



# Artificial Intelligence, Big Data and Fundamental Rights

## Country Research France

**2020**

Report provided to FRA  
under contract D-SE-19-T02<sup>1</sup>

**DISCLAIMER:** This document was commissioned under contract as background material for comparative analysis by the European Union Agency for Fundamental Rights (FRA) for the project [Artificial Intelligence, Big Data and Fundamental Rights](#). The information and views contained in the document do not necessarily reflect the views or the official position of the FRA. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion.

<sup>1</sup> Report prepared by Ecorys and Science Po Chair Digital, Governance and Sovereignty. While every effort has been made by the FRA contractor to refer to relevant national institutions, policy developments and law relating to the field of AI and fundamental rights, given the wide reach of AI developments and the quickly evolving nature of the field there may be omissions or recent developments at national level that are not referred to in this country research.

## Table of contents

<b>1</b>	<b>Constitutional and institutional context</b>	<b>4</b>
1.1	Map of the major stakeholders	4
1.1.1	Parliament and government	4
1.1.2	Decentralised bodies	7
1.1.3	Public bodies and agencies	8
1.1.4	Advisory councils and bodies	12
1.1.5	Research institutions	15
1.1.6	Judiciary	16
1.1.7	Public-private partnerships and relations between the private and public sector	19
1.1.8	Civil society	20
1.1.9	Business associations	21
1.2	International relations	21
1.2.1	General strategy	22
1.2.2	European linkages – Council of Europe and OECD	22
1.2.3	International linkages – G20	22
1.3	National strategies and guidelines	23
1.3.1	The CNIL Report	23
1.3.2	The Villani Report	24
1.3.3	The French National Strategy on AI: AI for Humanity	25
1.3.4	The implementation of the AI for Humanity national strategy	26
1.4	Standards and voluntary guidelines; the role of the private sector	27
1.4.1	Government standards and guidelines	27
1.4.2	Self-regulation in the private sector	27
1.4.3	Standards organizations	27
1.5	Sample recent developments	28
1.5.1	Facial recognition	28
1.5.2	Tax fraud anticipation system	31
1.5.3	Healthcare applications	32
1.5.4	Retail	33
<b>2</b>	<b>Laws and regulations applicable to AI and big data</b>	<b>34</b>
2.1	General	34
2.2	Application of fundamental rights laws to AI	36
2.2.1	Protection of personal data	37
2.2.2	Privacy challenges raised by the Open Data policy of judicial decisions	40
2.2.3	Protecting citizens in case of algorithmic decision making	42
2.2.4	Transparency requirements imposed on public administrations	44
2.3	Overview of laws applicable to AI and big data	47
<b>3</b>	<b>Future development</b>	<b>86</b>
<b>4</b>	<b>References</b>	<b>88</b>

## Abbreviations

AAI	Independent Administrative Authority
ACSEL	Association pour le Commerce et les Services en Ligne
AFNOR	Association Française de Normalisation
AI	Artificial Intelligence
ALICEM	Association Française de Normalisation
CADA	Commission d'accès aux documents administratifs
CAHAI	Ad Hoc Committee on Artificial of the Council of Europe
CCNE	Comité Consultatif National d'Éthique pour les sciences de la vie et de la santé
CEA	Commissariat à l'Énergie Atomique et aux Energies Alternatives
CEN	European Committee for Standardization
CENELEC	European Committee for Standardization in Electronics and Electrotechnics
CEPEJ	European Commission for the Efficiency of Justice of the Council of Europe
CEPII	Centre d'études prospectives et d'informations internationales
CERNA	Commission de réflexion sur l'éthique de la recherche en sciences et technologie du numérique d'Allistene
CESE	Economic, Social and Environmental Council
CNCDH	National Consultative Commission on Human Rights
CNDS	Commission Nationale de Déontologie de la Sécurité
CNIL	Commission nationale de l'informatique et des libertés
CNN	Conseil National du Numérique
CNRS	French National Centre for Scientific Research
CRPA	Code of relations between the public and the administration
CSA	Conseil Supérieur de l'Audiovisuel
DGCCRF	Direction Générale de la Consommation, de la Concurrence et de la Répression des Fraudes
ECHR	European Convention on Human Rights
EDS	Entrepôt de données de santé
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
GIP	Groupement d'Intérêt Public
GPAI	Global Partnership on AI
HALDE	Haute Autorité de Lutte contre les Discriminations et pour l'Égalité
ICST	Information, Communication and Space Technology
IEC	International Electrotechnical Commission
INDS	National Institute for Health Data
INRIA	National Institute for Research in Computer Science and Automation
ISO	International Standards Organization
OECD	Organisation for Economic Co-operation and Development
OPECST	Office parlementaire d'évaluation des choix scientifiques et techniques

# 1 Constitutional and institutional context

## 1.1 Map of the major stakeholders

### 1.1.1 Parliament and government

#### Parliament

The French Parliament is made up of two assemblies, the National Assembly and the Senate. These two assemblies examine and pass laws, monitor the government, and assess public policies. The national assembly, which is elected by direct universal suffrage, plays a predominant role in the legislative process, since it has the final say in cases of disagreement with the senate. Furthermore, it may vote the government out of office. Much work has been done regarding artificial intelligence in both assemblies. In the national assembly, the study group *économie numérique de la donnée, de la connaissance et de l'intelligence artificielle* is currently examining France's digital and knowledge-based data economy as well as artificial intelligence (AI).<sup>2</sup> However, this group has yet to release a report or any policy recommendations. In the senate, a recent report dealt with the European strategy on AI:<sup>3</sup> this report mainly analysed the European Commission's proposals in this area and prepared for a resolution to promote investment in artificial intelligence in Europe.

Parliamentary work is supplemented by the **Parliamentary Office for Scientific and Technological Assessment** (*Office parlementaire d'évaluation des choix scientifiques et techniques – OPECST*), which was set up by law n° 83-609 of 08 July 1983. This office informs the parliament on scientific and technological options and developments, which feeds into parliament's decision-making. The OPECST is composed of eighteen members of the national assembly and eighteen senators. Over the past few years, the OPECST has consistently dealt with new technologies and artificial intelligence. The OPECST has released various reports, for example:

- *Artificial intelligence and health data* (2019),<sup>4</sup>

---

<sup>2</sup> XVe Législature, Assemblée nationale, 'Groupe d'études : Économie Numérique de La Donnée, de La Connaissance et de l'intelligence Artificielle', accessed 18 March 2020, [http://www2.assemblee-nationale.fr/instances/resume/OMC\\_PO746837/legislature/15](http://www2.assemblee-nationale.fr/instances/resume/OMC_PO746837/legislature/15).

<sup>3</sup> André Gattolin et al., 'Intelligence Artificielle: L'urgence d'une Ambition Européenne, Rapport d'information, Fait Au Nom de La Commission Des Affaires Européennes', 31 January 2019.

<sup>4</sup> Gérard Longuet and Cédric Villani, 'L'intelligence Artificielle et Les Données de Santé, Rapport Fait Au Nom de l'office Parlementaire d'évaluation Des Choix Scientifiques et Technologiques' (Paris: Assemblée Nationale, 21 March 2019).

- *The algorithms which serve the public action: the case of the Post-Bac Admission portal (2018),<sup>5</sup> and*
- *For a mastered, useful and demystified AI (2017).<sup>6</sup>*

The OPECST also published briefings on *Facial Recognition (2019),<sup>7</sup>* and the *Internet of Things (2018).<sup>8</sup>* The OPECST suggests to promote safe, transparent and fair algorithms and robots, and to elaborate a charter of artificial intelligence and robotics.<sup>9</sup>

## Government

The **Prime Minister** is the Head of Government and is appointed by the President of the Republic, i.e. the Head of State. The Prime Minister “directs the actions of the Government” (article 21 of the Constitution), sets out essential political guidelines, and ensures the coordination of government action. The Prime Minister ensures the implementation of laws and exercises regulatory power. According to article 20 of the constitution, the Prime Minister has [various services](#) at its disposal in the name of the government. These services include the **General Secretary of the Government, France Stratégie** (see below) and the **Interministerial Directorate for Digital Services** (*Direction interministérielle du numérique – DINUM*). The latter was recently created by a decree of 25 October 2019 and replaced the DINSIC (*direction interministérielle du numérique et du système d’information et de communication de l’État*). Within the General Secretary of the Government, the “*Direction de l’information légale et administrative*” (**DILA**) has started an AI project called “the Chatbot Factory”, which is a conversational agent designed for the website [service-public.fr](http://service-public.fr).

Ministers head ministerial departments and supervise public legal entities acting within their ministerial department’s field of competence. Although regulatory power is, in principle, exercised by the Prime Minister, it is often delegated to ministers. Major policy lines and

<sup>5</sup> Villani, Cédric and Gérard Longuet, ‘Les Algorithmes Au Service de l’action Publique: Le Cas Du Portail Admission Post-Bac, Rapport Au Nom de l’office Parlementaire d’évaluation Des Choix Scientifiques et Technologiques’ (Paris: Assemblée Nationale, 15 February 2018).

<sup>6</sup> Claude De Ganay and Dominique Gillot, ‘Pour Une Intelligence Artificielle Maîtrisée, Utile et Démystifiée, Rapport Fait Au Nom de l’office Parlementaire d’évaluation Des Choix Scientifiques et Technologiques’ (Paris: Assemblée Nationale, 15 March 2017).

<sup>7</sup> Didier Baichère, ‘Briefing 14: Facial Recognition’ (Science and Technology Briefings, Parliamentary Office for Scientific and Technological Assessment, July 2019), 14, <http://www2.assemblee-nationale.fr/content/download/179314/1794787/version/2/file/Note+Reconnaissance+Faciale+-+EN.pdf>.

<sup>8</sup> Didier Baichère, ‘Briefing 1: Internet of Things (Connected Objects)’ (Science and Technology Briefings, Parliamentary Office for Scientific and Technological Assessment, March 2018), 1, [http://www2.assemblee-nationale.fr/content/download/79390/813627/version/1/file/notescientif\\_objets+connectees+ENG20190409.pdf](http://www2.assemblee-nationale.fr/content/download/79390/813627/version/1/file/notescientif_objets+connectees+ENG20190409.pdf).

<sup>9</sup> De Ganay and Gillot, ‘Pour Une Intelligence Artificielle Maîtrisée, Utile et Démystifiée, Rapport Fait Au Nom de l’office Parlementaire d’évaluation Des Choix Scientifiques et Technologiques’.

strategies regarding technological development and AI are set out by the Prime Minister and the **Secretary of State for Digital Affairs** (*secretariat d'Etat chargé du Numérique*). The latter is in charge of digital issues through authority delegated by the Prime Minister. The aforementioned DINUM, which is a service of the Prime Minister, has been placed under the authority of the Minister of Action and Public Accounts (*Ministère de l'Action et des Comptes Publics*), and is further at the disposal of the Minister of Economy and Finance (*Ministère de l'Economie et des Finances*) and the Secretary of State for Digital Affairs.

The **DINUM** supports public administrations in their digital transformation, advises the government about digital issues, and develops services and resources, such as [FranceConnect](#), [data.gouv.fr](#), or [api.gouv.fr](#). The DINUM is also responsible for the [TECH.GOUV program](#), which aims to accelerate the digital transition of public services.<sup>10</sup> In June 2018, six AI projects were selected by the DINUM and the Directorate of Public Transformation (*Direction interministérielle de la transformation publique – DITP*).<sup>11</sup> On 17 July 2019, a list of 15 new AI projects was disclosed.<sup>12</sup> There are

<sup>10</sup> The AI France Summit, which took place in Paris on February 2019, was organized as part of this program: France Stratégie, 'AI France Summit, 19 February 2019', accessed 18 March 2020, <https://www.strategie.gouv.fr/debats/ai-france-summit>.

<sup>11</sup> These six projects were: the detection of irregular land use (*Direction départementale des Territoires et de la Mer de l'Hérault*), the detection of restaurants posing health risks based on customers' comments (*Direction générale de l'alimentation, ministère de l'Agriculture et de l'Alimentation*), the control of nuclear risks and activities (*Autorité de sûreté nucléaire*), improving environmental policing controls (*Agence française pour la biodiversité, ministère de la Transition écologique et solidaire*), improving post-surgery treatments (*Centre hospitalier universitaire de Toulouse*), and answering users' questions thanks to a "voice bot" (*Centre national chèque emploi associatif, agence centrale des organismes de sécurité sociale*). See: Numerique.gouv.fr, 'Intelligence artificielle: 6 projets sélectionnés pour être expérimentés dans les services publics', 22 November 2018, <https://www.numerique.gouv.fr/actualites/intelligence-artificielle-6-projets-selectionnes-pour-etre-experimentes-dans-les-services-publics/>.

<sup>12</sup> These fifteen projects are: optimizing the processing of adverse health event reports (*Direction Générale de la Santé*), facilitating access to patients' information (*Centre hospitalier universitaire de Bordeaux*), development of an automatic warning system to assist in the monitoring of workers exposed to ionising radiation (*Institut de radioprotection et de sûreté nucléaire*), development of AI in dematerialized legality controls (*Direction Générale des collectivités locales*), improving the on-line pre-complaint system (*Direction Générale de la gendarmerie nationale*), identifying false customs declarations with text mining (*Direction Générale des douanes et des droits indirects*), improving the identification of the employer in the population census (*Institut national de la statistique et des études économiques – INSEE*), development of a tool to assist the establishment of craft businesses (*Chambre des métiers et de l'artisanat*), the identification of molecules contaminating the environment and the profiling of pollution sources (*Institut national de l'environnement industriel et des risques*), the development of a solution for monitoring and exploiting information to improve economic security (*Direction Générale des entreprises, Service de l'information stratégique et de la sécurité économique*), the automatic identification of a series of disputes involving the same decision (*Conseil d'Etat*), the detection of unfair terms and practices in contracts, quotations and invoices (*Direction générale de la concurrence, de la consommation et de la répression des fraudes*), facilitating the calculation of the positioning of terrestrial reference points from satellite data (*Institut national de l'information géographique et forestière*),

three departments within the DINUM. These are: the "Infrastructure and Operated Services" department (*Infrastructure et Services Opérés – ISO*), which designs and operates value-added infrastructure services that are shared between administrations. Such services include, for example, the interdepartmental network (*Réseau Interministériel de l'Etat – RIE*). Another department within the DINUM is the "Performance of digital services" department (*Performance des Services Numériques*), which designs and supports the implementation of inter-ministerial action plans regarding mutualisation, dematerialization, project management and quality of digital services. The third department within DINUM is the ETALAB department, which is the French task force for Open Data. ETALAB coordinates the design and implementation of the State's strategy regarding public data.

More particularly, **ETALAB** manages the platform [data.gouv.fr](https://data.gouv.fr), which is intended to make all public information of the state, public institutions and, if they agree, also of local authorities, freely available. ETALAB serves as the [Chief Data Officer of the French State \(\*Administrateur général des données\*\)](#). ETALAB is also in charge of supporting administrations in [the opening and responsible use of public algorithms](#) and of promoting data sciences and artificial intelligence in the public sphere. ETALAB has a programme called "[Lab IA](#)", which is aimed at conducting [data sciences and AI projects](#). Finally, ETALAB aims to implement the principles of "open government" ([gouvernement ouvert](#)). These principles refer to: transparency of public action, consultation with civil society, citizen participation, and open innovation. In particular, ETALAB coordinates France's action within the Open Government Partnership ("[Partenariat pour un gouvernement ouvert – PGO](#)"), together with the Ministry of Europe and Foreign Affairs.

### 1.1.2 Decentralised bodies

The main units of local government are defined by the French Constitution (*collectivités territoriales*). They are the *régions*, the *départements*, the *communes*, and the overseas territories. A small number of local governments with special status (*collectivités territoriales à statut particulier*), have slightly different administrative frameworks (Corsica, Paris, Lyon, Marseille).

- Regional councils of the 21 metropolitan *regions* and five overseas *régions* are directly elected and play a role in economic and social development, education, and cultural matters.
- The 96 *départements* in metropolitan France and five overseas *départements* are run by a General Council elected for six years and

---

identifying differences in caselaw (*Cour de cassation*), improving the coastal mapping (*Service hydrographique et océanographique de la marine*). See: [Numerique.gouv.fr](https://numerique.gouv.fr), 'Intelligence artificielle: 15 nouveaux projets vont être expérimentés dans les administrations', 17 July 2019, <https://www.numerique.gouv.fr/actualites/intelligence-artificielle-15-nouveaux-projets-vont-etre-experimentes-dans-les-administrations/>.

responsible for the main departmental services of welfare, health, administration, and departmental employment.

- Each of the 36,500 *communes* has a municipal council elected for six years and responsible for “the affairs of the commune.” Each council elects a mayor who is in charge of the municipal police, and who ensures public order, security, and health. Mayors further guarantee the supervision of public places to prevent adverse events, such as fires and floods. In certain cities, such as Lyon and Lille, cooperative urban communities have been created to enable the joint management and planning of some municipal services, such as waste management and road building. Some *communes* within urban areas of more than 50,000 inhabitants have created joint development projects by means of a new form of administrative units, which is known as the *communauté d’agglomération*.

