OSAKA UNIVERSITY LAW REVIEW No. 68 (February 2021) 83-96

The Ethical Use of Artificial Intelligence in Predictive Medicine

Diogo COSTA CUNHA

Elon Musk's announcement about the Neuralink project, which aims to implant a chip with artificial intelligence in the brains of living beings[1], seems to have come out of a science fiction book. At the dawn of the third decade of the twenty-first century, a dystopian future worthy of *1984*[2] could be taking shape ahead of us. Conversely, artificial intelligence could be the disruptive technology that will be the foundation of our way of life in the coming decades, as the advent of the Internet was at the beginning of the millennium.

This is why it is up to the legal standard to take up the questions relating to artificial intelligence and ethics now in order to move towards a peaceful future. Legal science must be the flight plan of artificial intelligence technologies in order to avoid accidents. Moreover, the question of the legal framework of artificial intelligence innovations is all the more relevant when health is at stake.

The use of artificial intelligence technologies in health and medicine is not new. On the contrary, medical science has always evolved in line with discoveries[3]. However, the technical computing power required to implement artificial intelligence and the availability of vast amounts of data nowadays available have enabled this technology to be incorporated into medicine[4]. We are then witnessing the advent of connected health which includes telemedicine[5], e-health[6] and even

---

1) Elon Musk, "An Integrated Brain-Machine Interface Platform with Thousands of Channels," *Journal of Medical Internet Research*, 21(10), (2019): p. 722; Abhinav Kulshreshth, Abhineet Anand, Anupam Lakanpal, "Neuralink – An Elon Musk Start up Achieve symbiosis with Artificial Intelligence," *ICCCIS*, (2019).

2) From the eponymous novel: George Orwell, *1984*, (Secker & Warburg, 1949).

3) Erwin H. Ackerknecht, *A short History of Medicine*, (Jhon Hopkins University Press, 2016).

4) Ray Kurzeil, *The Singularity is Near: When Humans Transcend Biology*, (Penguin, 2006).

5) Distance medicine: as defined by French code of public health: Art. L. 6316-1 *Code de la santé publique*: "Telemedicine is a form of remote medical practice using information and communication technologies".

6) Digital health, defined by the WHO guidelines as "the use of information and communications technology in support of health and health-related fields", WHO Guideline, *Recommendations on digital intervention for health system strengthening*, (2019): p. 1↗

m-health[7]. These forms of connected health are facilitated by the use of artificial intelligence and its accessibility. Furthermore, the use of artificial intelligence and e-health helps in reducing costs and arise care[8], therefore as long as this technology is ethical it will lead health towards performance and efficiency.

The use of artificial intelligence in health is part of a context beyond technology. The relationship between them is also necessarily social and ethical[9]. Indeed, the issue here is the treatment of ill patients and therefore the performance of health and hospital systems. Performance is defined by three objectives: healthcare performance, obviously, but also economic performance and the respect of ethics. Promoting one to the detriment of the other is not efficient[10]. We are therefore trying to find out whether the use of artificial intelligence in medicine allows an increase in care, a reduction in costs, and is not an obstacle in accessing healthcare or in medical confidentiality.

Thus, it appears that the legal normative framework must absolutely allow a balance between these objectives in order to guarantee performance. Artificial intelligence cannot be used to supplement the human relationship between patient and doctor[11]. Nor can it be a means of imposing a medical procedure on the patient[12]. The massive use of data and artificial intelligence are only tools towards health transformation that enhance human intelligence, both individual and collective, in order to enable performance. However, several legal issues come into conflict in the context of artificial intelligence-assisted medicine. Medical law, governing the relations between the patient and the doctor, public health law, governing the interactions between the national power and the population, but also personal data and digital law, dealing with the rights of individuals to control their data.

↘(quoting the Assembly resolution WHA58.28 *in* WHO Resolutions and Decisions, (2005): p. 121).

