

# TECHETHOS

FUTURE ○ TECHNOLOGY ○ ETHICS

## Annex 9.7 National legal case study: Digital extended reality in France

D4.2 Comparative analysis of national legal case  
studies December 2022

Draft version submitted to the European Commission for review



AUSTRIAN INSTITUTE  
OF TECHNOLOGY



ASSOCIAZIONE  
ITALIANA  
PER LA RICERCA  
INDUSTRIALE



All European  
Academies



TechEthos receives funding from the EU H2020 research and innovation programme under Grant Agreement No 101006249. This deliverable and its contents reflect only the authors' view. The Research Executive Agency and the European Commission are not responsible for any use that may be made of the information contained herein.

## D4.2 National legal case studies: Annex 9.7 Digital extended reality in France

Work Package	WP4 Policy, legal and regulatory analysis		
Work Package lead	Trilateral Research (TRI)		
Partner name	CEA		
Lead Author(s)	Laurynas Adomaitis (CEA), Alexei Grinbaum (CEA)		
Other contributors	Julie Vinders (TRI), Ben Howkins (TRI)		
Date published	23/12/2022		
Version number	1.0	Status	Final

## Version control

Version	Date	Description
0.1	07/09/2022	Outline
0.2	28/09/2022	First draft
0.3	02/11/2022	Draft for inclusion in D4.2 and QA
1.0	23/12/2022	D4.2 final version

## Keywords

France, Legal framework, Extended reality, Natural language processing



## The TechEthos Project

TechEthos is an EU-funded project that deals with the ethics of the new and emerging technologies anticipated to have high socio-economic impact. The project involves ten scientific partners and six science engagement organisations and runs from January 2021 to the end of 2023.

TechEthos aims to facilitate “ethics by design”, namely, to bring ethical and societal values into the design and development of new and emerging technologies from the very beginning of the process. The project will produce operational ethics guidelines for three technologies for users such as researchers, research ethics committees and policy makers. To reconcile the needs of research and innovation and the concerns of society, the project will explore the awareness, acceptance and aspirations of academia, industry and the general public alike and reflect them in the guidelines.

TechEthos receives funding from the EU H2020 research and innovation programme under Grant Agreement No 101006249. This deliverable and its contents reflect only the authors' view. The Research Executive Agency and the European Commission are not responsible for any use that may be made of the information contained herein.

# Table of contents

<b>1. Introduction .....</b>	<b>6</b>
1.1 Purpose of the French legal case study .....	6
1.2 Scope and Limitations .....	7
1.3 Overview of the French legal system .....	7
1.4 Current state of XR in France .....	8
<b>2. XR-specific legal developments .....</b>	<b>9</b>
<b>3. Domain-specific legal issues .....</b>	<b>11</b>
3.1 Human rights law .....	11
3.1.1 Dignity .....	11
3.1.2 Bias and Fairness .....	11
3.1.3 Protection of vulnerable Persons .....	12
3.1.4 Autonomy .....	12
3.2 Privacy and data protection law .....	13
3.2.1 Consent .....	13
3.2.2 Profiling .....	13
3.2.3 Mental data .....	14
3.3 Consumer rights law .....	14
3.3.1 Virtual assets .....	14
3.4 Liability for harms .....	15
3.4.1 Liability for harms under tort law .....	15
3.4.2 Liability for harms criminal law .....	15
<b>4. Overview of gaps and challenges .....</b>	<b>16</b>
<b>5. Conclusion .....</b>	<b>17</b>
<b>6. References .....</b>	<b>18</b>

## List of tables

Table 1: List of Definitions .....	4
Table 2: List of Abbreviations.....	4
Table 3: Overview of nine national legal case studies (TechEthos WP4) .....	7

## Definitions and abbreviations

Table 1: List of Definitions

Term	Explanation
Digital Extended Reality	AI-powered digital technologies (hardware and software) capable of perceiving and processing human sensorial outputs, e.g., voice, gestures, language, movement, emotions, and other elements of human communication), allowing extended or mixed virtual scenarios (e.g., visual, audio, linguistic or haptic) to be tailor-made or “customized” based on the user interest and behaviour (and thus profile, model, predict, discriminate, and influence the user’s behaviour or nudge their choices).

Table 2: List of Main Abbreviations

Term	Explanation
CERNA	Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene
CNIL	Commission nationale de l’informatique et des libertés
DoA	Description of Action
GDPR	General Data Protection Regulation
PC	Project Coordinator
WP	Work Package
XR	Digital Extended Reality

# Abstract

The objective of this study is to review the current state of the law and legal responses on digital extended reality (XR) in France, as evidenced in policy, legislation, case law and regulation. It focuses on those issues affecting and/or contributing fundamental human rights and freedoms, socio-economic inequalities, and stimulation of innovation. This study also looks at developments in XR that may influence constitutional or human rights, and proposals to create or adapt existing law in response to those XR developments.