Within this framework, various local French communities have announced that they are developing AI projects, even though those projects do not always involve *machine learning* as such. Examples of AI projects in this regard include the following.<sup>13</sup> Many cities are currently developing videosurveillance systems (see below 1.5.1). Furthermore, the City of Marseille has launched a predictive policing project in cooperation with Engie Ineo, which is called “*Big data de la tranquillité publique*”.<sup>14</sup> The project is designed to collect and cross-reference numerous sources to assist municipal police officers in their daily duties. In concrete terms, the objective is to anticipate possible disturbances. Depending on the sectors, each day is stamped with a green, orange or red colour, and the algorithm assigns a dangerousness score ranging from 1 to 10. For the moment, the processed data has been collected by the municipality (markets, municipal police, events, urban supervision centre, works, etc.). But the city wants to develop its platform and integrate data from partners such as telephone operators, hospitals, fire brigades, national police and social network data. The City of Nice is developing both a predictive policing tool called “SenCity”, which is developed in cooperation with Engie Ineo, and a video surveillance project called “SafeCity”, which is developed in cooperation with Thales.<sup>15</sup>

### 1.1.3 Public bodies and agencies

Various independent agencies have jurisdiction over AI projects. These are: the National Commission on Informatics and Liberty (*Commission nationale de l’informatique et des libertés – CNIL*), the Superior Council

<sup>13</sup> Institut d’aménagement et d’urbanisme de la région d’Île-de-France and Camille Gosselin, *La police prédictive: enjeux soulevés par l’usage des algorithmes prédictifs en matière de sécurité publique* (Paris: IAU Île-de-France, 2019).

<sup>14</sup> Jean-Marc Leclerc, ‘Un rapport analyse les enjeux de la police prédictive’, Le Figaro.fr, 6 February 2020, <https://www.lefigaro.fr/actualite-france/un-rapport-analyse-les-enjeux-de-la-police-predictive-20200206>.

<sup>15</sup> Félix Tréguer, ‘La Smart City policière se répand comme traînée de poudre’, Club de Mediapart, 7 July 2018, <https://blogs.mediapart.fr/felix-treguer/blog/070718/la-smart-city-policiere-se-repand-comme-trainee-de-poudre>.



of the Audiovisual (*Conseil Supérieur de l'Audiovisuel* – CSA), the Commission for Access to Administrative Documents ([\*Commission d'accès aux documents administratifs\*](#) – CADA), and the Defender of Rights (*Défenseur des droits*). Each of these independent agencies will be addressed in turn below.

**The Data Protection Agency: the CNIL.** The National Commission on Informatics and Liberty (*Commission nationale de l'informatique et des libertés* – CNIL) is an independent [French](#) administrative agency, which stands as the French data protection authority. The CNIL was created by the Data Protection Act of 1978 (*loi informatique et libertés*), following the rejection of the SAFARI project, which was a program designed to create a centralized governmental database where French citizens would have been identified with a single specific number<sup>16</sup>. The strong opposition to this program led the French government to set up a commission mandated to recommend concrete measures intended to guarantee that any developments in information technology would remain respectful of privacy, individual rights and public liberties. This 'Commission on Information Technology and Liberties' then recommended that an independent oversight authority be created. The CNIL acts on behalf of the state, without being under the authority of the government or a minister. It is composed of 18 elected or appointed members. The CNIL is responsible for ensuring the protection of all personal data contained in files and computer or paper processing, both in the public and private sectors. The CNIL is therefore in charge of ensuring that information technology is at the service of citizens and does not affect human identity, human rights, privacy and individual or public freedoms. The CNIL's power are stated in article 8 of the Data Protection Law (Loi "Informatique et Libertés"). The CNIL alerts, advises and informs various audiences. The law gives the CNIL the power to suggest to the Government legislative or regulatory measures to adapt the protection of liberties to the evolution of computer processes and techniques. It can make recommendations and respond to requests for consultation from public authorities. For example, the CNIL has recently released a report on facial recognition.<sup>17</sup> It has also, at the request of a local authority, issued an opinion on the testing of facial recognition in two high schools.<sup>18</sup> In addition, the CNIL has regulatory powers for the enactment of model regulations on information systems security or for the adoption of simplified standards or exemptions from declaration. The CNIL then has the power to authorise certain sensitive processing operations, like, for example, biometric processing necessary to check the identity of individuals. The CNIL has also a power of control and

<sup>16</sup> Victor Demiaux, « De la CNIL au RGPD : 40 ans de protection des données », L'Histoire, 25 May 2018  
<https://www.lhistoire.fr/entretien/de-la-cnil-au-rgpd%C2%A0-40-ans-de-protection-des-donn%C3%A9es>

<sup>17</sup> CNIL, 'Reconnaissance Faciale: Pour Un Débat à La Hauteur Des Enjeux', 15 November 2019, <https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux>.

<sup>18</sup> <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>

sanction. It may carry out any control relevant to its mission, take individual decisions with regard to persons, impose sanctions and order emergency measures. The CNIL can carry out controls on its own initiative, but it can also act following complaints and reports from users. The control may result in a formal notice to comply with the law or in a sanction provided for in article 45 of the Data Protection law which may be pecuniary (fine) or non-pecuniary (public warning, order to stop the treatment). In 2019, the CNIL imposed a €50,000,000 fine on Google for not complying with the provisions set out in the General Data Protection Regulation (GDPR) provisions.<sup>19</sup> Appeals against the CNIL's regulatory or individual decisions may be made to the Council of State. For example, the Council of State approved the CNIL's guidelines which provided for an additional 12 months delay (until mid-2020) to comply with the GDPR provisions concerning cookies and trackers<sup>20</sup>.

**The Superior Council of the Audio-visual** (*Conseil Supérieur de l'Audiovisuel – CSA*). The CSA is an independent public authority created in 1989 and in charge of regulating the audio-visual sector. Its main role is to protect both freedom of expression and public interest. Its action is based on the respect and the protection of individual rights and freedoms, social responsibility and the necessity to ensure the economic and technological regulation of the audio-visual market. Although the CSA has no direct jurisdiction over technology issues, it is competent in every matter involving the media and freedom of expression. It has the power to make individual decisions regarding publishers, broadcasters or distributors. The CSA has recently released a recommendation to online platforms regarding fake news.<sup>21</sup> It has also published a study, which questions the capacity to adequately inform the public on YouTube's recommendation algorithm.<sup>22</sup>

<sup>19</sup> CNIL, 'Délibération de La Formation Restreinte N° SAN – 2019-001 Du 21 Janvier 2019 Prononçant Une Sanction Pécuniaire à l'encontre de La Société GOOGLE LLC', 21 January 2019, <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038032552>.

<sup>20</sup> CE 16 octobre 2019, Associations "La Quadrature du net" et "Caliopen", req. n°433069

<sup>21</sup> CSA - Conseil supérieur de l'audiovisuel, 'Recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations', 16 May 2019, <https://www.csa.fr/Arbitrer/Espace-juridique/Les-textes-reglementaires-du-CSA/Les-deliberations-et-recommandations-du-CSA/Recommandations-et-deliberations-du-CSA-relatives-a-d-autres-sujets/Recommandation-n-2019-03-du-15-mai-2019-du-Conseil-superieur-de-l-audiovisuel-aux-operateurs-de-plateforme-en-ligne-dans-le-cadre-du-devoir-de-cooperation-en-matiere-de-lutte-contre-la-diffusion-de-faussees-informations>.

<sup>22</sup> CSA - Conseil supérieur de l'audiovisuel, 'Capacité à informer des algorithmes de recommandation: une expérience sur le service YouTube', 12 November 2019, <https://www.csa.fr/Informer/Collections-du-CSA/Focus-Toutes-les-etudes-et-les-comptes-rendus-synthetiques-proposant-un-zoom-sur-un-sujet-d-actualite/Les-etudes-du-CSA/Capacite-a-informer-des-algorithmes-de-recommandation-une-experience-sur-le-service-YouTube>.

**The Commission for Access to Administrative Documents** (*Commission d'accès aux documents administratifs* – CADA). The Commission for Access to Administrative Documents is an independent administrative authority responsible for ensuring the freedom of access to administrative documents and public archives. It is also in charge of questions related to the reuse of public information. Claims before the CADA can be filed by natural or legal persons whose demand of access to administrative documents or of reuse of public information has been rejected. The commission may also be consulted by public administrations. When the CADA's opinion is in favour of seeing a claim satisfied, i.e. to have a document communicated to a claimant by an administration, the administration in question must express its position within one month. If the administration still refuses to communicate the document, the claim must be brought before an administrative judge. The CADA publishes an annual report of activity, as well as its favourable opinions. Over the recent months, several claims were brought before the CADA with a view to bring about the online publication of the main characteristics of the algorithms used by social organizations, namely the National Family Allowances Fund (*Caisse Nationale des Allocations Familiales* – CNAF)<sup>23</sup> and Parcoursup, an online guidance tool on courses for graduates.<sup>24</sup> In both cases, the CADA's decision was in favour of transparency.

**The Defender of Rights** (*Défenseur des droits*). The Defender of Rights is an independent authority created in 2011 through the merging of 4 former institutions: the *Médiateur de la République*, the *Défenseur des Enfants*, the *Haute Autorité de Lutte contre les Discriminations et pour l'Égalité* (HALDE) and the *Commission Nationale de Déontologie de la Sécurité* (CNDS). There are around 500 delegates of the Defender of Rights that are disseminated within the French territory. The Defender of Rights is responsible for defending the rights and liberties of citizens, especially against administrations. It also has special prerogatives in the promotion of the rights of children, the fight against discrimination and the respect of ethics by security forces. Any individual or legal entity can directly and free of charge file a complaint before the Defender of Rights in the following cases:

- They believe they are being discriminated against;
- They find that a representative of public forces, e.g. of the police, gendarmerie, or customs, or of private forces, e.g. private security officers, has not respected the rules of good behaviour;
- They encounter problems in their relations with a public service, e.g. with the Family Allowance Fund, Employment Centre, pension funds, et cetera;
- They believe that children's rights are violated.

<sup>23</sup> CADA, 'Avis Du 18 Juillet 2019, Caisse Nationale Des Allocations Familiales (CNAF), N° 20185277', 18 July 2019, 18, <https://www.doctrine.fr/d/CADA/2019/CADA20185277>.

<sup>24</sup> CADA, 'Avis du 6 juin 2019, Ministère des Armées, n° 20185611', Doctrine, 6 June 2019, <https://www.doctrine.fr/d/CADA/2019/CADA20185611>.

The Defender of Rights acts as a mediator (*ombudsman*). It can also make official recommendations, ask an authority to take action, and submit comments to courts. In 2017, the Defender of Rights was seized by the user of a platform of classified ads for real estate rentals and made a recommendation to platforms in order to avoid the publication of discriminatory advertisements.<sup>25</sup> In 2019, several claims about Parcoursup were brought by associations and unions before the Defender of Rights. The latter adopted an official recommendation asking the government to disclose the methodology of the Parcoursup algorithms.<sup>26</sup> In 2019, the Defender of Rights also adopted various opinions on the proposed legislation on Bioethics (*projet de loi relative à la bioéthique*) in which he dealt with the use of AI tools in healthcare. In its Opinion (Avis) n°19-11 of September 5 2019, the Defender of Rights insisted on the need to maintain human intervention when algorithms are used and the value of an interdisciplinary approach. In its Opinion (Avis) n°19-13 of December 20, 2019, the Defender of Rights highlighted the necessity to train healthcare professionals to the use of algorithms, the importance of specifying how to set up the algorithms, the need to ensure that algorithms work with data that is representative of the population in order to avoid discrimination and the possibility to reformulate the procedures for obtaining consent. On May 31 2020, the Defender of Rights released a report on algorithmic biases entitled “*Algorithmes: prévenir l’automatisation des discriminations*” which includes various recommendations.<sup>27</sup>

#### 1.1.4 Advisory councils and bodies

France has an extensive number of advisory councils and bodies.

**The Council of State** (*Conseil d’État*) The Council of State advises the government on the preparation of laws, ordinances and certain decrees. It also answers the government’s queries on legal affairs and conducts studies upon the request of the government, and through its own initiative regarding administrative or public policy issues. Every year, the Council of State publishes its annual reports. Over the past few years, the Council of State released two reports dealing with artificial intelligence: “Digital Technology and Fundamental Rights” (*Le numérique et les droits fondamentaux*, 2014),<sup>28</sup> and “Public Power and

<sup>25</sup> Défenseur des droits, ‘Décision Du Défenseur Des Droits N°2017-036’, 26 January 2017, [https://juridique.defenseurdesdroits.fr/doc\\_num.php?explnum\\_id=16120](https://juridique.defenseurdesdroits.fr/doc_num.php?explnum_id=16120).

<sup>26</sup> Défenseur des droits, ‘Décision Du Défenseur Des Droits N°2019-021’, n.n., [https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/decision\\_defenseur\\_des\\_droits\\_2019-021.pdf](https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/decision_defenseur_des_droits_2019-021.pdf).

<sup>27</sup> Défenseur des droits, *Algorithmes : prévenir l’automatisation des discriminations*, May 2020 <https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/synth-algos-num2-29.05.20.pdf>

<sup>28</sup> Le Conseil d’État, ‘Étude annuelle 2014 - Le numérique et les droits fondamentaux’, Conseil d’État, 9 September 2014, <https://www.conseil-etat.fr/ressources/etudes->

Digital Platforms: Supporting ‘Uberisation’” (*Puissance publique et plateformes numériques: accompagner l’“ubérisation”*, 2017).<sup>29</sup> The 2014 Report suggested adopting new principles to protect fundamental rights in the digital age, including: the ‘self-determination of data’, net neutrality, loyalty of platforms, definition of standards under the CNIL’s supervision, the right to be unlisted, whistleblowing procedures, collective redress for consumers, protection of personal data, sanctions against unlawful content, media pluralism, and open data policy. More particularly, this report suggested that French legislation be amended to regulate predictive algorithms, which has, since then, been passed.<sup>30</sup>

**The Economic, Social and Environmental Council** (*Conseil économique, social et environnemental – CESE*). The CESE is a consultative assembly. The council examines economic, social or environmental changes and suggests reforms. The Prime Minister is obliged to ask the Council’s opinion on any plan or programming law dealing with economic, social or environmental issues. The Prime Minister may also request the council’s advice about laws dealing with other matters. Parliament may refer to the council as well. The council may also decide to intervene on a given issue on its own initiative: for example, the council has called for more transparency of allocation algorithms, such as those used by Parcoursup.<sup>31</sup>

**France Stratégie**. The organization “*France Stratégie*” is a public think tank placed under the authority of the Prime Minister. It is in charge of conducting expertise and prospective analysis on major social and economic topics. France Stratégie publishes reports and analyses, organises debates, makes recommendations to the government, and contributes to the evaluation of public policies. In 2018, France Stratégie released a [report on AI and the future of work](#).<sup>32</sup> Additionally, France Stratégie runs a network of eight public bodies with sectorial expertise. For example, the Council of Economic Analysis (*Conseil d’Analyse Economique*), which is composed of economists, carries out independent economic analysis for the government. The leading French centre for research and expertise on the world economy, the [Centre d’études prospectives et d’informations internationales \(CEPII\)](#), produces studies, research, databases and analyses on the major issues of the world economy.

---

publications/rapports-etudes/etudes-annuelles/etude-annuelle-2014-le-numerique-et-les-droits-fondamentaux.

<sup>29</sup> Le Conseil d’État, ‘Étude annuelle 2017 - Puissance publique et plateformes numériques: accompagner l’“ubérisation”’, Conseil d’État, 28 September 2018, <https://www.conseil-etat.fr/ressources/etudes-publications/rapports-etudes/etudes-annuelles/etude-annuelle-2017-puissance-publique-et-plateformes-numeriques-accompagner-l-uberisation>.

<sup>30</sup> Propositions n°23, 24, 25.

<sup>31</sup> Laure Delair and Albert Ritzenthaler, ‘L’orientation Des Jeunes’ (CESE 12, 11 April 2018).

<sup>32</sup> Salima Benhamou and Lionel Janin, ‘Intelligence Artificielle et Travail, Rapport à La Ministre Du Travail et Au Secrétaire d’État Chargé Du Numérique’ (Paris: France Stratégie, March 2018).

**The National Consultative Committee on Ethics** (*Comité Consultatif National d'Éthique pour les sciences de la vie et de la santé – CCNE*). The National Consultative Committee on Ethics is an independent institution created in 1983. Its mission is to deliver opinions on the ethical challenges and the social issues raised by progress in the fields of biology, medicine and health. In a way, the CCNE is a think tank designed to alert public authorities and society in general. Today, every reform on ethical questions in the aforementioned areas must include a public debate initiated by the CCNE, after consulting the competent parliamentary committees and the OPECST. Various individuals can bring an issue before the CCNE, including the President of the Republic, the Presidents of the Parliamentary Assemblies, members of the government, higher education institutions, and others. The CCNE can also decide to deal with any questions raised by a citizen or a group of citizens on its own initiative. In 2019, the CCNE released an opinion on the issues raised by big data in the health sector.<sup>33</sup> At the time of writing, lawmakers actively working to adopt a new law on bioethics have been using this opinion in their deliberations.