7) Mobile health, defined by the WHO guidelines as "the use of mobile wireless technologies for public health", WHO Guidelines *ibid.* (quoting the Global Observatory for e-Health, *M-Health: new Horizons for health through mobile technologies*, WHO, Global Observatory for e-Health series, vol. 3, (2011): p. 6).

8) Magali Bouteille-Brigant, "Les enjeux de la *e-santé* au sein de la relation médicale," *Dalloz IP/IT*, 11, (2019): p. 593.

9) *Ibid.*

10) Michaël Krkac, "L'interrogation croissante sur la conciliation entre éthique et performance," *Revue droit & santé*, 95, (2020), p. 488.

11) Magali Bouteille-Brigant, *op. cit.*

12) Michaël Krkac, *op. cit.*

Moreover, this assistance to human intelligence can take place throughout the care process. As a result, this intervention undeniably raises questions of responsibility in the event of errors, whether they be errors of interpretation by the doctor or errors resulting from the medical device. According to the INSERM (French national medical research institute), artificial intelligence is used in many different ways. It can be used in cases of precision medicine and personalised treatment, as a decision-making aid for the doctor and diagnosis aid, in assisted surgery, or even in the use of companion robots[13].

However, only artificial intelligence technologies that are used to prevent the appearance or spread of diseases will be discussed here[14]. This involves predictive medicine for a particular patient, but also prevention in the population. The question of the use of artificial intelligence for preventive or predictive purposes is far thornier because patients, who are not yet ill, are not bonded by a medical contract[15]. It is only a question of preventing the appearance of diseases, as a precautionary measure, and it is essential to know whether or not the legal norm allows the potentially liberticidal use of artificial intelligence in the name of mere precaution.

In this context, the use of artificial intelligence in health must be distinguished in two cases. On the one hand, it can be at the service of an individual, and be used in a predictive role (I), but it can also be at the service of the population in a preventive context (II).

I. The use of artificial intelligence servicing the individual

The focus here is on the relationship between medical law, i.e. the relationship between the doctor – or paramedic – and the patient, and digital and data law. This relationship can be studied through the prism of two interactions. It is then necessary to address the use of artificial intelligence when it aims to prevent diseases (A), but also, when the disease is proven, its evolution (B).

A. *Disease prevention*

The prevention of diseases is first and foremost to be distinguished from assistance in diagnosis. In the latter case, the patient is already suffering from

13) INSERM, *Intelligence artificielle et santé*, (2018): https://www.inserm.fr/information-en-sante/dossiers-information/intelligence-artificielle-et-sante (accessed 27 october 2020).

14) *Ibid.* Which are also defined and mentioned by INSERM.

15) About medical contract and consent between parties: Gérard Mémeteau et al., *Cours de droit médical*, (5th ed., LEH, 2016): §. 540.

symptoms and the doctor can use artificial intelligence, among other means such as consulting a colleague, to help him in establishing a diagnosis. In this case, he must ask the patient for his consent, except in emergencies or special cases[16], in order to be able to rely on a third party, whether human or not[17]. However, here we are talking about people who have no symptoms nor visible signs of illness. Therefore, the use of artificial intelligence by cross-referencing data, personal or not, can anticipate the onset of the disease and detect it beforehand[18]. It must be understood here that this is not a relationship between a patient and a doctor, but between a consumer and a company, which offers its services in order to avoid referral to a doctor.

This detection, this mystical prediction, is made possible by cross-referencing data obtained from the person. This data can come from medical devices[19], but also more widely from all kinds of connected objects[20]. It is not the medical nature of the data that makes this prediction possible, but rather the cross-referencing of multiple data about the person, which may be personal on the one hand, or non-personal on the other.

In Europe, personal data is regulated by the General Data Protection Regulation (GDPR)[21]. Indeed, the regulation lays down the principle that when personal data

16) Article L. 1111-4, *Code de la santé publique*.