A summary overview of the main findings and legal issues surrounding XR in France is provided in section 5.1.1 of the TechEthos D4.2 Comparative analysis of national legal case studies. This report is primarily aimed at informing the French government and French policy makers regarding the regulatory challenges of XR in France. Furthermore, it provides further background to readers to the specific French context of the main points and key regulatory challenges identified in the comparative analysis to which this report is annexed.



# 1. Introduction

Digital extended reality (XR) presents many significant legal issues that impact socio-economic equality and fundamental rights in France. This study provides an overview of those legal issues and challenges.

This study analyses relevant laws and policies from the French legal system in relation to XR. For the purpose of the TechEthos project and this national legal case study, we have used the following definition for XR:

- **Digital Extended Reality (XR)** refers to AI-powered digital technologies (hardware and software) capable of perceiving and processing human sensorial outputs, e.g., voice, gestures, language, movement, emotions, and other elements of human communication), allowing extended or mixed virtual scenarios (e.g., visual, audio, linguistic or haptic) to be tailor-made or “customized” based on the user interest and behaviour (and thus profile, model, predict, discriminate, and influence the user’s behaviour or nudge their choices)<sup>1</sup>

For more information about the TechEthos technology families and their innovation ecosystems, visit: <https://www.techethos.eu/resources/>.

This **introduction** sets out the purpose of the French legal case study, and describes the scope and limitations of the study, before providing a high-level overview of the French legal system and current state of XR in France. **Section II** explores the existing and proposed laws and policies that specifically address XR. **Section III** explores the legal implications of XR in relation to specific legal domains, including human rights law, privacy and data protection, use in legal systems, and liability for harms. **Section IV** provides an overview of the gaps and challenges in relation to the regulation of XR. **Section V** concludes the case study followed by a reference list at the end.

## 1.1 Purpose of the French legal case study

The objective of this study is to review the current state of the law and legal responses on XR in France, as evidenced in policy, legislation, case law and regulation. We prepared this study through desk research, using legal research and academic databases such as Google Scholar and consultation with legal experts.

There are currently no XR-specific laws or policies in country France. However, existing law and regulations (e.g., privacy laws) may and should cover these technologies, including any harms resulting from them. Legal academic discourses in country have focused on digital sovereignty, consent, fraud, algorithmic bias, profiling, protection of vulnerable individuals, and the regulation of digital assets.

This study is part of a series of national legal case studies prepared in the TechEthos project covering three technology families: climate engineering, neurotechnologies, and XR. A complementary report

---

<sup>1</sup> Buchinger E., Kinegger M., Zahradnik G., Bernstein M.J., Porcari A., Gonzalez G., Pimponi D., Buceti G. (2022). In short: Digital Extended Reality. TechEthos Project Factsheet based on TechEthos technology portfolio: Assessment and final selection of economically and ethically high impact technologies, Deliverable 1.2 to the European Commission. Available at: [www.techethos.eu](http://www.techethos.eu).

covers the international and European Union law dimensions of the three technology families. The following table provides an overview of the nine country studies conducted as part of the *Comparative analysis of national legal case studies* (D4.2 of the TechEthos project):

Table 3: Overview of nine national legal case studies (TechEthos WP4)

Climate Engineering	Neurotechnologies	Digital Extended Reality
Australia	Germany	France
Austria	Ireland	Italy
United Kingdom	United States	United Kingdom

## 1.2 Scope and Limitations

This study was prepared as part of the TechEthos project's work package on policy, legal and regulatory analysis. Therefore, the scope is demarcated by that project task's workplan. The legal issues related to XR are too vast to be covered comprehensively in a study of this size. Instead, this study focuses on a limited range of topics with significant human rights and socio-economic impacts that are of high policy relevance, particularly in the European context.

## 1.3 Overview of the French legal system

The French legal system is based on the civil law tradition. The French Constitution, which was established in 1958, is the supreme source of law.<sup>2</sup> The Constitution establishes the framework for the three branches of government: the executive, the legislative and the judicial.

The executive branch is headed by the President of the Republic, who is elected by universal suffrage for a five-year term. The President appoints the Prime Minister, who leads the government. The government is responsible for proposing and implementing laws.

The legislative branch is composed of the National Assembly and the Senate. The National Assembly is the lower house and is composed of 577 deputies, who are elected by universal suffrage for a five-year term. The Senate is the upper house and is composed of 348 senators, who are elected by indirect suffrage for a six-year term. The Senate's role is consultative.

The judicial branch is composed of the Constitutional Council, the Supreme Court, the Court of Cassation and the Council of State. The Constitutional Council is responsible for ensuring that laws are in line with the Constitution. The Supreme Court is the highest court for civil and criminal matters. The Court of Cassation is the highest court for matters of public law. The Council of State is the highest administrative court.