**The National Consultative Commission on Human Rights** (*Commission nationale consultative des droits de l'homme – CNCDH*). The National Consultative Commission on Human Rights is a public body that promotes and protects human rights. It is an independent administrative authority (AAI) and is in charge of advising the government in the fields of human rights, international humanitarian law, and humanitarian action. The main missions of the CNCDH are:

- ensuring that France complies with its institutional and international commitments regarding human rights;
- advising the government and parliament on prospective bills;
- promoting cooperation between public authorities and civil society;
- alerting the public about human-rights issues; and
- participating in human rights training and education.

The commission may, on its own initiative, publicly advocate to parliament and the government on measures that favour the protection and the promotion of human rights. The Defender of Rights (*Défenseur des droits*) sits *ex officio* among the members of the CNCDH. In 2018, the CNCDH published an opinion on privacy in the digital era to raise awareness about the necessity to protect privacy.<sup>34</sup>

**The National Digital Council** (*Conseil National du Numérique – CNNum*). The National Digital Council is in charge of analysing digital issues related to the digital transition of society and the economy. The

---

<sup>33</sup> CCNE, 'Avis N° 130: Données Massives et Santé: Une Nouvelle Approche Des Enjeux Éthiques' (Comité Consultatif National d'Éthique, 29 May 2019).

<sup>34</sup> CNCDH, 'Avis "Protection de La Vie Privée à l'ère Numérique"' (Commission Nationale Consultative des Droits de l'Homme, 22 May 2018), [https://www.cncdh.fr/sites/default/files/180522\\_avis\\_vie\\_privée\\_et\\_numerique\\_0.pdf](https://www.cncdh.fr/sites/default/files/180522_avis_vie_privée_et_numerique_0.pdf).

CNNum is placed under the authority of the Secretary of State in charge of digital issues. Its official function is to advise the Government on the conduct of public policies related to digital challenges. The CNNum also contributes to the development of France's official positions on digital questions at European and international levels. Finally, the CNNum publishes opinions and recommendations. In 2017, the CNNum published a joint report with France Stratégie on the impact of AI.<sup>35</sup> This report formulated various recommendations. It advised to organize a consultation to anticipate the impacts of AI, to training people, to rethink human-machine complementarity, to raise awareness on the value of data, to integrate AI into businesses, to give access to public data, and to organize data flows.

### 1.1.5 Research institutions

In the academic field, most French universities have experts working in the field of AI, particularly in development, research into AI's applications, and its consequences. According to the [AI Observatory in France](#), which is a service created within the Ministry of Higher Education and in charge of maintaining a mapping of AI actors, France counts 5,300 high-level researchers divided into 250 teams, and more than 1,000 students trained in 18 specialized master's degrees. France ranks third in the production of scientific articles on AI. The two major research institutions in the field are the National Institute for Research in Computer Science and Automation (INRIA) and the French National Centre for Scientific Research (CNRS). The INRIA is a public science and technology institution, which is supervised by the French Ministries of Research and Industry. The CNRS is a publicly funded institution, which covers all scientific disciplines. In 2018, the French government selected four projects to form a network of Interdisciplinary Institutes of Artificial Intelligence (*Instituts Interdisciplinaires d'Intelligence Artificielle – 3IA*) in Grenoble, Nice, Paris, and Toulouse. Each project will benefit from funding of around € 20,000,000 each.

In 2010, some major national players in Information, Communication and Space Technology (ICST) research decided to join forces and to create the **Allistene Alliance**. This alliance is comprised of the Alternative Energies and Atomic Energy Commission (*Commissariat à l'Énergie Atomique et aux Énergies Alternatives – CEA*), the National Centre for Scientific Research (*Centre national de la recherche scientifique – CNRS*), the Institut Mines-Télécom, the INRIA, and the organisation of university presidents (*Conférence des Présidents d'Université – CPU*). Allistene's aim is to promote collaborative thinking in terms of foresight and overall strategy. Allistene is organised into working groups, which are called "programmatic groups". Within the Allistene Alliance, one department is dedicated to ethical issues: the

<sup>35</sup> Rand Hindi and Lionel Janin, 'Anticiper Les Impacts Économiques et Sociaux de l'intelligence Artificielle, Stratégie Nationale En Intelligence Artificielle, Rapport Du Groupe de Travail 3.2, Conseil National Du Numérique' (France Stratégie, March 2017).

Digital Science and Technology Research Ethics Board (*Commission de réflexion sur l'éthique de la recherche en sciences et technologie du numérique d'Allistene – CERNA*), which was created in 2012. The CERNA's mission is to address digital ethics from a science and technology perspective. The CERNA's approach is multidisciplinary and involves various experts at the European and international level. The CERNA provides studies and recommendations and aims to raise awareness about ethical issues of the digital transition.

In 2018, the CERNA published a report entitled "Research Ethics in Machine Learning".<sup>36</sup> This report recommends creating a unified national research initiative on the societal and ethical impact of digital sciences and technologies. In addition, the CERNA formulated various recommendations to researchers working in the field of machine learning. These recommendations are aimed at avoiding discrimination and bias while promoting fairness and explainability. In 2018, the CERNA published another report that makes various suggestions regarding the use of AI in healthcare.<sup>37</sup> In particular, the CERNA suggests that any future law on bioethics provide for guaranteed human intervention in the medical process and clarifies the methods to obtain patients' consent for using algorithmic treatment.

In 2017, the government entrusted the INRIA with the task of launching a new platform dedicated to the development of transparency and accountability of algorithms. The Transalgo platform<sup>38</sup> promotes ethics and transparency and gives information about how data collection works or how algorithmic discrimination can be assessed.

### 1.1.6 Judiciary

Another relevant stakeholder is the judiciary, which may have to deal with concrete cases on the use of AI and algorithmic decision-making. The Constitutional Council, the administrative courts and the civil courts have all already dealt with cases in which they had to review the compatibility of algorithm-based decision-making with the right to a fair trial and principles of transparency.

The **Constitutional Council** is a court vested with the power to review the constitutionality of legislation. It is not a supreme court that would be hierarchically superior to the Council of State (*Conseil d'État*) or the Court of Cassation (*Cour de Cassation*). The Constitutional Council verifies the constitutionality of the laws voted in parliament prior to promulgation. The Constitutional Council can also receive complaints

<sup>36</sup> Research Ethics Board of Allistene, 'Research Ethics in Machine Learning, CERNA Report' (Allistene, the Digital Sciences and Technologies Alliance, February 2018).

<sup>37</sup> Allistene, 'Numérique & Santé: Quels Enjeux Éthiques Pour Quelles Régulations? CERNA Report' (Allistene, the Digital Sciences and Technologies Alliance, 19 November 2018).

<sup>38</sup> Transalgo, 'Transalgo: Plateforme scientifique pour le développement e la transparence et de la redevabilité des algorithmes et des données', accessed 18 March 2020, <https://www.transalgo.org/>.



challenging the constitutionality of laws that are already promulgated. Such complaints are called “applications for a priority preliminary ruling on the issue of constitutionality” and are transmitted by the Council of State or the Court of Cassation. Within this framework, the Constitutional Council has rendered three main decisions relating to AI.

- Decision n°2018-765 DC of 12 June 2018 dealt with the [law n° 2018-493 of June 20 2018](#), which extended the cases in which a decision having legal effects specifically or significantly affecting a person may be made using automated processing of personal data.<sup>39</sup> The Constitutional Council ruled that the new law defined the appropriate guarantees to safeguard the rights and freedoms of individuals. The council highlighted that the law provided three conditions that needed to be met to have recourse to automatic decision making: (1) the main characteristics of the algorithm must be communicated upon request; (2) the individual administrative decision must be subject to administrative recourse, and (3) no sensitive data shall be used. But the Constitutional Council also insisted that the data processor must be able to explain, in detail and in an intelligible format, to the person in question how the data processing was applied. The council concluded that algorithms likely to revise by themselves the rules that they apply cannot be used without the oversight and validation of the data processor.
- In Decision n°2019-796 DC of December 27 2019,<sup>40</sup> the Constitutional Council partially censured article 154 of the finance law for 2020, which authorizes the customs and tax administrations, on an experimental basis and for three years, to collect personal data on public websites and to process them to establish breaches and violations of French legislation. The Constitutional Council ruled that the data collection and processing carried out to establish the defect or delay of a tax return in the cases where the administration has already sent a formal notice to the taxpayer constituted a disproportionate violation of the right to privacy and the freedom of expression and communication. To establish other infringements (mostly: trading in prohibited goods, undeclared professional activity and fraudulent tax domiciliation), the provisions of art. 154 were considered as constitutional.
- On 15 January 2020,<sup>41</sup> the Council of State transmitted to the Constitutional Council a question for a priority preliminary ruling (*Question Prioritaire de Constitutionnalité*) on the constitutionality of article L. 612-3 of the *Code de l'éducation*. This provision deals with the national procedure for pre-enrolment in higher education. Candidates may request information about the application process, such as the examination criteria and the pedagogical justification

<sup>39</sup> Conseil Constitutionnel, 'Décision N° 2018-765 DC Du 12 Juin 2018: Loi Relative à La Protection Des Données Personnelles', 12 June 2018, <https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm>.

<sup>40</sup> Conseil Constitutionnel, 'Décision N° 2019-796 DC Du 27 Décembre 2019: Loi de Finances Pour 2020', 27 December 2019, <https://www.conseil-constitutionnel.fr/decision/2019/2019796DC.htm>.

<sup>41</sup> Le Conseil d'État, 'Base de jurisprudence, Decision n° 433296', 15 January 2020, <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-01-15/433296>.

for decision-making on applications. According to article L. 612-3 of the *Code de l'éducation*, access to the documents relating to the algorithmic processing used by higher education institutions to judge applications shall be restricted to applicants who make a request, after the decision concerning them has been taken, and solely for information relating to the criteria and arrangements for examining the application. Third parties may not make requests. This provision is thus being contested on the grounds that it limits applicants' ability to properly understand and evaluate the algorithms used to take decisions. On 03 April 2020<sup>42</sup>, the Constitutional Council ruled that the aforementioned provision is constitutional while making a reserve of interpretation. According to the council, higher education institutions must publish the criteria against which applications have been examined at the end of the national pre-registration procedure. The report must specify the extent to which algorithmic processing was used and respect the privacy of applicants.

The **Council of State** (*Conseil d'État*) is the highest administrative jurisdiction. It is the judge of last resort for cases relating to executive power, local authorities, independent public authorities, public administration agencies or any other agency invested with public authority. Therefore, the Council of State exercises judicial review over CNIL's and CSA's decisions. The Council of State is also responsible for the day-to-day management of the administrative tribunals and courts of appeal. The Council of State thus plays a crucial part in exercising oversight over the government, the administration and independent agencies from a jurisdictional point of view and ensures that they conform to the law. The Council of State has adopted various decisions regarding algorithmic treatments. On 04 May 2018,<sup>43</sup> the Council of State rejected the claim of a taxpayer on the basis of article 47A of the code of tax procedures (*Livre des procédures fiscales*). Article 47A of the code of tax procedures (*Livre des procédures fiscales*) lists the prerogatives and obligations of the administration in the event of a tax audit. According to the Council of State,<sup>44</sup> the tax administration must transmit to the investigated company the files used for the determination of tax increases, but the administration is not obliged to communicate the programs, materials and algorithms that were used to produce those files. In addition, the Council of State adopted a decision regarding the Parcoursup algorithm and ruled that student unions do not have the right to be informed of the criteria used by institutions of higher education in making decisions on students' applications.<sup>45</sup> However, the

<sup>42</sup> Conseil Constitutionnel, Décision 2020-834 QPC, 3 avril 2020.

<sup>43</sup> Conseil d'État, 8ème - 3ème chambres réunies, 4 mai 2018, n°410950, accessed 18 March 2020.

<sup>44</sup> Conseil d'État, 8ème - 3ème chambres réunies, 4 mai 2018, n°410950.

<sup>45</sup> Le Conseil d'État, 'Conseil d'État, 12 juin 2019, Université des Antilles, n°427916 & 427919', 12 June 2019, <https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-12-juin-2019-universite-des-antilles>.

Council of State has also highlighted that the Decree of 19 March 2019 (which is now in effect) provides that higher education institutions must release the general criteria used in their selection process. On 15 January 2020,<sup>46</sup> the Council of State transmitted to the Constitutional Council a question for a priority preliminary ruling (*Question Prioritaire de Constitutionnalité*) on the constitutionality of article L. 612-3 of the *Code de l'éducation*. The Constitutional Council adopted its decision on 03 April 2020.

The **Court of Cassation** (*Cour de cassation*) is the highest civil jurisdiction. Civil, commercial, social, and criminal cases are first tried in courts of first instance. Their decisions may be appealed before a court of appeal, which re-examines all the factual and legal aspects of the case. Decisions rendered at last resort by first-level courts and decisions delivered by courts of appeal may themselves be appealed to the Court of Cassation. The Court of Cassation is not a third level of jurisdiction: when decisions are referred to the Court of Cassation, they decide whether the rules of law have been correctly applied by the lower courts based on the facts. Civil courts are responsible for ensuring the application of consumer law and privacy rules by private actors. For example, in February 2019, the court of first instance of Paris ruled that a number of clauses contained in the Google's Terms of Use were illegal<sup>47</sup>. The decision was mainly based on consumer protection law (*article L 212-1 code de la consommation*) and on the data privacy law n°78-17 of 06 January 1978 called "*Informatique et Libertés*".

### *1.1.7 Public-private partnerships and relations between the private and public sector*

The INRIA (National Institute for Research in Computer Science and Automation) collaborates with Facebook and Microsoft via a joint research centre, which is specialised in big data and machine learning. Other partnerships on AI are also currently being launched by French research institutes. For example, the Ecole Polytechnique has concluded a partnership on AI with Fujitsu and created a Chair on "Artificial Intelligence and Visual Computing" with Google. In 2019, the Ministry of Education launched the innovation and AI partnership (*Partenariat d'innovation et intelligence artificielle - P2IA*), which aims to provide teachers with new tools of personalised learning.

On 03 July 2019, in line with the French government's AI for Humanity strategy, the Ministry of Economy and Finance and eight of France's global industry players, namely Air Liquide, Dassault Aviation, EDF, Renault, Safran, Thales, Total, and Valeo, signed a manifesto on Artificial

<sup>46</sup> Le Conseil d'État, 'Base de jurisprudence, Decision n° 433296', 15 January 2020, <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-01-15/433296>.

<sup>47</sup> Tribunal de Grande Instance de Paris, 12 février 2019, Google/ UFC Que Choisir, n°14/07224

Intelligence for Industry.<sup>48</sup> In the manifesto, the eight companies put forward a common strategic foundation for AI to establish leadership positions in their respective markets at international level. Since then, six other companies (Schlumberger, ST, Orange, Naval Group, Michelin, Saint Gobain) have joined them.<sup>49</sup> The signatories identify themes of common interest, with specific reference to the use of AI in industrial environments: trust, explainability and even certifiability; embedded systems (i.e. autonomous electronic systems used to perform a task); AI for design, simulation, development, testing and logistics; AI for maintenance and Industry 4.0; as well as issues related to very high performance, reliability, robustness, and more generally the use of AI in critical systems. The companies call for coordinated action, first by industry players, but also by the academic community and policymakers. The signatories have agreed to conduct a joint review to share findings with policymakers and to establish a coordinated plan of action with the French AI ecosystem. They also intend to encourage the participation of all public and private stakeholders who share this common strategic vision of AI. Through this manifesto, industrial signatories seek to develop a collective response to the need for sovereign AI capabilities in terms of both economic sovereignty (technological independence of French companies operating internationally) and national sovereignty (one of the four priorities identified in the Villani report). In this respect, on 6 February 2020, Thalès, EDF and Total announced a joint AI lab that will develop AI technologies adapted to industrial needs.<sup>50</sup>

### 1.1.8 Civil society

Civil society is well-organised in France and often engages in consultations with the government on new policies and regulation (including technological policies) or in strategic litigation. Examples of organisations that are particularly active in the field of AI, big data and fundamental rights are the following non-profit organisations: IA pour l’Ecole, Association française pour l’IA, and France is AI. A few associations are particularly active in the promotion of public freedoms and the protection of transparency and privacy, like “*La Quadrature du Net*”<sup>51</sup> or even the website “NextInpact”.<sup>52</sup> For example, *La Quadrature du Net* has brought various proceedings to protect privacy and civil liberties. In 2018, *La Quadrature du Net* filed a civil claim before the

<sup>48</sup> Reuters, ‘Huit industriels unissent leurs efforts dans l’IA’, *Reuters*, 3 July 2019, <https://fr.reuters.com/article/topNews/idFRKCN1TY28G-OF RTP>.

<sup>49</sup> Marion Garreau, ‘EDF, Thales et Total ouvrent un laboratoire commun en IA - Technos et Innovations’, *Usine Nouvelle*, 7 February 2020, <https://www.usinenouvelle.com/editorial/edf-thales-et-total-ouvrent-un-laboratoire-commun-en-ia.N927479>.