17) In the case of a remote expertise ("*télé-expertise"*), where the doctor asks for an expertise from a specialist. This procedure exists in French law since, 2010, and has been since more and more used. Article R. 6316-1 2° *Code de la santé publique*. About consent and conditions, articles R. 6316-2 and R. 6316-3, *Code de la santé publique*.

18) Cédric Villani et al., "Focus 2 – La santé à l'heure de l'IA," *Donner un sens à l'intelligence artificielle*, (2018): p. 196 ; Emily Mullin, "Earlier diagnosis could help researchers to develop drugs to slow the progress of the disease," *MIT Technology Review*, vol. 121, n° 2, (2018).

19) As defined by article 2 (1) of the Regulation (EU) 2017/745 of the European Parliament and the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) n° 178/2002 and Regulation (EC) n° 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, *OJUE*, (2017).

20) Meaning all sorts of IoT. About data collection: Bénédicte Bévière-Boyer, "Données massives en santé : ébauche d'un droit prospectif," in *Innovations en santé publique, des données personnelles aux données massives (big data) : aspects cliniques, juridiques et éthiques*, Christian Hervé and Michèle Stanton-Jean, (ed. Dalloz, 2018): p. 93.

21) Regulation (EU), 2016/679 of the European Parliament and the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), *OJEU*, (2016).

is collected, the consent of the person from whom the data originates is mandatory, not only with respect to the collection but also with respect to its use. The data provider is entitled to know to what extent and for what purposes such data may be used. The condition is, however, that the data must be "personal"[22], i.e. that it allows an individual to be identified. In the context of health data, these are also qualified as "special"[23], which leads to additional measures of precaution for the collector. However, as previously explained, not all data useful for disease prevention is necessarily "special" or sensitive. For example, a connected refrigerator counting the number of times it is opened and recording the hours is not a source of sensitive data. However, these data can be used for detecting cardiovascular diseases or diabetes. Nevertheless, all these data must be personal, as they are linked to an individual and must enable the prevention of his or her illnesses.

Nonetheless, not all the data used are personal, since artificial intelligence in its functioning will necessarily compare these data with scientific data, or at least objective, and non-personal data. Indeed, this predictive analysis made by artificial intelligence must be based on a known reference frame. Very often it will use Big Data[24].

However, in addition to measures enhancing the Big Data, the greatest legal precaution is related to the use of personal data. Indeed, if in the context of a medical device there is no doubt that the person who consents to the collection consents to its medical use. In the context of data collection by ordinary connected objects, consent to medical use is far more difficult to obtain[25]. Moreover, this case presupposes that the data are collected by different companies. Therefore, it seems complicated for the consumer to consent to the collection of data from each collector only in the context of medical use. Data collection contracts are often adhesion contracts[26], and the consumer giving access to his data for medical

22) In the sense of "personal data" defined by article 4 (1) of the GDPR,: "any information relating to an identified or identifiable natural person".

23) See article 9 (1) of the GDPR,: "Processing personal data […] concerning health […] shall be prohibited"; the use of these data on preventive medicine or public health reasons is only an exceptions granted by article 9 (1) (h) and (i).

24) François Bertucci et al., "Santé numérique et « cancer hors les murs », *Big Data* et intelligence artificielle," *Bulletin du Cancer*, Vol. 117, n°. 1, (2020): p. 102.

25) Claude Huriet, "Big Data : tous aliénés ?," in *Innovations en santé publique, des données personnelles aux données massives (big data), op. cit.*, p. 25.

26) Article 6 (1) (b) *GDPR,*; Christiane Féral-Schuhl, *Cyberdroit : le droit à l'épreuve de l'internet*, (ed. Dalloz, 2020): §. 113-31 and following.

purposes frequently has to consent to multiple uses[27]. Moreover, this use by multiple companies is sometimes made outside the user's national borders, which implies additional complications[28].

