowerment regarding post-mortem issues is still a big challenge. Data subjects are bound by the contractual terms they agreed online with the service provider, most being still unread by the user or unclear, and some being very favourable to the service provider. Nevertheless, efforts have been made by big online companies (such as Google) regarding the exercise of data subjects' rights to control their digital life. Since a judgement[79] of 2014 related to the implementation of the right to be forgotten fixed under the EU GDPR, Google is now offering, in addition to the

[78] UN OHCHR. Recommendation, December 2019, cf. supra. Article 21.14.
[79] CJEU, Google Spain SL et Google Inc. c. AEPD and M.C. González, C-131/12, 13 May 2014.

possibility of internet users to exercise their right to be forgotten[80], a possibility to submit a request regarding a deceased user's account[81], whatever the type of data contained under their account. This post-mortem digital privacy policy includes two options. It allows the living data subject to eventually plan post-mortem privacy settings through the "Inactive Account Manager", presented as the best way to let them know "who should have access to your information, and whether you want your account to be deleted". It also allows to thirds such as immediate family members and data subject representatives to make a request for either closing and erasing the account of a deceased user, for requesting for funds from a deceased user's account or for obtaining data from this account. Google specifies that any request will be carefully reviewed by their teams and that their primary responsibility "is to keep people's information secure, safe, and private", therefore they "cannot provide passwords or other login details." Using such options will affect the concerned user's Google account and any related products or services. Other operators such as Facebook[82] or Twitter[83] are working on their post-mortem digital privacy policy. Facebook even offer the possibility to the legacy contact to decide about keeping a memorialized account[84] which could eventually continue to evolve with living persons such as family members or friends that could be allowed to publish on this account. The designated legacy contact is the final owner of the account and can decide to close it or to manage certain confidentiality settings[85]. This type of account is not available on the public interface of Facebook.

Post-mortem digital privacy issues regarding genetic data should also be envisaged with regard to the raise[86] of Direct To Consumer Genetic Testing (DTCGT) services and attached risks[87], still often misunderstood[88]. Users of 23andMe and AncestryDNA companies' services can request for deletion of their personal account, including testing results, and destruction of their samples[89]. The terms of services mention different samples and data storage limitations, from no sample storage and destruction by default to 10 years maximum where the user opted for sample storage through 23andMe biobanking consent, and storage "for an indefinite time period" after the initial genetic testing for AncestryDNA. Otherwise, there is no specific options related to post-mortem digital privacy, for delegated privacy settings for example. Both companies require specific user's consent for performing research on the

[80] https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&pli=1
[81] https://support.google.com/accounts/troubleshooter/6357590?hl=en
[82] Facebook Legacy Policy. See https://www.facebook.com/help/1568013990080948
[83] Chris Welch. Twitter halts plan to remove inactive accounts until it can memorialize dead users. The company apologized for confusion around its plan to remove accounts. The Verge. 27 November 2019.
[84] https://www.facebook.com/help/1506822589577997
[85] https://www.facebook.com/help/1568013990080948
[86] Bran Hedeman, Alaap Shah. Privacy Concerns Loom as Direct-to-Consumer Genetic Testing Industry Grows. Epub on Healthlawadvisor.com. Epstein Beker Green blog. 28 June 2019.
[87] Edge MD, Coop G. Attacks on genetic privacy via uploads to genealogical databases. *Elife*. 2020;9:e51810. Published 2020 Jan 7. doi:10.7554/eLife.51810
[88] Jen King. "It's not personal" – DNA, Privacy, and Direct To Consumer Genetic Testing. Standford Law School. Center for Internet and Society. Epub. 7 November 2019.
[89] http://www.citigen.org/2017/07/12/what-happens-to-your-genetic-data-when-you-take-a-commercial-dna-ancestry-test/ (Accessed March 2020)

provided materials and make it quite explicit that they could provide access to the samples and data in the context of commercial or non-commercial partnerships "to learn about human history and migration" or "to discover links between genetic factors and human diseases, traits or conditions"[90]. Both companies inform users about the anonymisation process they implement before giving external access to the materials for research purposes. Recent guidelines issued by the Future of Privacy Forum in July 2018 invites DTCGT companies to "provide a process for Consumers to indicate the handling of their account, such as granting access, deletion, and/or transferring account control, in case of death or if a Consumer becomes incapacitated, and/or, implement a process for a successor to request the transfer of an account after the death or if a Consumer becomes incapacitated[91]", going in the sense of a delegated post-mortem digital privacy policy.

These initiatives should be seen as a complement to limited protection of privacy after death afforded through contract law, some authors[92] even suggest to extend tort law to privacy issues after data subject's death because, inter alia, "a deceased user's right to privacy is at the mercy of the service provider's terms under the contractual approach", and the service provider is deciding alone about the criteria used for assessing post-mortem data access requests in the absence of identified specific legal criteria. Also, privacy policies of online services are rapidly evolving what can weaken individual's control over data management.