<sup>50</sup> Air Liquide et al., ‘Manifeste Pour l’intelligence Artificielle Au Service de l’industrie: Les Industriels Français Engagés Dans l’intelligence Artificielle’, 3 July 2019.

<sup>51</sup> ‘*La Quadrature Du Net*’, accessed 18 March 2020, <https://www.laquadrature.net>.

<sup>52</sup> nextinpact.com, ‘Next INpact - Actualités informatique et numérique au quotidien’, accessed 18 March 2020, <https://www.nextinpact.com>.

CNIL on the behalf of 12,000 individuals against Google, Apple, Facebook, Amazon and LinkedIn for not complying with GDPR.<sup>53</sup> As a result, Google was fined by the CNIL on January 2019.<sup>54</sup> Another claim was filed before the Marseille administrative court against the experiment of facial recognition in two high schools.<sup>55</sup> This experiment was interrupted in November 2019 after the CNIL's Opinion was released (see below). In July 2019, *La Quadrature du Net* brought a new proceeding before the Council of State to contest the legality of the decree that authorized the ALICEM identification system.<sup>56</sup> This litigation is still pending. In January 2020, *La Quadrature du Net* and *La Ligue des Droits de l'homme* introduced an application for interim measures against the video surveillance project of the city of Marseille ("SafeCity") which was rejected by the administrative court.<sup>57</sup>

### 1.1.9 Business associations

The main business associations dealing with AI are the Association pour le Commerce et les Services en Ligne (ACSEL)<sup>58</sup> and the "Hub France IA", which gathers major groups like Air Liquide, Air France, SNCF and Société Générale.<sup>59</sup> In addition, in March 2018, in the wake of the AI for Humanity summit, 30 companies created the "Impact AI" collective,<sup>60</sup> which was created by 30 companies in 2019. The collective comprises of 48 companies and has created four working groups. The first working group created an AI Observatory to assess the perception of AI in France. The second working group aims to federate its members' initiatives in the field of responsible AI.

## 1.2 International relations

<sup>53</sup> La Quadrature du Net, 'Données personnelles', accessed 18 March 2020, [https://www.laquadrature.net/donnees\\_perso/](https://www.laquadrature.net/donnees_perso/).

<sup>54</sup> CNIL, 'Délibération de La Formation Restreinte N° SAN – 2019-001 Du 21 Janvier 2019 Prononçant Une Sanction Pécuniaire à l'encontre de La Société GOOGLE LLC'.

<sup>55</sup> La Quadrature du Net, 'Reconnaissance faciale: un recours pour faire barrage à la surveillance biométrique', 19 February 2019, <https://www.laquadrature.net/2019/02/19/reconnaissance-faciale-un-recours-pour-faire-barrage-a-la-surveillance-biometrique/>.

<sup>56</sup> La Quadrature du Net, 'La Quadrature du Net attaque l'application ALICEM, contre la généralisation de la reconnaissance faciale', 17 July 2019, <https://www.laquadrature.net/2019/07/17/la-quadrature-du-net-attaque-lapplication-alicem-contre-la-generalisation-de-la-reconnaissance-faciale/>.

<sup>57</sup> La Quadrature du Net, 'Safe City à Marseille: Premier recours contre la vidéosurveillance automatisée', 20 January 2020, <https://www.laquadrature.net/2020/01/20/safe-city-a-marseille-premier-recours-contre-la-videosurveillance-automatisee-de-lespace-public/>.

<sup>58</sup> Aysel, 'L'association de l'économie numérique', accessed 20 March 2020, <https://www.acsel.eu/>.

<sup>59</sup> Accueil, 'Hub France IA', accessed 20 March 2020, <https://www.hub-franceia.fr/>.

<sup>60</sup> 'Impact AI', accessed 20 March 2020, <http://impact-ai.fr/>.

### 1.2.1 General strategy

In February 2019, the Ministry of Economy published a report entitled “Artificial intelligence: state of the art and prospects for France” ([Intelligence artificielle: état de l’art et perspectives pour la France](#)). According to this report, France has two options: either to become an international leader in AI or to create a niche by focusing on a particular type of use of AI. For the moment, the French government has decided to invest massively in AI projects. The French President has also expressed its wish to collaborate with the EU to develop a common strategy on AI.

### 1.2.2 European linkages – Council of Europe and OECD

In May 2019, France, as a member of the OECD, approved the [OECD Council Recommendation on Artificial Intelligence](#) and adopted the [OECD AI Principles](#).

Regarding the Council of Europe, France announced during the French Presidency of the Committee of Ministers of the Council of Europe (17 May – 27 November 2019) that the issues of digital technology and artificial intelligence would be examined, which also led to the establishment of the Ad Hoc Committee on Artificial Intelligence ([CAHAI](#)) by the Committee of Ministers of the Council of Europe.

### 1.2.3 International linkages – G20

In 2018, just before the G7 summit, France and Canada announced a new initiative called **Global Partnership on AI (GPAI)** or *Groupe International d’experts en IA (G2IA)*.<sup>61</sup> This international expert group supports the responsible development of artificial intelligence with regard to human rights, inclusion, diversity, innovation and economic growth. The GPAI is meant to represent a global reference on AI that will promote international cooperation and coordination in the development of public policies related to AI. In October 2019, during the second “AI for Humanity” summit in Paris,<sup>62</sup> the French President

---

<sup>61</sup> See: Ministère de l’Europe et des Affaires étrangères, ‘Déclaration franco-canadienne sur l’intelligence artificielle’, France Diplomatie - Ministère de l’Europe et des Affaires étrangères, 7 June 2018, <https://www.diplomatie.gouv.fr/fr/dossiers-pays/canada/rerelations-bilaterales/evenements/article/declaration-franco-canadienne-sur-l-intelligence-artificielle-07-06-18>; G7, ‘Annexe B: Déclaration Des Ministres de l’Innovation Du G7 Au Sujet de l’intelligence Artificielle’, 18 March 2018, <http://www.g8.utoronto.ca/employment/2018-labour-annex-b-fr.html>; and Gouvernement du Canada, ‘Vision commune de charlevoix sur l’avenir de l’intelligence artificielle’, AMC, 20 February 2020, [https://www.international.gc.ca/world-monde/international\\_relations-reactions\\_internationales/g7/documents/2018-06-09-artificial-intelligence-artificielle.aspx?lang=fra](https://www.international.gc.ca/world-monde/international_relations-reactions_internationales/g7/documents/2018-06-09-artificial-intelligence-artificielle.aspx?lang=fra).

<sup>62</sup> Institut de France, ‘Global Forum on AI for Humanity, Quai Conti, Preliminary Program Outline’ (Paris: Institut de France, October 2019).

announced the creation of two centres of expertise on AI in France and in Canada.<sup>63</sup>

As a member of the G20, France is part of its various initiatives taken in the field of AI. More specifically, in June 2019, the G20 Trade and Digital Economy Ministers outlined the G20's commitment to a human-centred approach to AI, guided by a series of G20 AI Principles.<sup>64</sup> The Principles have a non-binding nature and are drawn from the [OECD Recommendation on AI](#) (adopted in May 2019), therefore underlining the need for inclusive growth, sustainable development and well-being, human-centred values and fairness, transparency and explainability, robustness, security and safety, and accountability.

### 1.3 National strategies and guidelines

In an old and well-known report written in 1978 on the "computerization of society",<sup>65</sup> French experts were concerned about issues of national sovereignty. Today, the major part of the discussion lies in ethical aspects. The priority given to ethics is noticeable in the CNIL report of 2017 and the Villani report of 2018, which paved the way for the governmental strategy announced in 2018.

#### 1.3.1 The CNIL Report

In 2016, the Digital Republic Law n° 2016-1321 of 7 October 2016 entrusted to the CNIL a "reflection on the ethical problems and the questions of society raised by the evolution of digital technologies".<sup>66</sup> The CNIL thus produced a report on the deployment of algorithms and artificial intelligence from an ethical perspective,<sup>67</sup> which was released in December 2017. The report insisted on the difficulty of defining AI and adopted a broad definition that includes all kinds of algorithms with a focus on machine learning.<sup>68</sup> The report began with a review of the major difficulties posed by the development of AI, such as the increasing delegation of tasks or decisions to machines, the discriminatory effect

<sup>63</sup> Élysée, 'Clôture du Global Forum on Artificial Intelligence for Humanity par le Président Emmanuel Macron', 30 October 2019, <https://www.elysee.fr/emmanuel-macron/2019/10/30/cloture-du-global-forum-on-artificial-intelligence-for-humanity-par-le-president-emmanuel-macron>.

<sup>64</sup> OECD, '2019 G20 Leaders' Summit - Digital (AI, Data Governance, Digital Trade, Taxation)', 28 June 2019, <https://www.oecd.org/about/secretary-general/2019-g20-leaders-summit-digital-osaka-june-2019.htm>.

<sup>65</sup> Simon Nora and Alain Minc, 'L'informatisation de La Société', Rapport Au Président de La République (Paris, May 1978).

<sup>66</sup> 'LOI N° 2016-1321 Du 7 Octobre 2016 Pour Une République Numérique', 2016-1321 § (2016).

<sup>67</sup> CNIL, 'Comment permettre à l'Homme de garder la main? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle', 15 December 2017, <https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de>.

<sup>68</sup> CNIL, 'Comment permettre à l'Homme de garder la main?', 16.

of algorithms, the dangers of profiling and personalization, the protection of personal data and individual freedom, the complexity of data selection, and the emergence of a new category of autonomous machines that are in some ways similar to humans. The report highlighted two founding principles to “put artificial intelligence at the service of humans”: loyalty and vigilance. The principle of loyalty implies that any algorithm, whether or not it deals with personal data, must be loyal towards users as consumers, citizens, and community members. The principle of “continued attention and vigilance” means that all stakeholders involved in “algorithmic chains” need to be aware of potential unforeseen consequences, particularly because of the unpredictable nature of AI, which is inherent to machine learning. Designers, businesses and citizens should all be involved in concrete procedures to implement this principle of vigilance (ethics committees, for example). The CNIL added six policy recommendations for the benefit of public authorities and the civil society: all the actors of the AI ecosystem should be trained in ethics; the interpretability and auditability of AI systems (to counter the “black box” effect) should be improved; a national platform in charge of auditing algorithms should be set up; research on ethical AI should be encouraged; and ethics functions within private companies should be strengthened. It is interesting to note that the CNIL underlined the possibility of the emergence of a new generation of guarantees and fundamental rights that would be specific to the digital age and would organise the global governance of our digital world.

### *1.3.2 The Villani Report*

In 2017, the previous government released the [France intelligence artificielle report](#). Following the 2017 elections, the mathematician and Member of Parliament Cédric Villani was tasked by the Prime Minister with examining France’s strategy on artificial intelligence. The Villani report is entitled “[For a meaningful artificial intelligence: towards a French and European strategy](#)”<sup>69</sup> and was submitted in March 2018. This report did not provide a very precise definition of AI but adopted a large and inclusive approach. The report not only considered the question of the development of artificial intelligence from the perspective of economic and innovation policies, but also focused on considering AI as a vector of human and social progress, for example by addressing the different ways in which humans and intelligent systems can complement each other. Primary [themes](#) of the Villani Report were: (1) developing a data-focused economic policy to improve access to data, (2) targeting four strategic sectors (healthcare, environment, transport, and defence), (3) boosting the potential of French research (4) planning for the impact of AI on labour, (5) making AI more environmentally friendly, (6) opening up the black boxes of AI, and (7) ensuring that AI supports inclusivity and diversity. Ethics are very present in the report, which

---

<sup>69</sup> Villani, Cédric, ‘Donner Un Sens à l’intelligence Artificielle: Pour Une Stratégie Nationale et Européenne’, 2018.



suggests investing heavily in research on the explicability of algorithms, to set up an ethics committee for digital technology and AI (on the model of the National Consultative Committee on Ethics – CCNE) and to create a strong link between ethics and software design. While the report discussed some legal issues, such as the rights of individuals over their data, it also highlighted that law cannot do everything.

### 1.3.3 The French National Strategy on AI: AI for Humanity

In March 2017, the previous French government presented a first version of its strategy for AI in a report entitled "[#France IA](#)".<sup>70</sup> In 2018, one day after the Villani report was released, the President of France presented the country's strategy in the field of artificial intelligence at the "[AI for Humanity](#)" conference in Paris and announced that a €1.5 billion budget would be allocated to this strategy.<sup>71</sup> The national strategy is largely based on recommendations from the Villani report and focuses on four major challenges:

- Reinforcing the AI ecosystem by setting up a national AI program coordinated by the *Institut National pour la Recherche en Informatique et Automatique* (INRIA), by doubling the number of students with training in AI, by strengthening synergies between public research and industry (with researchers devoting 50% of their time to working in companies as compared to 20% nowadays), by creating individual research chairs to attract the best researchers, and by launching calls for proposals to attract the best research projects.
- Developing an open data policy (especially in the healthcare sector) by continuing to open up public data, by supporting the creation of public and private data exchange platforms, by developing a European framework for the protection of personal data and by creating a health data hub controlled by the National Institute for Health Data (*Institut National des données de santé – INDS*).
- Creating a regulatory and financial framework favouring the emergence of "AI champions" by supporting AI research projects and start-ups (1.5 billion euros) by reforming existing regulations to address new issues, such as driverless vehicles, by the creation of a "European DARPA",<sup>72</sup> and by using AI to improve public policies, for example on lifelong learning, the anticipation of needs, individualisation of learning pathways, et cetera.

<sup>70</sup> Gouvernement français, France IA, '[#FranceIA: Une Stratégie Pour La France En Matière d'Intelligence Artificielle](#)', March 2017, 5. This report defines AI as "a set of concepts inspired by human cognition or by the biological brain, and intended to assist or supplement the individual in the processing of massive information."

<sup>71</sup> The "AI for Humanity" website states that "Defining artificial intelligence (AI) is not easy. The field is so vast that it cannot be restricted to a specific area of research: it is more like a multidisciplinary programme. Originally, it sought to imitate the cognitive processes of human beings. Its current objectives are to develop automatons that solve some problems better than humans, by all means available".

<sup>72</sup> On the model of the US Defense Advanced Research Projects Agency. See: 'Defense Advanced Research Projects Agency', accessed 20 March 2020, <https://www.darpa.mil/>.

- Reviewing AI regulation and ethics to make sure that the very best standards of acceptability for citizens are respected, supporting humanities research about AI, disclosing all the algorithms used by the French administration, and encouraging diversity.

#### 1.3.4 The implementation of the AI for Humanity national strategy

- **Research.** The first “steering committee” on the national AI strategy took place in November 2018. Two ministers presented a detailed approach to the research part of the plan. They announced that €665 million would be made available by 2022 (60% from government and 40% from external investment). A budget of €70 million was granted to the creation of 200 research chairs, mostly at [INRIA](#) and the [National Research Agency](#) (CNRS). The government also decided to favour four promising ecosystems called 3IA’s (Interdisciplinary Institute for Artificial Intelligence). Four 3IA institutes – Grenoble, Nice, Paris, and Toulouse – were chosen to become interdisciplinary institutes on Artificial Intelligence. They share a sum of € 100 million from the *AI for Humanity* budget and will receive another €300 million from public-private funds. €60 million were set aside for public-private laboratories, so called “labcoms”. A supercomputer, worth €115 million, with a processing power of over 10 Petaflops, should be installed at the “plateau de Saclay” hub and is meant to be functional in 2020.
- **Defence.** On 05 April 2019, the Minister of Armed Forces presented the new strategy for artificial intelligence and defence.<sup>73</sup> The French approach advocates a responsible and controlled use of artificial intelligence in the defence sector. €100 million will be invested every year, for example in planification, cyberspace, logistics, and intelligence. The minister also announced a special committee that will focus on the ethical issues related to the use of AI in defence. In September 2019, the ministry’s task force on AI released a report which presents the ministry’s roadmap on AI (see [Rapport de la Task Force IA](#)).<sup>74</sup>
- **Economy.** On 3 July 2019, the government presented the economic part of the national strategy for AI. This [plan](#) insists on three priorities: implementing a French offer in AI, making AI accessible to all businesses, as well as developing a French and European data economy. The government launched a call for applications named “AI

<sup>73</sup> Florence Parly, ‘Discours de Florence Parly, ministre des Armées\_Intelligence artificielle et défense’, 5 April 2019, [https://www.defense.gouv.fr/english/salle-de-presse/discours/discours-de-florence-parly/discours-de-florence-parly-ministre-des-armees\\_intelligence-artificielle-et-defense](https://www.defense.gouv.fr/english/salle-de-presse/discours/discours-de-florence-parly/discours-de-florence-parly-ministre-des-armees_intelligence-artificielle-et-defense).

<sup>74</sup> Cabinet de la ministre des Armées, ‘Communiqué: Publication du rapport du ministère des Armées sur l’intelligence artificielle’, 20 December 2019, [https://www.defense.gouv.fr/salle-de-presse/communiqués/communiqué\\_publication-du-rapport-du-ministere-des-armees-sur-l-intelligence-artificielle](https://www.defense.gouv.fr/salle-de-presse/communiqués/communiqué_publication-du-rapport-du-ministere-des-armees-sur-l-intelligence-artificielle).