The Commission nationale de l'informatique et des libertés (CNIL) is a French data protection authority created in 1978 by the Data Protection Act (Loi Informatique et Libertés). It is responsible for ensuring

<sup>2</sup> Constitution Du 4 Octobre 1958, 4 October 1958.



that data processing complies with the French data protection law. The Data Protection Act was passed in 1978 in response to concerns about the potential for abuse of personal data.<sup>3</sup> The law requires that personal data must be collected and processed fairly and transparently, and only for specified, explicit and legitimate purposes. Personal data must be accurate and up to date, and must be kept for no longer than is necessary for the purposes for which it is processed. Individuals have the right to access their personal data and to request that it be corrected if it is inaccurate.

The CNIL is responsible for enforcing the Data Protection Act as well as the General Data Protection Regulation (GDPR) and has a range of powers to do so, including the power to issue warnings, orders and fines. It also has the power to carry out investigations and audits, and to order the suspension or deletion of data processing operations that do not comply with the law.

The French Data Protection Act was one of the first data protection laws in the world, and the CNIL is one of the oldest data protection authorities. It has played a leading role in the development of data protection law and practice in France and internationally.

Within the DTI (Directorate of Technology and Innovation) of CNIL, LINC (CNIL's Digital Innovation Laboratory) participates in debates linking ethics, freedoms, data and digital uses.

One of the focus areas of the LINC laboratory is the concept of a metaverse. A member of LINC has published an article, outlining ethical and potential legal issues within virtual and augmented reality.<sup>4</sup>

Another area in which LINC has produced a research dossier is on vocal assistants.<sup>5</sup> Although these efforts do not constitute any legal measure currently, they may influence future policy action.

## 1.4 Current state of XR in France

At the time of writing, “The Sandbox” is the dominating metaverse space in France. Several well-known companies and brands own land on the metaverse and operate there, including Groupe Carrefour, Groupe Casino, AXA Assurances, Ubisoft, and Groupe Havas.<sup>6</sup> In 2022, Meta and Simphon have launched a coding academy dedicated to the Meta’s metaverse in France.<sup>7</sup>

<sup>3</sup> Loi N° 78-17 Du 6 Janvier 1978 Relative à l’informatique, Aux Fichiers et Aux Libertés, 6 January 1978.

<sup>4</sup> R. Chatellier, *Métavers : réalités virtuelles ou collectes augmentées ?*, 5 November 2021, available at <https://linc.cnil.fr/fr/metavers-realites-virtuelles-ou-collectes-augmentees> (last visited 28 October 2022); *Métavers : ce jeu dont qui sera le héros ?* / CNIL, 2022, available at <https://www.cnil.fr/fr/metavers-ce-jeu-dont-qui-sera-le-heros> (last visited 16 March 2022).

<sup>5</sup> LINC, *[dossier] Assistants vocaux*, juin 2018, available at <https://linc.cnil.fr/fr/dossier-assistants-vocaux> (last visited 28 October 2022).

<sup>6</sup> F. David, *Metaverse français : les principaux metaverses en France*, 24 May 2022, BeinCrypto France, available at <https://fr.beincrypto.com/apprendre/metaverse-francais-les-principaux-metaverses-en-france/> (last visited 24 October 2022).

<sup>7</sup> C. Simon, *Meta lance une ‘académie du métavers’ en France à la rentrée 2022*, 12 June 2022, L’Express.fr, available at [https://www.lexpress.fr/actualites/1/societe/meta-lance-une-academie-du-metavers-en-france-a-la-rentree-2022\\_2175065.html](https://www.lexpress.fr/actualites/1/societe/meta-lance-une-academie-du-metavers-en-france-a-la-rentree-2022_2175065.html) (last visited 24 October 2022).



## 2. XR-specific legal developments

This section presents an overview of the legal developments pertaining to XR technologies in France. It examines relevant policies and laws in relation to XR and identifies the national authorities involved in the implementation and enforcement of such laws and policies.

### Current debates and future policy and/or legal developments

France's Digital Republic Act has been adopted in 7 October 2016 and mentions the creation of a Commission for Digital Sovereignty.<sup>8</sup> Its aim was supposed to be to investigate how national sovereignty can be understood in the globalized digital arena and create tools that enhance France's digital sovereignty, like developing an independent operating system. A French Senate report on the issue was published in 2019.<sup>9</sup> However, this proposal has not transitioned into concrete legislation and this idea was eventually abandoned.

Ethical and legal research efforts have also been dedicated to exploring the idea of digital sovereignty. Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene (CERNA) – an ethics and policy research consortium - has published a report that addresses how sovereignty, as a pivotal and defining notion of the relationship of legitimate authority between human beings under the rule of law, is affected by the rapid and global technological change. To enhance the digital sovereignty of France, the CERNA report recommends enhancing access to data for scientific purposes, providing ethical and privacy-oriented training, and strongly supporting open access research.<sup>10</sup>

France currently supports European Commission's initiatives to increase protection for journalists and freedom of expression online (the European Democracy Action Plan) and to require greater accountability from digital service providers (the Digital Services Act).<sup>11</sup>

The biggest foundational legal debate in France concerns the identity associated with an avatar. In a mission letter dated February 14, 2022, the Minister of Economy, the Minister of Culture and the Secretary of State for Digital Transition and Electronic Communications requested the establishment of an exploratory mission on the development of a metaverse. Camille François, researcher at Columbia University, Adrien Basdevant, lawyer at the Paris Bar, and Rémi Ronfard, researcher at Inria have published a report in October 2022, which focuses on the issue of identity, among others.<sup>12</sup>

Currently, the users of the metaverse can use a pseudonym and an avatar, which raises questions of identity verification and traceability of actions. How to trace the identity of people in the Metaverse in case of illicit activity? How to verify that a person is who they claim to be? How to avoid fraud and

<sup>8</sup> LOI N° 2016-1321 Du 7 Octobre 2016 Pour Une République Numérique (1), 2016-1321, 7 October 2016.