Imposing data collection in the name of health prevention is impossible. The right to privacy takes precedence over this mere eventuality, all the more so as uses outside the health context will be certain[29]. In addition, in the context of prevention, it is impossible for the owner of the artificial intelligence to objectively prove the effectiveness of the device. Indeed, its recommendations and alerts may have made it possible to prevent and avoid the disease, just as they may have been mistaken about its advent. It is therefore impossible to impose an obligation of result on them.

Using therefore data as a preventive measure is a matter of contract law and relies on the parties' willingness to consent. It is therefore based on a relationship of consent and trust between the parties and must be left to their discretion. It is important to note here that consumers are at first free to decide whether or not to purchase these devices, whether they are medical, paramedical or simply connected objects, and secondly to consent to the collection of their data in their operation. Even if their massive introduction would make it possible to reduce health costs, it is impossible to impose the conclusion of a contract in an arbitrary manner.

B. *Disease surveillance*

Fundamentally, when the patient's illness is declared, it is no longer a question of a contractual relationship, but of medical law governing the juridical relations between the medical practitioner and the patient towards a better medicine[30]. This is why it is no longer a question of contractual freedom, but of a tacit contract of mutual trust between the patient and the doctor[31]. The patient is then a partner in

27) Maïlys Michot-Casbas, Christian Hervé, "Introduction Les données massives en santé : enjeux éthiques des Big Data dans la réaltité pratique du soin," in *Innovations en santé publique, des données personnelles aux données massives (big data), op. cit.*, p. 1.

28) Such as international law enforcement.

29) Such as insurance fraud for instance.

30) Gérard Mémeteau et al., *op. cit.*, §. 41, quoting: Jean Savatier, "Défense et illustration du droit médical," *Archives de philosophie du droit*, (1954-1955): p. 123.

31) Gérard Mémeteau et al., *op. cit.,* §. 541; which is different from a mere consumeristic relationship: Stéphane Prieur, "Retour sur la relation juridique de soins en tant que relation consumériste," in *Mélanges en l'Honneur de Gérard Mémeteau, Droit médical et éthique médicale : regards contemporains,* Bruno Py, François Vialla, Julie Leonhard, vol. 2, (ed. LEH, 2015): p. 73 ff.

the therapeutic decision, but the doctor remains the decision-maker. This relationship of trust is mentioned without being defined in the French Public Health Code in article R. 4127-15, included in the medical code of ethics[32], and in accordance with Hippocrates' oath: "I would never deceive their trust"[33].

Furthermore, article L. 1111-6 of the French Public Health Code mentions the notion of "person of trust", who is entitled, in the absence of the patient's capacity, to take part in the therapeutic relationship. Consequently, if an outside person is to be expressly appointed to this task, it appears that both parties to the tacit contract of mutual trust have an active role in the therapeutic choice.

Therefore, in the context of this contract of mutual trust between the patient and the practitioner, it should be noted that the patient trusts the doctor to administer the best care and to use the best techniques known to science for this purpose. The use of artificial intelligence, in order to predict the evolution of a disease, most often chronic, and to tend towards recovery, could be tacit between the doctor and the patient. However, the doctor has a number of tasks, including informing the patient of the therapeutic method used[34].

In fact, there is a mechanism that allows the doctor to refer to parties outside the contract of mutual trust, to the human intelligence of fellow practitioners, without violating medical confidentiality[35]. Now, if this procedure is possible, if the doctor is given - or even summoned - the opportunity to choose the therapeutic approach outside the relationship that binds him to the patient, it seems logical by analogy that he can do likewise with a technology, a non-human intelligence. Therefore, under the cover of the tacit relationship of trust and the patient's initial authorisation, it can be deduced that the use of artificial intelligence in the therapeutic decision-making process can be understood within the functions of the doctor and can be used. This external aid of artificial intelligence can in particular be used to assist in the choice of drug treatment. For example, in oncology, the genomic profile of an individual can be compared with that of a similar individual to establish an early diagnosis and predict the evolution of his health. His biological profile can be detailed in order to provide him with the most personalised treatment. This is what IBM is now experimenting with the artificial intelligence called Watson, where in 30% of the cases submitted, Watson proposed

32) Conseil National de l'Ordre des Médecins, *Code de déontologie médicale*, (ed. CNOM 2019).