Challenges<sup>75</sup> whose objective is to encourage French companies to develop artificial intelligence projects, mostly by connecting providers and users of AI. The government also wants to improve data sharing between administrations and companies. On the same day, in line with the French government's AI for Humanity strategy, the Ministry of Economy and Finance and eight of France's global industry players (Air Liquide, Dassault Aviation, EDF, Renault, Safran, Thales, Total and Valeo) signed a manifesto on Artificial Intelligence for Industry (see above).

## 1.4 Standards and voluntary guidelines; the role of the private sector

### 1.4.1 Government standards and guidelines

In France, it is mainly the CNIL that develops good practices and recommendations regarding data processing and artificial intelligence (see above). For example, the CNIL has very recently released a report that includes guidelines on facial recognition.<sup>76</sup>

### 1.4.2 Self-regulation in the private sector

While AI is used by many companies in France (57.4% of the companies surveyed by ACSEL) only 29.8% of those respondents have established rules of conduct or an internal usage charter.<sup>77</sup> 39.4% had been considering whether to do so. Among those who did, half of their guidelines deal with data protection and GDPR compliance, and 16.7% of the rules are related to algorithmic design. 34.4% of the interviewees did not know what the guidelines are for. The first official ethical charter adopted by a major group is Thales' charter. Thales has also undertaken not to manufacture [killer robots](#).

### 1.4.3 Standards organizations

The French Association for Standardization (Association Française de Normalisation- AFNOR)<sup>78</sup> is an association created in 1926. It is made up of nearly 2,500 member companies and works under the supervision

---

<sup>75</sup> Direction Générale des Entreprises, 'Challenges IA - Appel à manifestation d'intérêts Sponsors – vague 2', Direction Générale des Entreprises (DGE), 26 November 2020, <https://www.entreprises.gouv.fr/numerique/challenges-ia-appel-a-manifestation-d-interets-sponsors-vague-2>.

<sup>76</sup> CNIL, 'Reconnaissance Faciale: Pour Un Débat à La Hauteur Des Enjeux'.

<sup>77</sup> Stéphanie Marius, 'IA: seule 1 entreprise sur 3 a mis en place une charte éthique d'usage', <https://www.ecommercemag.fr/>, 31 January 2019, 1, [https://www.ecommercemag.fr/Thematique/data-room-1223/Breves/seule-entreprise-mis-place-charte-ethique-usage-336978.htm#&utm\\_source=social\\_share&utm\\_medium=share\\_button&utm\\_campaign=share\\_button](https://www.ecommercemag.fr/Thematique/data-room-1223/Breves/seule-entreprise-mis-place-charte-ethique-usage-336978.htm#&utm_source=social_share&utm_medium=share_button&utm_campaign=share_button).

<sup>78</sup> <https://www.afnor.org/>

of the Ministry of Economy. AFNOR's mission is to lead and coordinate the entire standards development process in conjunction with the 25 French standards offices (BN) and to promote the use of standards by businesses as well as to develop the certification of products and services. It represents France at the International Standards Organization (ISO) and the European Committee for Standardization (CEN). Since 01 January 2014, it has also been a member of the European Committee for Standardization in Electronics and Electrotechnics (CENELEC) and of the International Electrotechnical Commission (IEC). AFNOR publishes the collection of NF standards.

Insofar as standardisation work has been carried out at the international level (ISO) to meet the challenges of artificial intelligence (robustness of solutions, regulation, ethics, etc.), AFNOR has set up a standardisation commission on this subject, whose work has not yet been completed<sup>79</sup>. In April 2018, the AFNOR published a white paper on the subject.<sup>80</sup>

## 1.5 Sample recent developments

### 1.5.1 Facial recognition

The government's facial recognition application, [Alicem](#) (*Authentification en ligne certifiée sur mobile*) was authorized by a [decree](#) in May 2019.<sup>81</sup> Alicem is a mobile application developed by the Ministry of Internal Affairs and the National Agency for Secure Securities (*Agence Nationale des Titres Sécurisés*). The application will allow users to prove their identity with their phone so that online administrative processes will be simplified. The application will provide access to 500 public services, like tax administration services, social security, or the services in charge of identity cards and driving licences. For now, Alicem – which does not require an AI technology – is still being tested but should be operational in 2020.<sup>82</sup> In July 2019, a recourse against the decree authorizing the use of the ALICEM technology was brought before the Council of State by *La Quadrature du Net* and is still pending at the time of writing the

<sup>79</sup> <https://normalisation.afnor.org/actualites/intelligence-artificielle-lapport-precieux-normes-volontaires/>

<sup>80</sup> [https://marketing.afnor.org/livre-blanc/intelligence-artificielle?\\_ga=2.235853633.1574016842.1591109860-1221974353.1591109860](https://marketing.afnor.org/livre-blanc/intelligence-artificielle?_ga=2.235853633.1574016842.1591109860-1221974353.1591109860)

<sup>81</sup> Legifrance.gouv.fr, 'Décret N° 2019-452 Du 13 Mai 2019 Autorisant La Création d'un Moyen d'identification Électronique Dénommé "Authentification En Ligne Certifiée Sur Mobile"', 8 February 2020, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000038476730&dateTexte=20200208>.

<sup>82</sup> Le Figaro and AFP, 'Identité numérique: l'État espère mettre en service son service Alicem en 2020', Le Figaro.fr, 19 February 2019, <https://www.lefigaro.fr/identite-numerique-l-etat-espere-mettre-en-service-son-service-alicem-en-2020-20200219>.

report.<sup>83</sup> The main argument of the plaintiff is the fact that users are not given the freedom to choose because ALICEM is the only way to create a valid digital identity to access online administrative services. According to *La Quadrature du Net*, an alternative system should be offered to users that reject facial recognition. This argument was also raised by the CNIL before the decree was adopted.<sup>84</sup>

In December 2019, the French ministry of digital affairs announced that the French government wants to experiment with the use of facial recognition in public spaces.<sup>85</sup> Facial recognition should be tested on the basis of the participants' consent for a period of six to 12 months.

The Région PACA (*Provence Alpes Côtes d'Azur*) has decided to carry out an experiment by using automatic facial recognition at the entrance of two high schools in Nice and Marseille. This project is based on biometrics and conducted in partnership with Cisco. Despite the fact that various organizations (*Quadrature du net*, *Ligue des droits de l'Homme*, *FCPE CGT Educ*) filed a recourse before the Marseille administrative court against the *Région's* decision,<sup>86</sup> the experiment started in January 2019. The Région decided to seek advice from the CNIL, and an impact analysis on possible privacy breaches was submitted to the CNIL in July 2019. On 17 October 2019, the plenary assembly of the CNIL issued an opinion stating that this scheme failed to comply with the principles of proportionality and data minimisation laid down in the GDPR (General Data Protection Regulation).<sup>87</sup> The experiment was stopped.

---

<sup>83</sup> La Quadrature du Net, 'La Quadrature du Net attaque l'application ALICEM, contre la généralisation de la reconnaissance faciale'.

<sup>84</sup> CNIL, 'Délibération N° 2018-342 Du 18 Octobre 2018 Portant Avis Sur Projet de Décret Autorisant La Création d'un Traitement Automatisé Permettant d'authentifier Une Identité Numérique Par Voie Électronique Dénommé "Application de Lecture de l'identité d'un Citoyen En Mobilité" (ALICEM) et Modifiant Le Code de l'entrée et Du Séjour Des Étrangers et Du Droit d'asile Demande d'avis N° 18008244' (2019).

<sup>85</sup> Carolin Piquet, 'Reconnaissance faciale: Cédric O n'est "pas certain" qu'Alicem soit un jour déployée', *leparisien.fr*, 24 December 2019, <http://www.leparisien.fr/high-tech/reconnaissance-faciale-cedric-o-n-est-pas-certain-qu-alicem-soit-un-jour-deployee-24-12-2019-8223705.php>.

<sup>86</sup> La Quadrature du Net, 'Reconnaissance faciale'.

<sup>87</sup> CNIL, 'Expérimentation de La Reconnaissance Faciale Dans Deux Lycées: La CNIL Précise Sa Position', 29 October 2019, <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>.

Various *collectivités locales*, like the *département* of Yvelines<sup>88</sup> and the cities of Nice,<sup>89</sup> Valenciennes,<sup>90</sup> Toulouse,<sup>91</sup> and Nîmes<sup>92</sup> are currently developing smart video surveillance systems.<sup>93</sup> These video surveillance systems<sup>94</sup> are composed of digital cameras designed with built-in algorithms. Microphones can be added to them, which are themselves equipped with intelligent software. These tools can be used to detect intruders, locate abandoned luggage, count cars, or even find an individual based on a detail (like the colour of a jacket). In Marseille, the video surveillance project is called "SafeCity" and was contested by *La Quadrature du Net* and *La Ligue des Droits de l'homme*. Both associations introduced an application for interim measures but their request was rejected by the administrative court.<sup>95</sup> Another claim on the same issue has been recently introduced.<sup>96</sup> Another example is the city of Nice that has decided to test facial recognition during major events. During the 2019 carnival, the Anyvision software scanned 5,000 faces and recognized the volunteers who had provided a passport photo.<sup>97</sup> In addition, the City of Nice launched a "Safe City" project in June 2018, which is a three-year experiment with Thales, combining video surveillance, internet of things technology and data analytics. The City of Nice has also decided to work on security in public transportation by

<sup>88</sup> Damien Guimier, 'Yvelines - Malgré quelques embûches, le dispositif départemental de vidéoprotection est lancé', *La Gazette de Saint-Quentin-en-Yvelines*, 12 February 2019, <https://lagazette-sqy.fr/2019/02/12/votreville/yvelines/malgre-quelques-embuches-le-dispositif-departemental-de-videoprotection-est-lance/>.

<sup>89</sup> Nice Matin, 'Plus de 100 nouvelles caméras de vidéosurveillance par an: la Police municipale de Nice bat des records', 9 September 2019, <https://www.nicematin.com/faits-divers/plus-de-100-nouvelles-cameras-de-videosurveillance-par-an-la-police-municipale-de-nice-bat-des-records-411210>.

<sup>90</sup> La Voix Du Nord, 'Faut-il s'inquiéter des caméras de vidéo surveillance chinoises, et gratuites, dont est équipée la ville de Valenciennes?', *La Voix du Nord*, 13 January 2020, <https://www.lavoixdunord.fr/694140/article/2020-01-13/valenciennes-des-cameras-intelligentes-et-chinoises-gain-ou-menace>.

<sup>91</sup> Philippe Emery, 'Toulouse: le pouvoir des caméras de vidéosurveillance', *ladepeche.fr*, 3 January 2019, <https://www.ladepeche.fr/article/2019/01/03/2934369-toulouse-le-pouvoir-des-cameras.html>.

<sup>92</sup> Midi Libre, 'Vidéosurveillance à Nîmes: "Il y a nécessité d'alerter les citoyens"', *midilibre.fr*, 4 June 2019, <https://www.midilibre.fr/2019/06/04/videosurveillance-a-nimes-il-y-a-necessite-dalerter-les-citoyens,8236621.php>.

<sup>93</sup> Grégoire Allix, 'Comment des villes "hyper connectées" contrôlent l'espace public', *Le Monde.fr*, 19 December 2018, [https://www.lemonde.fr/economie/article/2018/12/19/au-nom-de-la-smart-city-des-ville-sous-surveillance\\_5399527\\_3234.html](https://www.lemonde.fr/economie/article/2018/12/19/au-nom-de-la-smart-city-des-ville-sous-surveillance_5399527_3234.html).

<sup>94</sup> Jordan Pouille, « Comment la vidéosurveillance « intelligente » s'impose dans les villes françaises », *La Vie*, 13 March 2020 [http://www.lavie.fr/actualite/france/comment-la-videosurveillance-intelligente-s-impose-dans-les-ville-francaises-11-03-2020-104578\\_4.php](http://www.lavie.fr/actualite/france/comment-la-videosurveillance-intelligente-s-impose-dans-les-ville-francaises-11-03-2020-104578_4.php)

<sup>95</sup> La Quadrature du Net, 'Safe City à Marseille'.

<sup>96</sup> Corentin Bechade, 'Marseille garde sa "vidéoprotection intelligente"... pour le moment.', 23 January 2020, <https://www.lesnumeriques.com/vie-du-net/la-videoprotection-intelligente-a-marseille-attaquee-par-deux-associations-n146335.html>.

<sup>97</sup> Jamal El Hassani, 'Expérimentation de reconnaissance faciale: Nice ravie, la Cnil sceptique', 28 August 2019, <https://www.journaldunet.com/economie/services/1443319-reconnaissance-faciale-nice-ravie-la-cnil-sceptique/>.

using the Two I<sup>98</sup> application. This app can assess the presence and number of women in the tramway or the presence of people in wheelchairs or bicycles in a street or a neighbourhood. The app is also capable of detecting people's stress or anxiety by image recognition.

### *1.5.2 Tax fraud anticipation system*

Article 154 of the financing law for 2020 allows tax and customs authorities to collect massive amounts of public data on social networks (such as Facebook, Snapchat or Instagram) or online sales platforms (such as LeBonCoin) to combat fraud as part of a three-year experiment. This provision was adopted in December. For now, the customs and tax authorities can process the data they already possess<sup>99</sup> in compliance with the Data Protection Act and under the control of the CNIL.<sup>100</sup> These data mainly come from the various mandatory declarations imposed on taxpayers, employers, social security beneficiaries, and insured persons who have concluded an insurance contracts. But article 154 provides for the massive extraction of public data on social networks and their processing using algorithms to detect fraud. However, only three areas are targeted by the government: (fake) tax domiciliation abroad, illegal businesses (such as illegal tobacco sales on Facebook) and hidden professional activities (such as undeclared work). The CNIL released its [opinion](#)<sup>101</sup> on this project in September and highlighted that the proposed processing operations are likely to infringe the rights and freedoms of the data subjects. In the Decision n°2019-796 DC of 27 December 2019 (see above §1.1.6),<sup>102</sup> the Constitutional Council partially censured article 154 of the finance law for 2020 and ruled that the data collection and processing carried out to establish the defect or delay of a tax return in cases where the administration has already sent a formal notice to the taxpayer is a disproportionate violation of the right to privacy and the freedom of expression and communication. The provisions of article 154 were considered as constitutional when applied in order to establish the other offences targeted by the law (mostly: trading in prohibited goods, undeclared professional activity and fraudulent tax domiciliation).

<sup>98</sup> Two-i, 'Video Content Analytics Equipped with AI and Machine Learning', accessed 20 March 2020, <https://two-i.com/>.

<sup>99</sup> JORF n°0055 du 6 mars 2014 page 4903 and texte n° 34, 'Arrêté Du 21 Février 2014 Portant Création Par La Direction Générale Des Finances Publiques d'un Traitement Automatisé de Lutte Contre La Fraude Dénommé "Ciblage de La Fraude et Valorisation Des Requêtes"' (2014).

<sup>100</sup> Commission Nationale de l'Informatique et des Libertés, 'Délibération N° 2014-045 Du 30 Janvier 2014 Portant Avis Sur Un Projet d'arrêté Portant Création Par La Direction Générale Des Finances Publiques d'un Traitement Automatisé de Lutte Contre La Fraude Dénommé "Ciblage de La Fraude et Valorisation Des Requêtes" (Demande d'avis N° 1726052)', 2014-045 § (2014); and Délibération n° 2016.

<sup>101</sup> Commission Nationale de l'Informatique et des Libertés, 'Délibération N° 2019-114 Du 12 Septembre 2019 Portant Avis Sur Le Projet d'article 9 Du Projet de Loi de Finances Pour 2020' (2019).

<sup>102</sup> Conseil Constitutionnel, 'Décision N° 2019-796 DC Du 27 Décembre 2019: Loi de Finances Pour 2020'.

### 1.5.3 Healthcare applications

Between August and October 2019, [two Parisian hospitals tested Gi Genius](#). This Gi Genius device is based on artificial intelligence to automatically detect and report, in real time, any anomaly related to colorectal polyps. This project is part of the AP-HP strategy regarding the use of AI in diagnosis and care. The AP-HP Health Data Warehouse (*Entrepôt de données de santé - EDS*)<sup>103</sup> collects administrative and medical data from more than 8 million patients treated within the 39 AP-HP facilities. The EDS is the first secure health data platform to benefit from an authorization from the CNIL.<sup>104</sup> Recently, the Valenciennes Hospital announced the use of a new AI application that predicts the number of patients that is likely to appear in their emergency ward.<sup>105</sup>

In addition, the French government decided, in November 2019,<sup>106</sup> pursuant to the Law n°2019-774 of 24 July 2019 on the organisation and transformation of the health system (Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé), to create a new database called the "Health Data Hub".<sup>107</sup> The Health Data Hub is a public interest group (Groupement d'Intérêt Public-GIP) formed between the state; organisations representing patients and users of the health system; producers of health data; and public and private users of health data, including health research organisations. The objective of the Health Data Hub is to ensure centralized access to health data by interconnecting the different databases. It is meant to replace the National Health Data System (Système National des Données de Santé), which contains data on health insurance, hospital billings, medical causes of death, medico-social data on the disabled and some reimbursement data from complementary organisations. Eventually, any data collected as part of a procedure reimbursed by the French Social Security will be centralized in the Health Data Hub. The aim is to make data available in order to enable the development of preventive, diagnostic and therapeutic projects based on AI. This Health

<sup>103</sup> Assistance Publique: Hôpitaux de Paris, 'L'Entrepôt de Données de Santé', *Direction de la Recherche Clinique et de l'Innovation de l'AP-HP* (blog), 15 December 2019, <http://recherche.aphp.fr/eds/>.