<sup>9</sup> G. Longuet, *Le Devoir de Souveraineté Numérique*, n° 7 tome (2019).

<sup>10</sup> 'Cerna (Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene', in 2018. *Research Ethics in Machine Learning*.

<sup>11</sup> European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, 2020.

<sup>12</sup> A. Basdevant, C. François and R. Ronfard, *Mission Exploratoire Sur Les Métavers* (2022).



identity theft with the use of avatars in a metaverse? Will an identity necessarily have to be associated with an avatar? How will we move from one metaverse to another? Will it be possible to explore a metaverse anonymously? How can we reconcile the desire for anonymity with the accountability of actions in a metaverse?

These questions can further be enhanced by the discussion of artificial or digital subjects that may produce actions and language autonomously, without a human-machine distinction. Thus, in addition to human anonymity, there is a question of avatar humanity in the first place – is there anyone behind an avatar? There are proposals to solve this issue by introducing watermarking or other techniques to enforce the human-machine distinction.<sup>13</sup>

In the report, some initial suggestions are made regarding the usage of identifying techniques to identify avatars and ensure the link between digital and material identity. For example, there are suggestions to use European Digital Identity Wallet and to apply eIDAS regulation.<sup>14</sup>

---

<sup>13</sup> A. Grinbaum and L. Adomaitis, The Ethical Need for Watermarks in Machine-Generated Language, arXiv:2209.03118, 7 September 2022.

<sup>14</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L, vol. 257, 23 July 2014.

## 3. Domain-specific legal issues

This section examines the legal implications of XR in a France context with respect to specific legal domains with a high socio-economic impact. The legal domains covered include human rights law, privacy and data protection law, use in legal systems (criminal, civil and evidence law), and liability for harms (tort, contract and criminal).

### 3.1 Human rights law

#### 3.1.1 Dignity

Article 52 (3) of the proposed AI Act claims that the manufacturer of an AI system “that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful (‘deep fake’), shall disclose that the content has been artificially generated or manipulated.”<sup>15</sup> Failure to do so would be punishable by fine (Article 71).

XR avatars can usually be distinguished into two categories. One is a picture, aggregated from a database of images by using Generative Adversarial Networks (GANs)<sup>16</sup>, but not resembling any subject in particular. The other category is an imitation of a single individual by using multiple images of them, like “the digital Einstein”<sup>17</sup> or Meta’s avatars that are designed based on visual appearance. The latter could be subject to the regulation; however the acceptable degree of resemblance needs to be established.

#### 3.1.2 Bias and Fairness

In 2017, the Defender of Rights and CNIL focused on the risks of discrimination that can result from algorithmic biases.<sup>18</sup> A debate is also underway at the European level with a goal to adapt a regulatory framework to mitigate such risks.<sup>19</sup> In 2020, the Council of Europe recommended that developers, manufacturers, and service providers should avoid any potential bias, including unintentional or hidden bias, as well as the risks of discrimination in the new Convention 108 guidelines.<sup>20</sup> In the resolution of February 2021, the European Parliament claimed that “outputs should be reviewed in order to avoid all forms of stereotypes, discrimination and biases, and where appropriate, make use of AI to identify and

<sup>15</sup> European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, 2021.

<sup>16</sup> Creswell et al., ‘Generative Adversarial Networks: An Overview’, 35 *IEEE Signal Processing Magazine* (2018) 53.

<sup>17</sup> <https://digitalhumans.com/digital-einstein/>

<sup>18</sup> Demiaux and Si Abdallah, ‘How Can Humans Keep the Upper Hand’, *Report on the Ethical Matters Raised by Algorithms and Artificial Intelligence. Paris: Commission Nationale Informatique et Libertés* (2017).

<sup>19</sup> European Commission, *supra* note 15.

<sup>20</sup> Council of Europe, Convention 108 + Convention for the Protection of Individuals with Regard to the Processing of Personal Data.



correct human biases where they might exist.”<sup>21</sup> The proposed European Artificial Intelligence Regulation (proposed AI Act), published by the European Commission on April 21, 2021, names measures to limit discriminatory biases and employs the notion of human oversight as the key to fighting them.<sup>22</sup>

Chatbots are used by human resources managers for recruitment as well as for career follow-up and employee training. Legal regulations are starting to be applied to implementations in human resources. Article 6 of the proposed AI Act and its Annex III consider recruitment systems to be high-risk by claiming “AI systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk.”<sup>23</sup> Therefore, legal compliance is mandatory *ex ante*, including risk management processes, monitoring, bias detection and correction, technical documentation, event logs, user consent, human oversight, robustness, security, accuracy, and proportionality.