At level of research projects, another example of relevant self-regulation can be found in the context of the Personal Genome Project (PGP)[93] in which participants are offered with the opportunity to publish their genomics sequence together with health and trait data for scientific research uses. This project very clearly displays the fact that the data concerned will be "public data" that will be shared "in an integrated, publicly-accessible format using a CC0 waiver or equivalent public domain license", an interesting standpoint. Also, it is made very clear that data are to be considered "non-anonymous", meaning that despite a careful oversight being performed up front, notably through projects' members' Institutional Review Boards (IRB) processes, "neither anonymity nor confidentiality of participant identities or their data are promised to research participants." The participant is able to manage himself the disclosure of data through a public profile online. Regarding post-mortem digital privacy, the project takes good note of the specificity of genomic data and strongly encourages participants within the consent form to designate a proxy (next of kin or other trusted individual) before enrolment, in order that in case the participant dies or become mentally incapacitated during the course of the project, the designated proxy has "the authority to decide to either (a) remove your cell lines and/or data from the study (subject to the limitations on removal described in this consent form); (b) allow the PGP to maintain your cell lines and/or data for continued research and use in accordance with this

[90] Op.cit.
[91] Future of Privacy Forum. Privacy Best Practices for Consumer Genetic Testing Services. Point IV. a. 31 July 2018.
[92] Natasha Chu. Protecting Privacy after Death. 13 Nw. J. Tech. & Intell. Prop. 255. 2015.
[93] https://www.personalgenomes.org/

consent form; or (c) authorize the PGP to obtain and add additional data, such as cause of death and/or tissue samples obtained during an autopsy, to the study on your behalf."[94] Potential participants are strongly encouraged to discuss this and their wishes with their family.

These examples show how different stakeholders in personal health data processing can self-organise around post-mortem digital privacy policies through a direct involvement of data subjects and through delegated management arrangements.

B. The French example of a national legislation merging autonomous and delegated post-mortem privacy management

While some States in the US have adopted specific legal provisions on digital remains and fiduciary property rights management[95] based on the notion of "digital assets", broader protection of non-proprietary digital data is unclear. What about EU Member States, like France? The last version of the French data Protection Act[96] (Loi Informatique et Libertés – LIL) inserts some post-mortem provisions through its Chapter V "Provisions governing the processing of personal data relating to parents of deceased persons". The French law adopts a mixed approach to post-mortem privacy based on a direct pro-active role of living data subjects and complementary provisions enshrined within special laws such as within the biomedical research law[97] and the Public Health Code, or through patrimony regulations. Indeed, French law created a new right for data subjects to write down "anticipated directives" relating to personal data, including personal health data, while the special laws, such as for biomedical research, organise conditions for accessing and processing the personal data and for the mandatory research project's ethical review. In substance, Article 84 of the LIL states that, by principle, data subjects' rights extinguish at the death of the data subject but that they can be provisory maintained where the person indicated her specific wishes by written. Article 48 prescribes that the data subject must be informed by the controller about "his right to define anticipated directives regarding the fate of his personal data after his death, in the conditions fixed under Article 85" of the LIL. The Article 85 informs about the scope of the directives which could concern any type of personal data and could be redacted either generally (for any type of context) or specifically (e.g. for a specific service). Data subjects can freely express their wishes regarding the storage, erasure or communication of the data after their death. These shall be without prejudice to the regulation applied to archiving involving personal data. Wishes expressed within the Directives can prove a given consent or a withdrawal to a processing. They can also provide

[94] Personal Genome Project (2012). Current Consent Form (2020). Available at: https://my.pgp-hms.org/static/PGP_Consent_2015-05-05_online_stamped.pdf

[95] Damian McCallig Blog. Digital remains. Understanding the regulation of your digital life. https://damienmccdli.wordpress.com/digital-remains-laws/ (Accessed on March 2020)

[96] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. As in force in 2020. https://www.cnil.fr/fr/la-loi-informatique-et-libertes

[97] Loi n°2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine (dite *loi Jardé*), as modified by Ordonnance n°2016-800 du 16 juin 2016. Integrated within the French Public Health Code.

general indications that will serve to a representative named as a trusty person in the exercise of the rights afforded under Chapter II of the LIL. Regarding this trusty person, the LIL plans that in case the data subject did not designated such a person, the heirs will be able to have access to the deceased personal data where it is necessary to deal with legacy organisation or implementation, or for closing or updating digital accounts of the deceased persons. In case of disagreements between the heirs in the exercise of the rights, the case shall be brought in front of a competent Court (Tribunal de Grande Instance). Interestingly, Article 85 III of the LIL obliges publicly available online service providers to inform data subjects about their policy regarding personal data processing in case of data subject's death and to allow them to decide about communication of the data towards a third that the data subject would designate (we find here elements related to data portability). By doing so, the LIL keeps access rights for health administration purposes (including health registries) and for processing for research, study and assessments in the field of health, except if the data subject expressly opposed by written during his life (see Article 86 LIL). Bernelin made a thorough analysis[98] of recent state-of-art in French law and jurisprudence regarding post-mortem privacy and highlighted the complexity of the established rules which are inserted within different legal corpus, each having different aims and scope. According to Bernelin, the LIL provisions are covering e-health matters but should not cover personal data processed through healthcare, these being submitted by law to special constraints, in particular regarding storage durations for the purpose of health administration and legal insurance, as proof of health service provision. Therefore, the Public Health Code fixes that health records must be stored 20 years after the last hospitalization of the patient or after the last consultation of the folder. Where the patient dies within the 10 years after his last consultation or hospitalization, the data must be stored for 10 years after his death. Same regarding the personal e-health record, 10 years of storage from the last access from the patient or from the date of his closure by the patient. The Public Health Code plans that a health professional or a legal representative of the deceased can request closure of the e-health record at data subject's death[99]. Same regarding scientific research where the personal data are to be stored as long as necessary for ensuring regulatory procedures for product marketing or validation, and 15 years after the end of the research project[100]. Recent debates for the revision of the French bioethics law[101] inserted several provisions related to post-mortem genetic examination in the medical interest of family members or for scientific research. For clinical purposes[102], this exceptional examination is conditioned by a physician suspicion of a familial genetic anomaly which can trigger a serious but preventable or treatable disease among family members. In the proposed procedure, the physician shall first check whether the deceased person opposed to such examination when