33) *Serment d'Hippocrate*, in : *Code de déontologie médicale, op. cit.*, p. 33.

34) Magali Bouteille-Brigant, *op. cit.*, p. 593.

35) *Supra*, footnote 17, about remote expertise.

more therapeutic options than the doctors[36].

However, the use of personal data in the medical relationship cannot be tacit. This assistance available to the doctor is subject to special provisions. The personal data used must firstly be expressly identified and have the express consent of the patient from whom it originates.

Firstly, the identification of personal data, the practitioner must carefully delimit the information used in this procedure. In fact, an excess of personal information that is useless for the diagnosis is not desirable. The CNIL, the French organisation responsible for data protection and ensuring compliance with the GDPR, warns that only 33% of people are aware of the use of artificial intelligence during their medical procedures[37]. It therefore seems essential to identify the data with the patient.

On the other hand, patients providing data are protected by the GDPR. Even in the context of a medical relationship, consent to the collection and subsequent use of data is essential. In this regard, the regime of data law and patients' rights is similar. Consent is the central element. Except in cases of emergency, or incapacity[38], the patient's consent is indispensable. In the context of data collection and subsequent use of the data it is compulsory[39]. Moreover, in this respect, the doctor is also subject to the requirements of the GDPR[40]. Therefore, in practice, the patient signs a discharge allowing him to consent to care and to the use of artificial intelligence in the context of his therapeutic care. However, the duration of this consent remains unclear.

Furthermore, another point deserves attention, namely that of responsibility in the event of progressive misdiagnosis. In addition to the questions of which doctor or owner of the artificial intelligence is responsible[41], another problem is the question of responsibility in the event of conflicting diagnoses. Indeed, once the doctor has used artificial intelligence, it is legitimate to ask whether or not he

---

36) Morgan Grit, "Algorithmes et intelligence artificielle : les recommandations de la CNIL," *Revue droit & santé*, 82, (2018): p. 245.

37) CNIL, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, (ed. CNIL, 2017): p. 21.

38) Unless represented by a person of trust. Art. L. 1111-6, *Code de la santé publique.*

39) Article 9 (1) (4) (i), *GDPR*.

40) Magali Bouteille-Brigant, *op. cit*.

41) Julia Sourd, "Intelligence artificielle, algorithmes : quelle réglementation pour quelle responsabilité ?," in *E-Santé : les enjeux de la médecine de demain*, Louise Delavenne, Anne-Claire Hubert, (ed. LEH, 2018): p. 61.

should necessarily follow its therapeutic indications. Being the guardian of the therapeutic decision[42], he can freely choose not to follow them. Consequently, in the event of an error, it is difficult to hold him responsible because he did not follow the recommendations of the artificial intelligence, just as it is equally difficult to hold him responsible when he has fully followed the indications resulting from it.

This is why, although artificial intelligence can be an integral part of the doctor's therapeutic arsenal and can be used in a relationship of mutual trust and with the patient's informed consent, it cannot be imposed on the doctor. Artificial intelligence in predictive medicine is a tool supporting the human intelligence of the practitioner, not an obligation incumbent on him, nor a substitute to him.

II. The use of artificial intelligence for collective good

By contrast, the relationship between public health law, the role of the state regarding population health, and digital and data law must be addressed here. Thus, artificial intelligence can be used in a context of anticipating the appearance or management of epidemics (or pandemics) (A), but also in the context of pharmacovigilance (B).