### 3.1.3 Protection of vulnerable Persons

Article 5 of the proposed AI Act prohibits the use of any artificial intelligence system that exploits the vulnerability of a group of individuals to influence the behaviour of any of these individuals and cause harm to them. In June 2021, CNIL has published recommendations for the protection of minors online.<sup>24</sup> These recommendations related to the “online” life of minors can pave the way for consultation with the stakeholders, in order to make them technically operational and propose practical advice and adapted educational resources. France’s civil law limits the type of consent that minors under the age of 18 can give. For example, this precludes them from owning or buying digital assets.<sup>25</sup>

### 3.1.4 Autonomy

The European Union law is moving to include measures to regulate manipulation by digital systems. Article 5 of the proposed AI Act prohibits the placing on the market, putting into service or use of an AI system that implements subliminal techniques beyond a person’s consciousness in order to materially distort a person’s behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm. The same section prohibits artificial intelligence systems that exploit any of the vulnerabilities of a specific group of persons in order to influence their behaviour and cause harm to them. Article 71 of the text defines the penalties for disregarding these prohibitions. In addition, a person who has suffered harm may seek financial compensation. Moreover, the Council of Europe has called for “open-ended, informed and inclusive public debates with a view to providing guidance on where to draw the line between forms of permissible persuasion and unacceptable manipulation.”<sup>26</sup>

<sup>21</sup> European Parliament Resolution of 19 May 2021 on Artificial Intelligence in Education, Culture and the Audiovisual Sector (2020/2017(INI)), 2021.

<sup>22</sup> European Commission, *supra* note 15.

<sup>23</sup> *Ibid.*

<sup>24</sup> <https://www.cnil.fr/fr/la-cnil-publie-8-recommandations-pour-renforcer-la-protection-des-mineurs-en-ligne>

<sup>25</sup> LOI N° 2019-486 Du 22 Mai 2019 Relative à La Croissance et La Transformation Des Entreprises (1), 2019-486, mai 2019.

<sup>26</sup> Council of Europe, Draft Declaration of the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes, 13 February 2019.



## 3.2 Privacy and data protection law

### 3.2.1 Consent

The issue of personal data protection has become crucial with the development of digital technology, the explosion of data processing, and the offering of free services in return for the use of data. The protection from the collection of personal data was considered to be part of privacy as early as the law of January 6, 1978, known as the Data Protection Act in France.<sup>27</sup> The European Union has begun regulating it in 2002 with regard to communication technologies.<sup>28</sup> It is now governed by the European regulation of April 27, 2016, known as the GDPR, especially its chapters II and III, that constitute a set of protective rights for the individual.<sup>29</sup>

The control of personal data protection falls under a national regulator, the CNIL in France, which monitors compliance with the GDPR and the French Data Protection Act, mostly by issuing opinions and formal notices and by applying sanctions under the oversight of the Council of State.<sup>30</sup> Although the national judge and the Court of Justice of the European Union are progressively developing case law on data protection, like the case of *Google v. Cnil*,<sup>31</sup> there are questions on the quality of consent, its meaning, and the conditions under which it is collected (legibility, clarity, and precision of clauses).<sup>32</sup> These tensions between the law and the actual collection of data, which stimulates the current reflections in this area.

### 3.2.2 Profiling

Article 4 of the GDPR defines profiling as any form of automated processing of personal data that consists of using that data to evaluate certain aspects of an individual, including analysing or predicting issues related to work performance, economic situation, behaviour, etc. Decisions resulting from profiling are governed by Article 47 of the French Data Protection Act<sup>33</sup> and Article 22 of the GDPR, as long as they are likely to have an effect on the individual. According to Article 22 of the GDPR, “the data

<sup>27</sup> Loi N° 78-17 Du 6 Janvier 1978 Relative à l’informatique, Aux Fichiers et Aux Libertés, 6 January 1978, *supra* note 3.

<sup>28</sup> 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), OJ L, vol. 201, 12 July 2002.

<sup>29</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance), OJ L, vol. 119, 27 April 2016.

<sup>30</sup> *Ibid.*

<sup>31</sup> Bougiakiotis, 'One Law to Rule Them All? The Reach of EU Data Protection Law after the Google v CNIL Case', 42 *Computer Law & Security Review* (2021) 105580; Zalnieriute, 'Google LLC v. Commission Nationale de l’informatique et Des Libertés (CNIL)', 114 *American Journal of International Law* (2020) 261; ECJ, *Google LLC, Successor in Law to Google Inc v Commission Nationale de l’informatique et Des Libertés (CNIL)*, Case C-507/17, 24 September 2019, available at <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507> (last visited 25 October 2022).