<sup>104</sup> Commission Nationale de l'Informatique et des Libertés, 'Délibération N° 2017-013 Du 19 Janvier 2017 Autorisant l'Assistance Publique – Hôpitaux de Paris à Mettre En Œuvre Un Traitement Automatisé de Données à Caractère Personnel Ayant Pour Finalité Un Entrepôt de Données de Santé, Dénommé "EDS". (Demande d'autorisation N° 1980120)', 2017-013 § (2017).

<sup>105</sup> AFP, 'Aux urgences de Valenciennes, l'intelligence artificielle prédit le flux de patients', *L'Express.fr*, 7 February 2020, [https://www.lexpress.fr/actualites/1/societe/aux-urgences-de-valenciennes-l-intelligence-artificielle-predit-le-flux-de-patients\\_2117570.html](https://www.lexpress.fr/actualites/1/societe/aux-urgences-de-valenciennes-l-intelligence-artificielle-predit-le-flux-de-patients_2117570.html).

<sup>106</sup> Arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé », *JORF* n°0278 du 30 novembre 2019, texte n° 13

<sup>107</sup> [https://solidarites-sante.gouv.fr/IMG/pdf/181012\\_-\\_rapport\\_health\\_data\\_hub.pdf](https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf)



Data Hub will benefit public research centres and private players (associations, start-ups, etc.) as long as their project is of general interest and that they have been authorised by the CNIL. The government issued calls for projects to select the first beneficiaries of the platform. Nineteen projects were selected.<sup>108</sup> Some of the projects concern pathologies (cerebrovascular accident, myocardial infarction, Parkinson's disease). Others are more oriented towards improving treatment, such as better management of adverse drug reaction reports or improved patient monitoring. Finally, several projects will use artificial intelligence techniques to analyse massive amounts of data, such as from mammograms and pacemakers.

#### *1.5.4 Retail*

Most French retailers are trying to develop AI projects to offer services comparable to those offered by Amazon Go. For example, the Casino Group has opened a new store "Le 4 Casino"<sup>109</sup> where AI is supposed to improve the customer experience. Customers will have the opportunity to scan their products and will then be charged directly on their credit cards when they leave the store. In the future, they will simply walk in the store, put the products in their baskets and be automatically charged at the exit, thanks to the AI implemented in the store's video cameras.

---

<sup>108</sup> <https://solidarites-sante.gouv.fr/>

<sup>109</sup> Mundubeltz-Gendron, 'Le 4 Casino, l'Amazon Go à La Française Du Groupe Casino', usine-digitale.fr, 5 October 2018, <https://www.usine-digitale.fr/article/le-4-casino-l-amazon-go-a-la-francaise-du-groupe-casino.N751194>.

## 2 Laws and regulations applicable to AI and big data

### 2.1 General

For the time being, there is no specific legislation governing AI in France, even though the question is dealt with under certain laws. The main legal principles regulating AI in French law can be summarized as follows: fairness and transparency. These two principles are closely related and stated in the two most notable laws on the subject: the Data Protection Law of 1978 and the Digital Republic Law of 2016.

- The **principle of fairness (“loyauté”)** was formulated by the Council of State in its 2014 annual study on “*Le numérique et les droits fondamentaux*” (“Digital technology and fundamental rights”).<sup>110</sup> The Council of State acknowledged that the principle of fairness applies to data collectors under the Data Protection Act which provides that data subjects must be informed in a loyal manner about the processing of their personal data (art. 4) and given a right of access (art. 64). The Council of State suggested that this principle should also be applied to platforms and more particularly to ranking and indexing algorithms.<sup>111</sup> According to the Council of State, fairness means providing a service in good faith without trying to alter or divert this service for purposes unrelated to the interest of users.<sup>112</sup> This principle of fairness was implemented by the Law n°2016-1321 of 7 October 2016 for a Digital Republic in article L111-7 of the Code of consumer law which provides that platforms must disclose their classification and referencing criteria.<sup>113</sup> The CNIL considers that the principle of fairness should apply to all algorithms.<sup>114</sup> An algorithm is fair if its functionality corresponds to the functionality known by the provider and the user. If the provider hides a feature of the algorithm, then the algorithm is unfair. Unfairness can also occur when the algorithm provides the agreed functionality while fulfilling another functionality that was not disclosed to the consumer (such as the collection of geolocation data from the user of a smartphone for commercial purposes). Moreover, a fair algorithm should not have the effect of creating, reproducing or reinforcing any discrimination.

<sup>110</sup> Le Conseil d’État, ‘Étude annuelle 2014 - Le numérique et les droits fondamentaux’.

<sup>111</sup> Le Conseil d’État, ‘Étude annuelle 2014 - Le numérique et les droits fondamentaux’, 279.

<sup>112</sup> Le Conseil d’État, ‘Étude annuelle 2014 - Le numérique et les droits fondamentaux’, 224, 273.

<sup>113</sup> Platforms must give a fair, clear and transparent information on the methods of referencing, classification and de-referencing of the contents, goods or services (see art. L111-7 and D. 111 7 of the Code of consumer law).

<sup>114</sup> CNIL, ‘Comment permettre à l’Homme de garder la main?’

- The Digital Republic Law of 7 October 2016 also implemented the **principle of transparency** of algorithmic decision making by public bodies by changing the provisions of the code of relations between the public and the administration. The French administrations are now subject to important publication and information requirements (see below). In particular, public administrations must publish online the rules defining the algorithmic processing used in the performance of their tasks when such algorithms are the basis of individual decisions (Article L. 312-1-1 of the Code of relations between the public and the administration).<sup>115</sup>

In other respects, the principles that should be applied to AI are still uncertain. Three examples of such an uncertainty can be given.

Firstly, the emergence and development of autonomous machines raise questions about the liability regime applicable to such machines<sup>116</sup>. For now, smart machines act in accordance with their programming, but “strong AI” will allow them to be entirely autonomous and unpredictable. It is difficult to determine who might be liable in such case: the user, the owner, the manufacturer of the machine, the designer of the AI or the programmer of the software built into the machine. Several existing regimes could, in this perspective, apply: responsibility for the action of things, liability for defective products, or bespoke regimes. The creation of a new regime that would be specific to AI could be envisaged as well.

Secondly, another example of uncertainty can be drawn from the fact that AI machines are able to create. They can paint, write newspaper articles, or compose music. This phenomenon raises the question of the legal regime applicable to their creations. Should they be the subject of an existing regime or should a specific regime be created? This question is addressed both in the field of industrial property and copyright law.<sup>117</sup>

<sup>115</sup> “Sous réserve des secrets protégés, les administrations (...) publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l’accomplissement de leurs missions lorsqu’ils fondent des décisions individuelles” (Art. L. 312-1-1 du code des relations entre le public et l’administration)

<sup>116</sup> Mireille Bacache, « Intelligence artificielle et droits de la responsabilité et des assurances », in A.Bensamoun et G. Loiseau (dir.), *Traité de l’intelligence artificielle*, Lextenso, 2019, p. 69 ; Grégoire Loiseau, “Les responsabilités du fait de l’intelligence artificielle”, *Communication Commerce électronique* n° 4, Avril 2019, comm. 24 ; Sarah Dormont, “Quel régime de responsabilité pour l’intelligence artificielle?” *Communication Commerce électronique* n° 11, Novembre 2018, étude 19 ; Delphine Bauer, “Intelligence artificielle: qui sera responsable?”, *Petites Affiches*, 29 mai 2018, n°107, p. 3 ; Anne-Sophie Choné-Grimaldi et Philippe Glaser, “Responsabilité civile du fait du robot doué d’intelligence artificielle: faut-il créer une personnalité robotique?” *Contrats Concurrence Consommation* n° 1, Janvier 2018, alerte 1 ; Alexandra Bensamoun et Grégoire Loiseau, “La gestion des risques de l’intelligence artificielle. De l’éthique à la responsabilité” *JCP G* n° 46, 2017, doct. 1203.

<sup>117</sup> Alexandra Bensamoun, « Intelligence artificielle et propriété intellectuelle », in A.Bensamoun et G. Loiseau (dir.), *Traité de l’intelligence artificielle*, Lextenso, 2019, p. 235 ; Michel Vivant, “Intelligence artificielle et propriété intellectuelle”, *Communication Commerce électronique* n° 11, Novembre 2018, étude 18 ; Jacques

Thirdly, the possibility of creating a new status for “electronic persons” is discussed in France<sup>118</sup>, following the European Parliament Resolution of 16 February 2017 on the civil rules on robotics. The Parliamentary Office for the Evaluation of Scientific and Technological Choices has emphasized that this idea was either unfounded or premature.<sup>119</sup>

Broadly speaking, the legal issues raised by AI are being dealt with gradually and step by step. For the moment, the French authorities do not seem to favour the adoption of a comprehensive legislation dealing with AI in general. On January 15, 2020, a draft law was placed before the French Parliament by a Member of Parliament.<sup>120</sup> The main goal of this proposed constitutional law is the adoption of an “Artificial Intelligence and Algorithms Charter” (“*Charte de l’intelligence artificielle et des algorithmes*”) that would have a constitutional value and would state basic principles inspired by the Asimov’s laws of robotics. This proposal is unlikely to succeed. On the contrary, specific regimes could gradually be created or adapted in order to respond to the challenges that arise. All in all, the debate in France is, for obvious reasons, influenced by European developments.

## 2.2 Application of fundamental rights laws to AI

In France, the fundamental rights provisions contained in the EU Charter of Fundamental Rights, the European Convention on Human Rights (ECHR) and many provisions of other international human rights treaties have direct effect and priority over national acts of Parliament. French case-law, legislation and policy documents refer to the standards and principles defined in the judgments of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

---

Larrieu, “Robot et propriété intellectuelle”, Dalloz IP/IT 2016 p.291 ; Audrey Lebois, “Quelle protection juridique pour les créations des robots journalistes”, Communication Commerce Electronique, décembre 2015, Étude 2 ; Jacques Larrieu, “Le robot et le droit d’auteur,” in *Mélanges en l’honneur du professeur André Lucas*, LexisNexis, 2014, p. 465.

<sup>118</sup> Grégoire Loiseau, « Intelligence artificielle et droit des personnes », in A.Bensamoun et G. Loiseau (dir.), *Traité de l’intelligence artificielle*, Lextenso, 2019, p. 35 ; Anne-Sophie Choné-Grimaldi et Philippe Glaser, “Responsabilité civile du fait du robot doué d’intelligence artificielle: faut-il créer une personnalité robotique?” *Contrats Concurrence Consommation* n° 1, Janvier 2018, alerte 1

<sup>119</sup> De Ganay and Gillot, ‘Pour Une Intelligence Artificielle Maîtrisée, Utile et Démystifiée, Rapport Fait Au Nom de l’office Parlementaire d’évaluation Des Choix Scientifiques et Technologiques’.

<sup>120</sup> Assemblée Nationale, ‘Charte de l’intelligence artificielle et des algorithmes: Proposition de loi constitutionnelle’, Assemblée nationale, 15 January 2020, [http://www.assemblee-nationale.fr/dyn/15/dossiers/charte\\_intelligence\\_artificielle\\_algorithmes](http://www.assemblee-nationale.fr/dyn/15/dossiers/charte_intelligence_artificielle_algorithmes).

The decisions of the French Constitutional Council are taken into account as well.

For the time being, the focus has been placed on the data protection law, the challenges raised by algorithmic decision-making, the questions arising from the open data policy on judicial decisions and transparency.

### 2.2.1 Protection of personal data

The Data Protection Act n°78-17 of 06 January 1978 called "*Informatique et Libertés*"<sup>121</sup> was adopted in 1978 to protect the rights and freedoms of individuals against the risks generated by the creation of public files. This law was, therefore, mainly intended to regulate the way public and private persons process files containing personal information that permit the identification of data subjects. The exponential development of data processing subsequently led to the modification of this regulation. France transposed Directive (EC) No. 95/46 of 24 October 1995 into French law by the Law n°2004-801 of 06 August 2004,<sup>122</sup> which determined the conditions subject to which personal data may be collected, exploited, stored, managed, used or otherwise processed. The adoption of this law gave the Constitutional Council the opportunity to decide that the right to privacy has a constitutional value under French Law.<sup>123</sup>

Twelve years later, on 27 April 2016, the European Union adopted the "European package" composed of the General Regulation (EU) 2016/679 on the protection of personal data (GDPR)<sup>124</sup> and the Directive (EU) 2016/680, which were complemented by the Regulation (EU) 2018/1725 of 23 October 2018. France had, in part, anticipated the implementation of these regulations by adopting the law n°2016-1321 of 07 October 2016 for a Digital Republic. Subsequently, the entire "European package" was fully transposed into French law by the adoption of the Law n°2018-493 of 20 June 2018 and its implementing decree (*décret d'application* – a government decree that implements a given legislation) n°2018-687 of 1 August 2018, which modified the Data Protection Law of January 1978. Then the Ordinance n°2018-1125 of 12 December 2018 entirely rewrote and renumbered the Data

<sup>121</sup> CNIL, 'La Loi Informatique et Libertés: Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés', 17 June 2019, <https://www.cnil.fr/fr/la-loi-informatique-et-libertes>.

<sup>122</sup> JORF n°182 du 7 août 2004 page 14063 and texte n° 2, 'LOI N° 2004-801 Du 6 Août 2004 Relative à La Protection Des Personnes Physiques à l'égard Des Traitements de Données à Caractère Personnel et Modifiant La Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés', 2004-801 § (2004).

<sup>123</sup> Conseil Constitutionnel, 'Décision n° 2004-499 DC du 29 juillet 2004', 29 July 2004, <https://www.conseil-constitutionnel.fr/decision/2004/2004499DC.htm>.

<sup>124</sup> EUR-Lex, 'Règlement (UE) 2016/679 Du Parlement Européen et Du Conseil Du 27 Avril 2016 Relatif à La Protection Des Personnes Physiques à l'égard Du Traitement Des Données à Caractère Personnel et à La Libre Circulation de Ces Données, et Abrogeant La Directive 95/46/CE (Règlement Général Sur La Protection Des Données) (Texte Présentant de l'intérêt Pour l'EEE)', 27 April 2016, <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32016R0679>.

Protection Law. Today, the main principles are applicable to Artificial Intelligence in the Data Protection Law, which constitutes to date the major regulation regarding data processing.

The protection regime organized by the Data Protection Act is based on traditional principles: first, the principle of purpose limitation, which provides that the processing must be carried out for a specific, legal and legitimate purpose (art. 4); second, the principle of fairness of the data collection which requires that data controllers tell what they do and do as they say (art. 4); third, the principle of proportionality, according to which the collected data must be relevant and strictly necessary (art. 4 and 5); fourth, the principle of storage limitation (art. 5); fifth, the principle of data security (art. 4). This regulation preserves the fundamental rights of the data subject and is independent from any financial perspective. The provisions of the law apply to all kinds of processing – whether automated or non-automated – of personal data. However, some specific situations are not covered, among which the processing of personal data for exclusively personal purposes or the processing of fully anonymous data. Furthermore, the old expression of "nominative information" was replaced by the notion of "personal data", which includes any information that makes it possible to identify natural persons by name or to make them identifiable, or even simply to single them out. This definition covers voice and image, but also technical identifiers like IP addresses or cookies. The "processing" covered by the law includes any operation – automated or otherwise – carried out on personal data. The "data controller" is thus subject to various obligations and responsibilities, as well as the "recipient" of information or the "subcontractor" who manages the processing on the data controller's behalf.

Prior to the transposition of the 1995 EU Directive in 2004, the law imposed a formalities regime that differentiated whether the controller was a public or private person. In fact, the Data Protection Act had been adopted in 1978 to regulate the processing of personal data by the administration and the formalities regime for public persons was, therefore, the most restrictive. Automated processing of personal data carried out on behalf of the state, public institutions, local authorities or private legal entities managing a public service required an opinion from the CNIL, followed by a regulatory act of authorization. The processing operations carried out by private actors were subject to a simple declaration regime combined with an undertaking that the processing operation would comply with the requirements of the law. The 1995 EU Directive (implemented by the Law of 6 August 2004) modified the approach by emphasizing the risks posed by the processing of personal data on rights and freedoms. For non-sensitive data, a simple declaration of compliance with the CNIL's simplified standards was required. The Data Protection Act also provided that an exemption from declaration could be granted in the event that the data controller designated an independent correspondent responsible for ensuring the application of the law and guaranteeing that the processing operations

would not infringe the rights and freedoms of data subjects. Where the processing operation involved personal data that could be considered sensitive, it was subject to an authorisation regime.