A. Anticipating and managing epidemics

Anticipating epidemics is not easy. Nevertheless, thanks to digital resources, it is now possible to increasingly anticipate any outbreaks on the horizon. The use of artificial intelligence and machine learning algorithms makes it possible to anticipate them. In the context of human flu, for example, it is possible to establish a data panel containing information on seasonal epidemics in order to accurately anticipate risk zones and seasons[43]. However, it is difficult to predict new outbreaks, resulting from unknown factors such as those of Covid-19. However, the data collected during this pandemic could serve as a basis for the prevention of future ones, particularly those obtained in the context of its management.

---

42) Meaning the doctor has a freedom of choice regarding the therapeutic response. Article L. 162-2, *Code de la sécurité sociale*. Defined by authors as the main principle granting the trusting relation and ethics between patient and doctor: Gérard Mémeteau et al., *op. cit.*, §. 325, quoting: Anne Laude et al., *Le droit de la santé*, (PUF-Thémis, 2007): p. 392; and Geneviève Rebecq, *La prescription médicale*, (PUAM, 1998).

43) Jean-Phillippe Gilbert et al., "Un appel à un cadre éthique lors de l'utilisation des données des médias sociaux pour des applications d'intelligence artificielle dans la recherche en santé publique," *Le Relevé des Maladies Transmissibles au Canada*, vol. 46, n° 6, (2020): p. 191.

Notheless, it is important to differentiate between the management of an epidemic and its prediction. Indeed, the more or less urgent nature of management one can legally justify derogations that the prediction cannot.

In the case of epidemics prediction, several types of data will be used: objective, generic and non-personal data on the one hand, but also subjective, precise and personal data on the other. The circulation and use of non-personal data are guaranteed by European Union law[44]. Indeed, aware of the growing data economy, the European single market is also free in the digital environment. The use of such data for predictive purposes is encouraged and facilitated. This includes scientific, statistical and global data. For example, it is possible to mention the different age proportions in a given territory, the proportion of people at risk for this disease - which presupposes that we know the causes and consequences - or the habits of the population[45].

However, these data will be further refined when cross-referenced with personal data in an artificial intelligence algorithm. For example, there are algorithms that can predict the evolution of the human flu according to the research carried out by Internet users[46]. Here again, the collection of data from connected objects makes it possible to predict behaviour, and therefore the outbreak or evolution of an epidemic. In this respect, data collection remains subject to the GDPR, and consent is no longer a medical act but a general personal data collection regime.

However, the doctor himself may be a source of data useful for the prediction of epidemics. Indeed, he can communicate the number of patients received with a particular disease, and then become a data manager subject to the GDPR's sanctions, outside of the relationship that binds him to the patient, if he does not make the data anonymous and does not prove his good diligence in terms of data storage. Therefore, if no overriding interest justifies a derogation from the principle, the collection of data cannot be freely used for the prevention of epidemics.

However, when an epidemic is declared, and when it is a particularly virulent

---

44) Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for free flow of non-personal data in the European Union, *OJEU*, (2018).

45) May be provided by the INSEE (*Institut National de la Statistique et des Études Économiques* – French National institute of statistics) or research organisations on an anonymous basis.

46) Fred S. Lu et al., "Improved state-level influenza nowcasting in the United-States leveraging Internet-based data and network approaches," *Nature Communications*, 10, (2019): art. 147.

pandemic justifying the establishment of a s*ui generis* state of emergency, as happened in France – and across the world – with Covid-19, it is legitimate to ask whether the health emergency does not supplant the standards protecting personal data to the benefit of emergency management. In this respect, it is appropriate to focus on the particular case of tracing applications which emerged during the Covid-19 pandemic, but which were not very successful in France, especially in the context of European free movement[47)].