<sup>32</sup> Gray et al., 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective', in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021) 1; Papadogiannakis et al., 'User Tracking in the Post-Cookie Era: How Websites Bypass GDPR Consent to Track Users', in *Proceedings of the Web Conference 2021* (2021) 2130.

<sup>33</sup> Loi N° 78-17 Du 6 Janvier 1978 Relative à l’informatique, Aux Fichiers et Aux Libertés, 6 January 1978, *supra* note 3.

subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”<sup>34</sup> Furthermore, under Articles 13– 2 f) and 14– 2 g) of the GDPR, individuals who are subject to a fully automated decision must be informed, at the time of collection of their data and at any other time about “the existence of automated decision-making [and] meaningful information about the logic involved” (Article 15).<sup>35</sup>

### 3.2.3 Mental data

In their report to the French ministries and secretaries of state of Economy and Culture, Basdevant, François, and Ronfard note that immersive technologies are extremely invasive in terms of acquiring personal data.<sup>36</sup> The tracking of eye-movement, facial expressions, inflections, voice textures, etc. can all be used in the analysis and prediction of behaviour and emotions. The report states that building a metaverse presents the challenge of preserving our mental space and data that until now has been less prominent, but which will undoubtedly be highly coveted and valued.

The researchers claim that existing French and European regulation “do not address the issues of mental integrity, mental self-determination and cognitive freedom. The debate is therefore not only about the protection of personal data, but more globally about defending fundamental rights.”<sup>37</sup> like the right to “physical and mental integrity”, as expressed in the Charter of Fundamental Rights of the European Union.<sup>38</sup>

## 3.3 Consumer rights law

### 3.3.1 Virtual assets

Much of the economic trade in metaverse is facilitated by Non-Fungible Tokens (NFTs), which is only a digital token giving access to the file saved in the blockchain. The NFT is therefore not the work itself. Basdevant, François, and Ronfard emphasize that the question of the regulation of virtual markets has mainly to do with the question of the taxation – how can digital assets on a blockchain be taxed and enforced.<sup>39</sup> Currently, the Article 150 VH bis of the French General Tax Code provides that the transfer exchange of digital assets for other digital assets by individuals is not taxable.<sup>40</sup> Whether or not NFTs will be included in the definition of digital assets will have major consequences for the economy of a metaverse, particularly in terms of taxation. The debates at the European level in reviewing MiCA (Markets in Crypto-assets) will have impact on how the taxation of NFTs is understood in France.<sup>41</sup>

<sup>34</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance), OJ L, vol. 119, 27 April 2016, *supra* note 29.

<sup>35</sup> *Ibid.*

<sup>36</sup> Basdevant, François and Ronfard, *supra* note 12.

<sup>37</sup> *Ibid.*

<sup>38</sup> Charter of Fundamental Rights of the European Union, OJ C, vol. 326, 26 October 2012.

<sup>39</sup> Basdevant, François and Ronfard, *supra* note 12.

<sup>40</sup> Article 150 VH Bis - Code Général Des Impôts, 24 May 2019.

<sup>41</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-Assets, and Amending Directive (EU) 2019/1937, 2020.





## 3.4 Liability for harms

### 3.4.1 Liability for harms under tort law

The legal problem of Artificial Intelligence (AI) spreading lies and misinformation concerns the responsibility of the manufacturer of a conversational agent, and not the conversational agent itself, since AI does not constitute a legal person. The legal texts on this subject are quite limited because they essentially relate to the formation of the contract. Article 1104 of the Civil Code imposes a requirement of good faith in contractual relations.<sup>42</sup> Article 1112 (1) provides an obligation to disclose information to the party who knows information which is decisive for the consent of the other party, when the latter is unaware of this information or trusts his co-contractor.<sup>43</sup> Moreover, for consent to be informed, it must not be obtained by fraud, on pain of rendering the contract void. Article 1137 provides that fraud (dol) "is the fact that a contracting party obtains the consent of the other party through manœuvres or lies. Fraud (dol) also results from an intentional concealment of information by one of the contracting parties which it knows is decisive for the other party."<sup>44</sup> Moreover, unfair commercial practices aiming at deceiving the consumer are prohibited by the Consumer Code.<sup>45</sup> The abuse of weakness is sanctioned by the criminal code.<sup>46</sup>

### 3.4.2 Liability for harms criminal law

Some illegal acts, such as prostitution, incest, torture, pedophilia or murder are sensitive themes in virtual worlds. Thus, the question of law and the digital body cannot be ignored by public authorities. Knowledge exchange among institutions will be necessary to tackle them. Some researchers in France suggest that the National Agency for Information Systems Security (ANSSI) could be the first point of contact in ensuring safety in a metaverse.<sup>47</sup> They also suggest that "France must invest in a major [forensic toolkit]. We therefore recommend creating a "French Chainalysis" to limit our technological and economic dependencies."<sup>48</sup>

A competing image of justice in a metaverse is described in a novel "Snow Crash", where justice is served by "burbclaves" that Neal Stephenson describes as "Franchise-Organized Quasi-National Entities". Each of these "burbclaves" makes its own rules, acting as a "city-state with its own constitution, a border, laws, cops, everything."<sup>49</sup> Meta has created a similar entity in November 2018 after Mark Zuckerberg met with Harvard Law School professor Noah Feldman, who had proposed the creation of a quasi-

<sup>42</sup> Article 1104 - Code Civil, 1 October 2016.