With the implementation of GDPR by the law of 20 June 2020, most prior formalities have been abolished. Data controllers are no longer subjected, as in the past, to an obligation of prior declaration to the CNIL but have, in return, various obligations, among which the obligation to carry out a prior impact assessment in the event of a high risk to the rights and freedoms of the data subject and, where appropriate, to consult the CNIL. However, the Data Protection Act reserves the possibility of individual or global authorization regimes in the case of a processing that generates a significant risk for the rights and freedoms of the people concerned (arts. 31 and 32): genetic data, biometric data or health data, personal data relating to criminal convictions and related offences or security measures, data collected in the performance of a task carried out in the public interest, including processing in the context of social protection and public health, national identification number or any other identifier of general application personal data implemented on behalf of the state and which are relevant to state security, defence or public security.

In most cases the authorization is given by the CNIL. A specific authorisation regime applies to the public sector: in some cases, authorization is required by order of the competent minister(s) after a reasoned and published opinion from the CNIL; in other cases, authorization must be obtained by order or by a deliberative body, after a reasoned and published opinion from the CNIL; in yet other cases, authorization by decree in the *Conseil d'Etat*, taken after a reasoned and published opinion of the CNIL, is required. Failure to carry out the prior formalities of declaration or authorisation is a criminal offence. Article 226-16 of the Criminal Code provides that processing personal data without complying with the prior formalities for its implementation shall be punishable by five years' imprisonment and a fine of €300,000. The law does not distinguish whether the omission is voluntary or involuntary.

Data controllers must implement "appropriate technical and organizational measures" to ensure that processing complies with the legislation, which they must be able to establish at any time. In the event of significant risks for the rights and freedoms of the persons concerned, they must carry out an analysis of the effect of the processing operations. They must also favour techniques that protect personal data from the very conception (*privacy by design*) and adopt default measures in order to reduce the need for data to what is strictly necessary given the purpose of the processing (*privacy by default*). They must, in addition, appoint a Data Protection Officer, keep a record of processing activities in order to establish compliance with regulations, implement measures to ensure an appropriate level of security given the risks for the rights and freedoms of the data subjects, and, finally notify

the CNIL or the person concerned (in certain cases) in the event of personal data breaches.

The data subjects concerned by the processing have a right to information, a right to be informed of personal data breaches (unless this information is likely to represent a risk for the national security, the national defence or the public security), a right not to be subject to a decision resulting exclusively from automated processing (see below), a right to portability so that they can retrieve their data or transfer them to a third party, and a right to digital oblivion which allows them to ask a search engine to delete certain results associated with their first and last names.

Individuals complaining of a violation of the law can take their case to the CNIL or to the courts. Any person or association may submit a complaint to the CNIL for non-compliance with the Data Protection Act and with the General Data Protection Regulation (GDPR). Indeed, the CNIL can carry out controls on its own initiative, but it can also act following complaints and reports from users. Following the complaint, the CNIL can then contact the data controller to verify its compliance with the law and request corrective action if necessary. The complaint may result in a formal notice to comply with the law or in a penalty which may be pecuniary (fine) or non-pecuniary (public warning, order to stop the treatment). In the event of a sanction, an appeal may be made to the Council of State. At the end, the complainant is informed of the actions taken. In addition, the persons concerned by the violation of the rules relating to the protection of their personal data may suffer financial or psychological damage. The person injured by unlawful data processing may seek legal redress and be awarded damages.

In this respect, French law was reformed in 2016 so that it is now possible for data subjects to take collective action in case of personal data breach: the class action may be brought with a view either to putting an end to the breach or to holding the person who caused the damage liable to obtain compensation for the damage suffered.<sup>125</sup> Finally, data controllers who do not comply with their obligations may incur criminal penalties as provided for by Articles 226-16 et seq. of the Penal Code. Penalties range up to 5 years' imprisonment and a fine of up to €300,000, in particular for breaches of fairness in data processing or breaches of data security and confidentiality.

### *2.2.2 Privacy challenges raised by the Open Data policy of judicial decisions*

---

<sup>125</sup> CNIL, 'La Loi Informatique et Libertés: Loi N° 78-17 Du 6 Janvier 1978 Relative à l'Informatique, Aux Fichiers et Aux Libertés', art. 43 ter II, III, IV.



In France, the expression “predictive justice” refers to the use of machine learning and natural language processing to provide statistical modelling for disputes based on the analysis of large volumes of past decisions. In other words, these technologies render the prediction of courts’ decisions possible, and various start-ups are currently offering new predictive tools to lawyers and judges. Predictive tools will soon benefit from large volume of data since French lawmakers have decided to publish all the judicial decisions rendered by French courts, though this reform has generated much debate.

The Law n°2016-1321 of 07 October 2016 for a Digital Republic has initiated the open data policy of the French administrations.<sup>126</sup> This law provided for the unrestricted free access to all the available data emanating from public administrations. This open data policy also concerns courts’ decisions (Article L 111-13 of the Code of the Organization of Justice and article 10 of the Code of Administrative Justice). The programming Law<sup>127</sup> n°2019-222 of 23 March 2019 on the justice system (*loi de programmation de la justice du 23 mars 2019*) slightly modified these provisions in this respect. The law now provides that the decisions made by the courts are made available to the public free of charge in electronic form. However, since court’s decisions contain personal information, this open data policy has caused an intense debate about the protection of privacy, whether it is the privacy of litigants, of judges or of third parties. Several protective measures were adopted during the vote of the law of 23 March 2019, in order to pseudonymize, as much as possible, the decisions that will be published. Paragraph 2 of Article L 111-13 of the Code of the Organization of Justice now provides that the surname and forenames of the natural persons mentioned in the decision, whether they are litigants or third parties, are removed prior to publication. The law also provides that any element enabling the identification of litigants, third parties, judges and members of the court’s registry must be hidden when disclosing this element is likely to undermine their security or privacy.

Meanwhile, French lawmakers have ruled out any possibility of nominative profiling of judges. Paragraph 3 of Article L111-13 of the Code of the Organization of Justice provides that the identity of judges and members of the Court’s Registry may not be used in order to assess, analyse, compare or predict their actual or alleged professional practices, under penalty of criminal sanctions. The intense debate over the development of sophisticated technological tools applied to court decisions has led the CEPEJ (European Commission for the Efficiency of Justice; which is a Council of Europe body) to promote ethical principles, which are intended for public and private actors that design and develop

---

<sup>126</sup> Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

<sup>127</sup> Programming laws may be adopted in all areas to determine the objectives of the action of the State. These laws are provided for in article 34, paragraphs 20 and 21, of the Constitution.

artificial intelligence tools based on the processing of courts' decisions.<sup>128</sup>

The implementing decree of this legislation has not been adopted yet, which means that these provisions are not effective for the moment.

The French government has recently decided to create a frame of reference on the compensation of personal injury, which is based on algorithms trained with past decisions. The purpose of the Datajust project is to draw up an indicative reference system for compensation for personal injury based on case law data. The Decree n° 2020-356 of 27 March 2020 authorized the Ministry of Justice to implement such automated processing for two years, but it is already clear that this project will continue on a permanent basis. The data processed by the algorithm will be the decisions rendered on appeal, between 01 January 2017 and 31 December 2019, by administrative and civil courts in disputes relating to compensation for personal injury. Specifically, the algorithm will process data relating to the amounts awarded by the courts, for each type of personal injury. The data extracted from the decisions will be those relating to the injuries suffered, the professional and financial situation of the victims, medical opinions, criminal offences and possible civil faults. In this context, the algorithm will make it possible to inform judges and litigants about the reference compensation. The idea is indeed to provide reliable information to victims of personal injuries, lawyers and judges.<sup>129</sup>

### 2.2.3 Protecting citizens in case of algorithmic decision making

In French law, algorithmic decisions made by private or public persons have been covered by the Data Protection Act since 1978. In fact, under the first paragraph of the former article 10 of the Data Protection Act of 6 January 1978, "*no court decision involving an assessment of the behaviour of a person may be based on an automated processing of personal data to evaluate certain aspects of his personality*".<sup>130</sup> Moreover, Article 10 prohibited any "*decision producing legal effects with regard to a person... taken solely on the basis of an automated data processing intended to define the profile of the person or to evaluate certain aspects of his/her personality*".<sup>131</sup> Under this article, decisions

<sup>128</sup> Commission européenne pour l'efficacité de la justice (CEPEJ), 'Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires', 13 September 2019, <https://www.coe.int/fr/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>.

<sup>129</sup> See the presentation of the project on the Etalab website: <https://entrepreneur-interet-general.etalab.gouv.fr/defis/2019/datajust.html>

<sup>130</sup> "*Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité*" (ancien article 10 Loi Informatique et Libertés).

<sup>131</sup> Toute "*décision produisant des effets juridiques à l'égard d'une personne [...] prise sur le seul fondement d'un traitement automatisé de données destiné à définir le*

taken on the basis of automated processing were lawful only when other reasons had also been taken into account. In 1995, the same principle was adopted in Article 15 of Directive 95/46/EC of 24 October 1995. These various provisions seem to have remained relatively unnoticed, until GDPR adopted on 27 April 2016 provided new rules regarding automated individual decision making, including profiling. Since GDPR entered into force, the Data Protection Act has been modified by the Law n°2018-493 of 20 June 2018 on the protection of personal data and the Ordinance n° 2018-1125 of December 12, 2018 which renumbered the Data Protection Act. The provisions of the former article 10 can now be found in article 47, which authorizes more widely automated decisions, but still rules out courts' decisions based on an automated processing of personal data intended to evaluate certain aspects of the defendant's personality.

Paragraph 2 of article 47 of the Data Protection Act of 06 January 1978 provides that "no decision which has legal effects on or significantly affects a person can be taken solely on the basis of automated processing of personal data, including profiling".<sup>132</sup> Therefore, decisions cannot be based on automated processing alone. However, there are exceptions to this principle. First, decisions taken on the sole basis of automated processing are lawful in cases corresponding to the exceptions provided for in article 22§2 GDPR. Second, the French law now allows individual administrative decisions taken on the sole basis of automated processing. In both cases, the decisions should not be based on the sensitive data referred to in article 9 GDPR (art. 47 Data Protection Law). Furthermore, the data subjects are afforded the right to be informed of the automated decision making. When article 22§2 GDPR is applicable, the rules defining the processing and the main characteristics of its implementation are communicated by the data controller to the data subject upon request.<sup>133</sup> In case of administrative decision making, the person concerned must be informed by an explicit mention.<sup>134</sup> The Data Protection Act also provides that the data controller ensures the control of the algorithmic processing and its evolutions to be able to explain to data subjects, in detail and in an intelligible form, how the processing was designed and applied to

---

*profil de l'intéressé ou à évaluer certains aspects de sa personnalité" (ancien article 10 Loi Informatique et Libertés).*

<sup>132</sup> "Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage" (art. 47, Loi Informatique et Libertés)

<sup>133</sup> "Les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande" (art. 47, Loi Informatique et Libertés)

<sup>134</sup> "Une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé" (article L. 311-3-1 du Code des relations entre le public et l'administration créé par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique).

them.<sup>135</sup> The information provided must put the data subject in a position to understand and contest the decision according to Article 119 II 5e of the Data Protection Act.<sup>136</sup>

The Constitutional Council has decided that the possibility of administrative automated decision making is compatible with the constitution.<sup>137</sup> The Constitutional Council based its decision on the important transparency obligations imposed on the public authorities and the guarantees offered by the Data Protection Act, like the right to information and the possibility to file a recourse against the decision. In particular, the council highlighted that the law provided for three conditions that must be met to use automatic decision making: the main characteristics of the algorithm must be communicated upon request, the individual administrative decision must be subject to administrative recourse, and no sensitive data shall be used. But the Constitutional Council also insisted that the data processor must be able to explain, in detail and in an intelligible format, to the person in question how the data processing was applied. The council concluded that algorithms "which can revise the rules they apply without the control and validation of the controller" (§71) cannot be used in automated decision making. This position is justified by the finding that such algorithms cannot be explained.

#### 2.2.4 Transparency requirements imposed on public administrations

The French administrations have been subject to important publication and information requirements since the adoption of the law for a Digital Republic of 2016. This law provided that public administrations must publish online the rules defining the algorithmic processing used in the performance of their tasks when such algorithms are the basis of individual decisions (Article L. 312-1-1 of the Code of relations between the public and the administration)<sup>138</sup>. These provisions were supplemented by the Decree n° 2017-330 of 14 March 2017 on the rights of individuals subject to individual decisions taken on the basis of algorithmic processing.

<sup>135</sup> "Le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard" (art. 47, Loi Informatique et Libertés).

<sup>136</sup> "Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques" (article 119 II 5<sup>e</sup> de la loi n° 78-17 du 6 janvier 1978).

<sup>137</sup> Conseil Constitutionnel, décision n° 2018-765 DC du 12 juin 2018.

<sup>138</sup> "Sous réserve des secrets protégés, les administrations (...) publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles" Legifrance.gouv.fr, 'Code Des Relations Entre Le Public et l'administration', art. L. 312-1-1).

In case of administrative decision-making, the person concerned must be informed in writing by an explicit mention, according to article L. 311-3-1 of the Code of relations between the public and the administration (CRPA)<sup>139</sup>. If the person concerned so requests, the rules defining the processing, the main characteristics of its implementation, the purpose of the algorithmic processing and the procedures for exercising the right to information shall be communicated by the administration (article L. 311-3-1-2, CRPA). Indeed, according to Article 47 of the Data Protection Act, the data controller must have ensured the control of the algorithmic processing and its evolutions to be able to explain to the data subject, in detail and in an intelligible form, how the processing was designed and applied.<sup>140</sup> More specifically, according to Article R. 311-3-1-2 of the CRPA, the administration must communicate upon request the degree and method of contribution of the algorithmic processing to decision-making; the processed data and their sources; the variables of the algorithm and their weighting in the case of the person concerned; and, finally, the tasks performed by the algorithm.<sup>141</sup> This right of access may be exercised with any administration, including local authorities, provided that it does not infringe secrets protected by law. Moreover, every administration employing more than fifty agents must publish on line the rules defining the main algorithmic processing used to make individual decisions (article L. 312-1-3 CRPA). The source codes of the algorithms used by the administration constitute communicable documents within the meaning of the Code of relations between the public and the administration (article L. 300-2 CRPA).

In addition to the general provisions contained in the CRPA, there are special legal provisions governing specific applications. Such provisions sometimes provide for exceptions. For example, article 47A of the code of tax procedures (*Livre des procédures fiscales*) provides for the prerogatives and obligations of the administration in the event of a tax audit. According to the Council of State,<sup>142</sup> the tax administration must transmit to the investigated company the files used to determine increased tax liabilities, but the administration doesn't have the

<sup>139</sup> "Une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé" (Code Des Relations Entre Le Public et l'administration, article L. 311-3-1).

<sup>140</sup> "Le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard" (CNIL, 'La Loi Informatique et Libertés: Loi N° 78-17 Du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés', art. 47).

<sup>141</sup> "L'administration communique à la personne faisant l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, à la demande de celle-ci, sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes: le degré et le mode de contribution du traitement algorithmique à la prise de décision; les données traitées et leurs sources; les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé; les opérations effectuées par le traitement" (Code Des Relations Entre Le Public et l'administration, article R. 311-3-1-2).

<sup>142</sup> Conseil d'État, 8<sup>ème</sup> - 3<sup>ème</sup> chambres réunies, 4 mai 2018, n°410950.

obligation to communicate the programs, materials and algorithms that were used to produce those files.

Another example is article L. 612-4 of the Code of Education, which rules the *Parcoursup* platform created by the Law n°2018-166 of 8 March 2018 to pre-register students in the various institutions of higher education. According to Article L. 612-3 of the Code of Education, the right to obtain information relating to the procedures and criteria applied to students' applications and to the pedagogical reasons justifying the final decision shall be reserved solely for applicants who so request, once the decision has been taken and exclusively for information relating to the procedures and criteria used in the examination of applications. A student union filed a claim to obtain the characteristics of the algorithm and the source code. While the judge of first instance ordered the defendant to communicate these elements<sup>143</sup>, the Council of State reversed the decision and ruled that the CRPA provisions regarding the right of access were not applicable to a student union.<sup>144</sup> However, as mentioned above, in the same decision, the Council of State highlighted that the Decree of 19 March 2019 (which is now in effect) provides that higher education institutions must release the general criteria used in their selection process. On 15 January 2020,<sup>145</sup> the Council of State transmitted to the Constitutional Council a question for a priority preliminary ruling (*Question Prioritaire de Constitutionnalité*) on the constitutionality of article L. 612-3 of the Code of Education, which is being contested on the grounds that it allows only a limited communication of the algorithmic treatments used to decide on the admission or non-admission of students. On 3 April 2020<sup>146</sup>, the Constitutional Council ruled that article 612-3 is constitutional but added that higher education institutions must publish the criteria used to review applications at the end of the national pre-registration procedure. In this case, the report must specify the extent to which algorithmic processing was used to carry out this examination and respect the privacy of applicants.