First of all, it is necessary to understand what the French health state of emergency permits and which are the sources. Contrary to all expectations, the French health state of emergency, established by the Law of 23 March 2020[48)], does not derive from the state of emergency provided by article 16 of the French Constitution[49)]. It also differs from the state of emergency introduced by the Law of 3 April 1955[50)]. It is in fact a *sui generis* regime whose only constitutional legitimacy is a parliamentary ratification consolidated by a decision of the French Constitutional Council[51)], which supports its legitimacy in the light of the "theory of exceptional circumstances"[52)]. It is therefore necessary to be cautious about infringements of personal freedoms, especially since the right to privacy is, on the other hand, enshrined in international texts[53)]. For example, the use of algorithms to track individuals and manage the pandemic, even if it could be ethically justified, cannot be imposed.

---

47) Marianne Long, Léa Paravano, Jean-Luc Sauron, "La protection des données à caractère personnel," *La Semaine juridique Administrations et Collectivités territoriales*, n° 41, (2020): chr. n° 2256, §21.

48) Loi n°2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, *JORF*, 24 March 2020, n° 0072.

49) Stating : "When the institutions of the Republic, the independence of the Nation, the integrity of its territory or the fulfilment of its international commitments are threatened in a serious and immediate manner and the regular functioning of the constitutional public authorities is interrupted, the President of the Republic shall take the measures required by these circumstances", Article 16, *Constitution du 4 octobre 1958*, as modified by Loi constitutionnelle n° 2008-724 du 23 juillet 2008 de modernisation des institutions de la Ve République, *JORF,* 24 July 2008, n° 0171.

50) Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence, as modified by Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, *JORF*, 27 February 2018, n° 0048.

51) Conseil Constitutionnel, Décision n°2020-800 DC du 11 mai 2020.

52) On that point: Didier Truchet, "Avant l'état d'urgence sanitaire : premières questions, premières réponses," *Revue française de droit administratif*, n° 4, (2020): p. 597.

53) While the French Constitutional Council is competent for a constitutional review, it is not qualified for treaty review.

Moreover, a second obstacle stands in front of these tracing applications. Sometimes they are not managed directly by the government - which would not be sufficient for their authorisation - but by private providers, often foreign[54]. In France, however, it was decided that the StopCovid application would not involve GAFAMs. Indeed, the application was based on Bluetooth technology and was able to alert the user who had been in contact with a contaminated third party. A unique identification number is assigned to each device and only this number is transmitted to the *Direction Générale de la Santé* – a Ministry section of the French health Department – so the users' data remains contained on the device[55]. However, this system, although anonymous, processes personal data and is subject to the GDPR[56]. In this sense, a valid legal basis on consent should be discarded, as Article 9 (2) (a) of the GDPR provides that, in the case of processing of data related to health, only explicit consent is possible, as the processing of such data is prohibited in principle[57]. Indeed, even if it is voluntary, the sanitary context does not allow free and informed consent within the meaning of the GDPR[58]. The legal basis chosen was Article 6 (1) and 9 (2) (i) of the Regulation[59]. These articles of the GDPR provide exceptional data treatment in cases of "important public interest ground" or "public interests grounds in the field of health". However, such a basis implies a "proportionate" use. It follows, therefore, that it is impossible to generalise its use.

B. Pharmacovigilance

Another use of artificial intelligence in the context of health prevention

54) As Germany adopted: Caroline Zorn, "État d'urgence pour les données de santé : l'application StopCovid," *Dalloz Actualités*, (12 May 2020). However, this solution would not exclude a control from the national authority, in France it would be the CNIL: Conseil d'État, 10e et 9e Ch. Réun., 19 juin 2020, *Recueil Dalloz*, n°36, (2020): note Fabienne Jault-Seseke, p. 2043.

55) Décret n° 2020-650 du 29 mai 2020 relatif au traitement des données dénommé « StopCovid », *JORF*, 30 May 2020, n° 0131, article 2.

56) Alexandra Bensamoun, Nathalie Martial-Braz, "Covid-19 (déconfinement) : avis de la CNIL sur l'application StopCovid," *Recueil Dalloz*, n°17, (2020): p. 934.