<sup>43</sup> Article 1112-1 - Code Civil, 1 October 2016.

<sup>44</sup> Article 1137 - Code Civil, 1 October 2018.

<sup>45</sup> Article L120-1 - Code de La Consommation, L120-1, 2008.

<sup>46</sup> Article 223-15-2 - Code Pénal, 14 May 2009.

<sup>47</sup> Basdevant, François and Ronfard, *supra* note 12.

<sup>48</sup> *Ibid.*

<sup>49</sup> N. Stephenson, *Snow Crash* (2003).



judiciary on Facebook.<sup>50</sup> The board officially began its work on October 22, 2020.<sup>51</sup> As these platforms operate in France, French users will be subjected to decisions by such “burbclaves.”

## 4. Overview of gaps and challenges

Digital sovereignty debates might have to extend to more general themes of how territorial land relates to digital law. For example, if fraud or other crimes are committed in the metaverse, which law enforcement agency should investigate it? Does it depend on where the cloud information is kept, what citizenship the subject holds, or does a metaverse merit its own law enforcement agency? These questions might be imbedded in the further discussions about digital sovereignty. Normally, if a crime is committed in France, French law applies. The IP address of the perpetrator may determine ‘where’ the crime was committed. However, there needs to be a decision made on how to treat crimes in the metaverse and when national LEAs should get involved.

The proposed regulation in the AI Act stresses that training, validation, and test datasets must be subject to appropriate data governance and management practices to mitigate possible biases.<sup>52</sup> It is not specified how systems will be tested for such biases. Should they be benchmarked against the equality of opportunities, equality of outcomes, or other criteria? These biases will be important in understanding how biometric data and mental data collected in a metaverse can be used fairly and unfairly.

A big ethical challenge, that has relevancy for legal liability, is how damage and responsibility in the metaverse are conceptualized. On one hand, virtual actions do not directly translate into physical damage, and despite immersion, users are aware of their stats in the digital space;<sup>53</sup> on the other hand, lasting psychological effects can be created by experiences in a metaverse. Thus, legal liability can be understood in terms of actions and their virtual analogues, the psychological effects they produce, or both. The model of responsibility and liability is still to be clearly conceptualized.

<sup>50</sup> Klonick, 'Inside the Making of Facebook's Supreme Court', *The New Yorker* (2021), available at <https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court> (last visited 25 October 2022).

<sup>51</sup> B. Fung, *Facebook's Oversight Board Is Finally Hearing Cases, Two Years after It Was First Announced* | *CNN Business*, 22 October 2020, CNN, available at <https://www.cnn.com/2020/10/22/tech/facebook-oversight-board/index.html> (last visited 25 October 2022).

<sup>52</sup> European Commission, *supra* note 15.

<sup>53</sup> L. Adomaitis, A. Grinbaum and D. Lenzi, *TechEthos D2.2: Identification and Specification of Potential Ethical Issues and Impacts and Analysis of Ethical Issues of Digital Extended Reality, Neurotechnologies, and Climate Engineering* (2022), available at <https://hal-cea.archives-ouvertes.fr/cea-03710862> (last visited 25 October 2022).

## 5. Conclusion

Although France possesses one of the longest histories of data protection in the digital age, there are no existent national legislation that would consider extended reality and the concept of a metaverse specifically and entirely. Different existent laws provide avenues to tackle particular issues in the metaverse, like data protection, manipulation, lying, or regulating and taxing digital assets. However, XR specific phenomena, like illicit activities in a virtual space, damage produced by autonomous chatbots and avatars, the double identity of avatar-human, anonymity of an avatar, are not entirely covered. Ongoing specific debates single out the question of identity as the main one for a legal framework. Should we identify avatars and how? Other specific concerns also stand out regarding posthumous data, impersonation, unfair biases, the privacy of biometric and mental data, consent practices and law enforcement in a metaverse. The ongoing discussions in France will likely carry over to the European level and vice versa, anything that is decided on the European level will be implemented in France.