[98] Margo Bernelin. Les données personnelles de santé des défunts: quelle protection ? RGDM n°72. Ed. LEH. P.229-244. September 2019.
[99] Article R.1111-34 French Public Health Code.
[100] Bernelin. Cf. Supra. See also: CNIL Reference Methodologies, MR001, MR003, MR004 on health researches.
[101] Assemblée Nationale. Projet de loi relative à la bioéthique. NOR : SSAX1917211L/Bleue-1, 24 July 2019.
[102] Op.cit. Article 8.

he was alive and, then, check whether family members oppose. Where one family member provides authorization, the test can be practiced. Such procedure does not authorize exhumation of the deceased person's body, it shall only be done on fresh samples procured in the context of an autopsy or on existing biological samples. Testing results will be available to all the family members and where a familial disease is confirmed the physician can appoint the concerned persons for consultation. For research purposes[103], either the deceased samples donor have been informed about the possibility to use the samples in research and expressed her consent or dissent to these activities or the person did not get the information and the researcher is obliged to submit the project to an ethics review performed in France by a Comité de Protection des Personnes (CPP). This latter will check whether an impossibility to contact a legal representative verifies and provide an opinion regarding the ethical and scientific relevance of the research.

From a general point of view, the doctrine suggests that the more time passes the less the data keeps a link with the identity of the person, this calling to envisage a particular regulation in post-mortem privacy going from the protection of data subject's memory and the protection of deceased data subjects' relatives interests to the regulation of the freedom of thirds which could access the data a long time after the initial data subject passed away[104]. The latter could rely on the respect of general principles of law (e.g. respect of human dignity) and of data protection law (e.g. data minimization; proportionality; transparency; security; confidentiality) without relying mandatorily on an individual. In such an approach, as Bernelin suggests, only certain purposes could justify to access to the health data related to a deceased person, in consideration of the public health interest and of related risks for relatives. This approach would favor a shift, along the time, within delegated modes of post-mortem privacy protection, from the one exercised by a natural person acting as a representative designated by the deceased, to a protection based on fundamental principles, on professionals' duties, deontology, and external independent reviews of processing plans. The famous French National Health Data System (SNDS – recently integrated into the Health Data Hub) centralizing the collection of health data nationwide (hospitals databases, social security services and health insurance data, handicap data and data from the registry of medical causes of death) is a good example of data access management based on collegial assessment of the public interest purposes of projects[105].

Conclusion

Post-mortem digital privacy is still looking for proper recognition in hard- and soft-law at International and EU levels. The documents studied are not focusing on such an issue but provides interesting elements for considering post-mortem digital privacy policies in current or future personal sensitive data processing, based on individuals' autonomy or delegations,

[103] Op.cit. Article 18.
[104] Bernelin. Cf. Supra.
[105] Système National des Données de Santé. Finalités Autorisées. https://www.snds.gouv.fr/SNDS/Finalites-autorisees (Accessed on March 2020)

on self-regulatory approach or on specific national regulations, in compliance with health- and research-related regulations' spirit. In personal health data protection, specific ethical tensions with regard to solidarity principle and other fundamental rights and freedoms such as the freedom of speech must be studied. While e-health domain could give raise to very proactive policies for the benefit of data subjects, in health systems, for healthcare and biomedical research, such possibilities seems limited due to other contingencies related to necessities in terms of public interest purposes. Therefore, delegated post-mortem digital privacy management modes are traditionally privileged in these sectors. Further researches are desirable, notably on national ethical and legal sensitivities and on self-regulation actions from data controller or processor acting in digital health in order to eventually show an emerging trend worldwide that could inform policy-makers. The recent practices of digital mourning and commemoration (e.g. digital funeral urns 'iRip'[106]) should question and be monitored if we consider the potential for new business opportunities based on data sciences and technological advances in profiling or digital cloning.

[106] Patricia Hartley. Digital Urns: The Latest Innovation From The Guys Who Brought You The Virtual Cemetery. Connecting Directors. Epub. Funeral Industry News. 27 March 2019.