57) Ludovic Pailler, "StopCovid : la santé publique au prix de nos libertés ?," *Recueil Dalloz*, n° 17, (2020): p. 935. Here, moreover, the author raises the question of Article 17 (1) (b) of the GDPR, which would require immediate deletion of the data as soon as consent is withdrawn by the user.

58) Alexandra Bensamoun, Nathalie Martial-Braz, *op. cit.*; Ludovic Pailler, *op. cit.*

59) Article 1, Décret n°2020-650.

concerns pharmacovigilance. The ANSM (*Agence Nationale de la Sécurité du Médicament et des Produits de Santé* - French Agency for Drug Safety), defines pharmacovigilance as the monitoring of drugs and the prevention of risks of undesirable effects resulting from their use[60]. The pharmacovigilance mission therefore consists of monitoring the side effects of medicines, depending on their design or use. The French Public Health Code expressly distinguishes between two types of pharmacovigilance needing data management, i.e. blood-derived medicines which must be traceable to their donor[61], and pharmaco-dependency, or addict-vigilance, which requires data to be collected on patients' drug habits[62]. In both cases, the use of artificial intelligence algorithms allows better analysis.

Nevertheless, in both cases, there are overlapping legal norms which do not facilitate the implementation of artificial intelligence. On the one hand, medical law provides for an obligation of confidentiality, and therefore the doctor cannot freely transmit the data collected for pharmacovigilance purposes. On the other hand, personal data law provides for the protection of sensitive data.

From a medical law approach, it should be noted that the doctor also has a duty to report any adverse effects due to a medicinal product[63]. However, in this context, a first contradiction appears within the field of medical law, on the one hand medical confidentiality is imposed, on the other hand there is an obligation to report. However, this contradictory duality can be supplemented by admitting that there is a possibility of shared secrecy between the practitioner, the patient and the pharmacovigilance organisation[64]. This shared secrecy nevertheless requires the patient's consent.

In parallel, when applied to the digital and algorithmic world, the informed consent described by the GDPR in Article 9 (2) (a) for health data is indispensable. Unless it is based, as in the case of tracking applications, on "important public interest grounds"[65] or "public interest grounds in the field of health"[66]. This second basis does require proportionate use, and in the context of pharmacovigilance it is easier to establish. Then, data management in this context could technically be

60) ANSM website, in : https://ansm.sante.fr/Declarer-un-effet-indesirable/Pharmacovigilance/Organisation-de-la-pharmacovigilance-nationale/(offset)/0 (accessed on 31 October 2020).

61) Article R. 5121-13, *Code de la santé publique.*

62) Articles R. 5131-112 and R. 5131-113, *Code de la santé publique.*

63) Article R. 5121-161, *Code de la santé publique.*

64) Mathieu Guerriaud, Sylvette Huichard, "La déclaration de pharmacovigilance à l'épreuve du secret professionnel," *Panorama de droit pharmaceutique*, n°1, (2014): p. 239.

65) Article 6 (1) (e), *GDPR*.

66) Article 9 (2) (i), *GDPR*.

included as a part of the confidentiality obligation binding on the doctor and be treated as a whole.

This is why the use of artificial intelligence algorithms in the context of pharmacovigilance can be made possible and more effective from a data processing point of view, but effective mass processing cannot take place without a reform aimed at reconciling the different obligations of the practitioner.

In summary, the use of artificial intelligence in predictive medicine, whether personal or collective, is not favoured by the data protection regime, particularly with regard to health data. For all that, although these measures and the use of artificial intelligence technologies would allow better management of diseases and increase healthy living, the risks involved do not allow the protective foundations of privacy to be jeopardised. In the absence of more secure technology, and in application of the precautionary principle, it is not possible to fully open up health to artificial intelligence. Perhaps, however, if forthcoming technological inventions, such as quantum computing, for example, make it possible to secure data with a certain degree of security, then it will be possible to relax the legal standard in favour of the widespread use of artificial intelligence in medicine.