## 6. References

- Adomaitis L., Grinbaum A. and Lenzi D., TechEthos D2.2: Identification and Specification of Potential Ethical Issues and Impacts and Analysis of Ethical Issues of Digital Extended Reality, Neurotechnologies, and Climate Engineering (2022), available at <https://hal-cea.archives-ouvertes.fr/cea-03710862> (last visited 25 October 2022).
- Basdevant A., François C. and Ronfard R., Mission Exploratoire Sur Les Métavers (2022).
- Bougiakiotis, 'One Law to Rule Them All? The Reach of EU Data Protection Law after the Google v CNIL Case', 42 Computer Law & Security Review (2021) 105580.
- Chatellier R., Métavers : ce jeu dont qui sera le héros ? | CNIL, 2022, available at <https://www.cnil.fr/fr/metavers-ce-jeu-dont-qui-sera-le-heros> (last visited 16 March 2022).
- Chatellier R., Métavers : réalités virtuelles ou collectes augmentées ?, 5 November 2021, available at <https://linc.cnil.fr/fr/metavers-realites-virtuelles-ou-collectes-augmentees> (last visited 28 October 2022).
- Council of Europe, Convention 108 +Convention for the Protection of Individuals with Regard to the Processing of Personal Data.
- Council of Europe, Draft Declaration of the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes, 13 February 2019.
- Creswell et al., 'Generative Adversarial Networks: An Overview', 35 IEEE Signal Processing Magazine (2018) 53.
- David F., Metaverse français : les principaux metaverses en France, 24 May 2022, BeinCrypto France, available at <https://fr.beincrypto.com/apprendre/metaverse-francais-les-principaux-metaverses-en-france/> (last visited 24 October 2022).
- Demiaux and Si Abdallah, 'How Can Humans Keep the Upper Hand', Report on the Ethical Matters Raised by Algorithms and Artificial Intelligence. Paris: Commision Nationale Informatique et Libertés (2017).
- European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, 2021.
- European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, 2020.
- Fung B., Facebook's Oversight Board Is Finally Hearing Cases, Two Years after It Was First Announced | CNN Business, 22 October 2020, CNN, available at <https://www.cnn.com/2020/10/22/tech/facebook-oversight-board/index.html> (last visited 25 October 2022).
- Gray, et al., 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective', in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (2021) 1.
- Grinbaum A. and Adomaitis L., The Ethical Need for Watermarks in Machine-Generated Language, arXiv:2209.03118, 7 September 2022.

Klonick, 'Inside the Making of Facebook's Supreme Court', The New Yorker (2021) , available at <https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court> (last visited 25 October 2022).

LINC, [dossier] Assistants vocaux, juin 2018, available at <https://linc.cnil.fr/fr/dossier-assistants-vocaux> (last visited 28 October 2022).

Longuet G., Le Devoir de Souveraineté Numérique, n° 7 tome (2019).

Papadogiannakis, et al., 'User Tracking in the Post-Cookie Era: How Websites Bypass GDPR Consent to Track Users', in Proceedings of the Web Conference 2021 (2021) 2130.

Simon C., Meta lance une 'académie du métavers' en France à la rentrée 2022, 12 June 2022, LExpress.fr, available at [https://www.lexpress.fr/actualites/1/societe/meta-lance-une-academie-du-metavers-en-france-a-la-rentree-2022\\_2175065.html](https://www.lexpress.fr/actualites/1/societe/meta-lance-une-academie-du-metavers-en-france-a-la-rentree-2022_2175065.html) (last visited 24 October 2022).

Stephenson N., Snow Crash (2003).

Zalnieriute, 'Google LLC v. Commission Nationale de l'informatique et Des Libertés (CNIL)', 114 American Journal of International Law (2020) 261.

Article 150 VH Bis - Code Général Des Impôts, 24 May 2019.

Article 223-15-2 - Code Pénal, 14 May 2009.

Article 1104 - Code Civil, 1 October 2016.

Article 1112-1 - Code Civil, 1 October 2016.

Article 1137 - Code Civil, 1 October 2018.

Article L120-1 - Code de La Consommation, L120-1, 2008.

'Cerna (Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene', in 2018. Research Ethics in Machine Learning.

Charter of Fundamental Rights of the European Union, OJ C, vol. 326, 26 October 2012.

Constitution Du 4 Octobre 1958, 4 October 1958.

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), OJ L, vol. 201, 12 July 2002.

European Parliament Resolution of 19 May 2021 on Artificial Intelligence in Education, Culture and the Audiovisual Sector (2020/2017(INI)), 2021.

ECJ, Google LLC, Successor in Law to Google Inc v Commission Nationale de l'informatique et Des Libertés (CNIL), Case C-507/17 , 24 September 2019, available at <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507> (last visited 25 October 2022).

Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés, 6 January 1978.

LOI N° 2016-1321 Du 7 Octobre 2016 Pour Une République Numérique (1), 2016-1321, 7 October 2016.

LOI N° 2019-486 Du 22 Mai 2019 Relative à La Croissance et La Transformation Des Entreprises (1), 2019-486, mai 2019.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-Assets, and Amending Directive (EU) 2019/1937, 2020.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance), OJ L, vol. 119, 27 April 2016.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L, vol. 257, 23 July 2014.

# TECHETHOS

FUTURE ○ TECHNOLOGY ○ ETHICS

Coordinated by



Partners



Linked Third Parties



@TechEthosEU



TechEthosEU

[www.techethos.eu](http://www.techethos.eu)

[info@techethos.eu](mailto:info@techethos.eu)