---

<sup>143</sup> 'Tribunal Administratif de La Guadeloupe N° 1801094', 4 February 2019; V Thibault Douville, 'Parcoursup à l'épreuve de La Transparence Des Algorithmes', 2019.

<sup>144</sup> Le Conseil d'État, 'Conseil d'État, 12 juin 2019, Université des Antilles, n°427916 & 427919'.

<sup>145</sup> Le Conseil d'État, 'Base de jurisprudence, Decision n° 433296'.

<sup>146</sup> Conseil Constitutionnel, Décision 2020-834 QPC, 3 avril 2020.

### 2.3 Overview of laws applicable to AI and big data

Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
Cross Sectoral	<p>French Constitution, which also includes the “<i>bloc de constitutionnalité</i>”;</p> <ul style="list-style-type: none"> <li>• Declaration of Human and Civic Rights (DHCR) of August 26<sup>th</sup> 1789</li> <li>• Preamble of the Constitution of October 27<sup>th</sup> 1946</li> <li>• Charter for the environment</li> </ul>	<p>Civil and political fundamental rights and liberties, notably:</p> <ul style="list-style-type: none"> <li>• Equality and non-discrimination (art. 1 Constitution, art. 1 and 6 DHCR)</li> <li>• Privacy (art. 2 DHCR)</li> <li>• Liberty (art. 3 DHCR)</li> <li>• Freedom of entrepreneurship (art. 4 DHCR)</li> <li>• Freedom of speech (art. 11 DHCR)</li> <li>• Guarantee of rights/ rule of law (art. 16 DHCR)</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• A law that is contrary to constitutional principles is invalid: <ul style="list-style-type: none"> <li>- Ex ante review: the law cannot be promulgated</li> <li>- Ex post review: the law is repealed</li> </ul> </li> <li>• Infringements to constitutional rights may be compensated (art. 1242 Civil Code)</li> </ul>	<ul style="list-style-type: none"> <li>• Contains fundamental rights and basic norms for legislation, government, the judiciary.</li> <li>• Constitutional review of Acts of Parliament is allowed (see above § 1.1.6). <ul style="list-style-type: none"> <li>- Ex ante review: after the law is voted in Parliament and before it is signed into law</li> <li>- Ex post review: priority preliminary ruling on the issue of constitutionality</li> </ul> </li> <li>• Three main decisions regarding AI (see above §1.1.6):</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<ul style="list-style-type: none"> <li>- Decision n°2018-765 DC of June 12, 2018<sup>147</sup>: algorithms that revise by themselves the rules which they apply cannot be used in automated decision making by public authorities</li>   <li>- Decision n°2019-796 DC of December 27 2019<sup>148</sup>: customs and tax administrations can collect personal data on public websites and process them in order to establish various infringements, like trading in prohibited goods, undeclared professional activity and fraudulent tax domiciliation. However, the data collection and processing carried out in order to establish the defect or delay of a tax</li> </ul>

<sup>147</sup> Conseil Constitutionnel, 'Décision N° 2018-765 DC Du 12 Juin 2018: Loi Relative à La Protection Des Données Personnelles'.

<sup>148</sup> Conseil Constitutionnel, 'Décision N° 2019-796 DC Du 27 Décembre 2019: Loi de Finances Pour 2020'.





Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<p>return in the cases where the administration has already sent a formal notice to the taxpayer is unconstitutional.</p> <ul style="list-style-type: none"> <li>- Decision n°2020-834 QPC of April 3 2020<sup>149</sup> : article L. 612-3 of the <i>Code de l'éducation</i> is constitutional but higher education institutions must publish the criteria against which applications have been examined at the end of the national pre-registration procedure. The report must specify the extent to which algorithmic processing was used to carry out this examination and respect the privacy of applicants</li> </ul>

<sup>149</sup> Conseil Constitutionnel, Décision 2020-834 QPC, 3 avril 2020.



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
	Civil Code	<ul style="list-style-type: none"> <li>• Privacy (art. 9)</li> <li>• Equality and non-discrimination (art. 16-3)</li> <li>• Right to compensation</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• Damages in tort</li> <li>• Injunction to cease the infringement (if necessary by means of a periodic penalty payment)</li> <li>• All measures, such as sequestration, seizure and others, likely to prevent or stop an invasion of privacy: such measures may, if there is an emergency, be ordered in summary proceedings</li> </ul>	<ul style="list-style-type: none"> <li>• Art 1240: the infringement of a subjective right (e.g. a constitutionally guaranteed right) may be compensated by damages when it is caused by a civil fault</li> <li>• "Anyone has a right to privacy" (art. 9). Includes respect for the secrecy of correspondence, i.e. the right to communicate confidentially with others by any means of communication (letter, telephone, e-mail)</li> <li>• "No one may be discriminated against on the basis of his or her genetic characteristics" (art. 16-3)</li> </ul>
	Penal Code	<ul style="list-style-type: none"> <li>• Equality/ non discrimination</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• Article 225-2: discrimination "committed against a natural or legal person, shall be punishable by three years"</li> </ul>	<ul style="list-style-type: none"> <li>• Article 225-1 defines discrimination: "Any distinction made between natural persons on the basis of their origin, sex, family status, pregnancy, physical appearance,</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
				<p>imprisonment and a fine of 45,000 euros when it consists of :</p> <p>1° Refusing to supply a good or service;</p> <p>2° hindering the normal exercise of any economic activity whatsoever;</p> <p>3° Refusing to hire, punish or dismiss a person;</p> <p>4° To make the supply of a good or service subject to a condition based on one of the elements referred to in Article 225-1 or provided for in Article 225-1-1</p> <p>5° To make an offer of employment, an application for an</p>	<p>particular vulnerability resulting from their economic situation - apparent or known to the perpetrator- their surname, place of residence, state of health or loss of autonomy, their disability, their genetic characteristics, their morals, their sexual orientation, their gender identity, their age, their political opinions, their trade union activities, their ability to express themselves in a language other than French, their membership or non-membership, real or supposed, of a particular ethnic group, nation, race or religion"</p>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				<p>internship or a period of training in a company subject to a condition based on one of the elements referred to in Article 225-1 or provided for in Article 225-1-1;</p> <p>6° To refuse to accept a person for one of the training courses referred to in 2° of Article L. 412-8 of the Social Security Code.</p> <p>Where the discriminatory refusal provided for in 1° is committed in a place open to the public or for the purpose of prohibiting access to it, the penalties are increased to five years' imprisonment and a</p>	



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
				<p>fine of 75,000 euros.”</p> <ul style="list-style-type: none"> <li>Article 432-7: discrimination “committed against a natural or legal person by a person holding public authority or entrusted with a public service mission, in the exercise or on the occasion of the exercise of his functions or mission, shall be punishable by five years' imprisonment and a fine of 75,000 euros when it consists of : 1° Refusing the benefit of a right granted by law; 2° hindering the normal exercise of</li> </ul>	



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				any economic activity."	
	Penal Code	<ul style="list-style-type: none"> <li>• Protection of personal data/ privacy</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• Criminal penalties, among others:               <ul style="list-style-type: none"> <li>- Article 226-16 provides that the processing of personal data without complying with the formalities prior to their implementation provided for by law is punishable by five years' imprisonment and a fine of 300,000 euros.</li> <li>- Article 226-19 provides that storing or keeping in</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Articles 226-16 to 226-24 punish the fact of having implemented a personal data processing without complying with the conditions laid down by the Data Protection Act.</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				<p>computerised storage, without the express consent of the person concerned, of personal data which directly or indirectly reveal the racial or ethnic origin, political, philosophical or religious opinions or trade union membership of persons, or which relate to their health or sexual orientation or gender identity, shall be punishable by five years' imprisonment</p>	



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
				and a fine of EUR 300 000.	
	Code of Labour Law	<ul style="list-style-type: none"> <li>• Non-discrimination/ Equality</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• Article L1132-4: Any discriminatory decision or practice is null and void</li> </ul>	<ul style="list-style-type: none"> <li>• Article L1132-1: no one may be excluded from a recruitment or be sanctioned, dismissed or subjected to any direct or indirect discriminatory measure, in particular as regards remuneration or professional promotion, on grounds of origin, sex, morals, sexual orientation, gender identity, age, marital status or pregnancy, genetic characteristics or particular vulnerability resulting from his or her economic situation, apparent or known to the author, his or her membership or non-membership, real or supposed, to an ethnic group, nation or alleged race, his or her political opinions, his or her trade union or mutualist activities, his or her</li> </ul>





Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					exercise of a local elective mandate, his or her religious beliefs, his or her physical appearance, his or her surname, his or her place of residence or his or her bank address, or because of his or her state of health, loss of autonomy or disability, his or her ability to express himself or herself in a language other than French
	Code of Consumer Law	<ul style="list-style-type: none"> <li>• Fairness (“loyauté”)</li> <li>• Transparency</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• Compliance with these obligations is monitored by an administrative agency, the DGCCRF (<i>Direction Générale de la Consommation, de la Concurrence et de la Répression des Fraudes</i>)</li> <li>• The DGCCRF can investigate on</li> </ul>	<ul style="list-style-type: none"> <li>• Article L111-7 was created by the Digital Republic Act n°2016-1321 of October 7, 2016. This article provides for the principle of fairness (“loyauté”) of platform’s algorithms</li> <li>• According to the principle of fairness (“loyauté”), when the platform engages in classifying or referencing of content, goods or services offered or put online by third parties by</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				<p>platforms' behavior, enjoin platforms to comply with the law or impose administrative fines.</p> <ul style="list-style-type: none"> <li>In this respect, article L 131-4 provides that platforms that do not comply with their obligations are liable to an administrative fine of €75,000 for a natural person and €375,000 for a legal entity.</li> </ul>	<p>means of computer algorithms, then it must provide clear and transparent information, in particular on the methods of referencing, classification and de-referencing and the ranking criteria</p> <ul style="list-style-type: none"> <li>Article L 111-7-1: On line platforms with more than 5 million users per month must draw up a charter of good practice to give effect to the obligations of clarity, fairness and transparency with regard to consumers</li> </ul>
	Data Protection Act ( <i>loi n°78-17 Informatique et Libertés</i> ) of January 6th 1978, as modified by Law n°2018-493 of 20 June 2018 on the protection of	<ul style="list-style-type: none"> <li>Privacy and protection of personal data</li> <li>Liberty and autonomy, right not to be registered without consent</li> </ul>	<p>Yes (in part). The law was voted in 1978 but was amended in order to implement:</p> <ul style="list-style-type: none"> <li>Directive 95/46</li> </ul>	<ul style="list-style-type: none"> <li>Any person or association may submit a complaint to the CNIL. The CNIL can carry out controls on its own initiative, but it can also act</li> </ul>	<ul style="list-style-type: none"> <li>Article 1: Information technology must be at the service of every citizen. (...). It must not infringe on human identity, human rights, privacy, individual or public freedoms".</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
	personal data and the Ordinance n° 2018-1125 of December 12 2018	<ul style="list-style-type: none"> <li>• Non discrimination</li> </ul>	<ul style="list-style-type: none"> <li>• GDPR 2016/679</li> <li>• Directive 2016/680</li> </ul>	<p>following complaints and reports from users. The control may result in a formal notice to comply with the law or in a sanction provided for in article 45 of the Data Protection law which may be pecuniary (fine) or non-pecuniary (public warning, order to stop the treatment). In the event of a sanction, an appeal may be made to the Council of State.</p> <ul style="list-style-type: none"> <li>• The person injured by unlawful data processing may</li> </ul>	<ul style="list-style-type: none"> <li>• The law provides for the conditions for the lawfulness of the processing of personal data (art. 5) and prohibits the processing of sensitive data with some exceptions (art.6)</li> <li>• The law provides for the obligations of any data controller, notably: <ul style="list-style-type: none"> <li>- Obligation to ask for consent (art. 5)</li> <li>- Interdiction to collect sensitive data except in specific cases (art. 64 to 86)</li> <li>- Loyal (fair) collection of data (art. 4)</li> <li>- Obligation to ensure data security (art. 4)</li> </ul> </li> <li>• The law provides for the rights of any data subject, notably:</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				<p>be awarded damages by civil courts. Class actions are possible.</p> <ul style="list-style-type: none"> <li>• Criminal penalties: data controllers who do not comply with their obligations may incur criminal penalties as provided for by articles 226-16 et seq. of the Penal Code (see above). Penalties range up to 5 years' imprisonment and a fine of up to €300,000, in particular for breaches of fairness in data processing or breaches of data</li> </ul>	<ul style="list-style-type: none"> <li>- right to be informed of the data collection (art. 5)</li> <li>- right to object to the data collection (art. 5)</li> <li>- right of access (art. 49)</li> <li>- right of rectification (art. 50-51)</li> <li>• The law provides that the CNIL's authorization is required in specific cases (art 31 and 32) for the collection of: <ul style="list-style-type: none"> <li>- some sensitive data (for ex: biometric data collected for identification)</li> <li>- data collected for the needs of law enforcement or defence</li> <li>- health data (art. 65 et seq.)</li> </ul> </li> <li>• The law includes provisions related to automated decision making:</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
				security and confidentiality.	<ul style="list-style-type: none"> <li>- Article 47 prohibits fully automated decision making subject to the exceptions provided for in article 22 GDPR and to the possibility for administrations to make automated administrative decisions</li> <li>- Article 95: No decision which produces legal effects concerning a person or significantly affects that person may be taken solely on the basis of an automated data processing intended to anticipate or evaluate certain personal aspects relating to the data subject.</li> <li>- Article 47: individual administrative decisions can be automated if 1/ the main characteristics of the algorithm are communicated upon</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<p>request, 2/ the individual administrative decision can be reviewed, 3/ no sensitive data is used and 4/ no algorithm that can revise the rules it applies without the control and validation of the controller is used.</p> <ul style="list-style-type: none"> <li>- Article 47: Any automated processing must include, under penalty of being declared null and void, an explicit statement specifying the purposes of the processing, a reminder of the right of communication, and the procedures for exercising this right</li> <li>- Article 47: the controller shall ensure that the algorithmic processing and its evolution are under control so as to be able to explain in detail</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					<p>and in an intelligible form to the data subject the manner in which the processing has been carried out with respect to him/her</p> <ul style="list-style-type: none"> <li>- Art. 119 II 5e: any natural person establishing his or her identity shall have the right to question the controller of a personal data processing system in order to obtain (...) information making it possible to understand and challenge the logic underlying the automatic processing operation in the event of a decision taken on the basis thereof which produces legal effects concerning the person concerned</li> <li>• The law deals with profiling:</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					<ul style="list-style-type: none"> <li>- Article 94: Personal data based on facts shall, as far as possible, be distinguished from data based on personal assessments.</li> <li>- Article 95: Any profiling that discriminates against natural persons on the basis of sensitive data is prohibited.</li> </ul>
Law enforcement	Data Protection Act ( <i>loi n°78-17 Informatique et Libertés</i> ) of January 6th 1978, as modified by Law n°2018-493 of 20 June 2018 on the protection of personal data and the Ordinance n° 2018-1125 of December 12 2018	<ul style="list-style-type: none"> <li>• Privacy and protection of personal data</li> <li>• Liberty and right not be registered without consent</li> </ul>	Yes (in part). The law was voted in 1978 but was amended in order to implement: <ul style="list-style-type: none"> <li>• Directive 95/46</li> <li>• GDPR 2016/679</li> <li>• Directive 2016/680</li> </ul>	<ul style="list-style-type: none"> <li>• The legality of the treatment may be contested before the administrative judge</li> <li>• Individuals may bring a claim before the CNIL after contacting the data controller (see above)</li> </ul>	<ul style="list-style-type: none"> <li>• Title III of the Data Protection Act (art. 87 et seq.) covers the processing of personal data for the purpose of the prevention, investigation, detection, prosecution or enforcement of criminal offences by any public authority</li> <li>• Article 87: such processing is lawful only if and insofar as it is necessary for the performance of those missions by a competent</li> </ul>





Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				<ul style="list-style-type: none"> <li>• Individuals may be awarded damages by an administrative court</li> </ul>	<p>authority. In this case, the proportionality of the time of storage of the personal data must be guaranteed and must take into account the purpose of the treatment and the nature or seriousness of the offences concerned.</p> <ul style="list-style-type: none"> <li>• Article 88: the processing of sensitive data is only allowed:               <ul style="list-style-type: none"> <li>- in cases of absolute necessity</li> <li>- subject to appropriate safeguards for the rights and freedoms of the data subject</li> <li>- if it is authorised by a law or regulation, or is intended to protect the vital interests of a natural person, or relates to data which have been manifestly made public by the data subject.</li> </ul> </li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<ul style="list-style-type: none"> <li>• Article 31.I and II: Processing operations carried out on behalf of the State 1/ which relate to State security, defence or public security or 2/ which have as their purpose the establishment or prosecution of criminal offences or the enforcement of sentences must be authorised by the Government after obtaining the opinion of the National Commission for Data Processing and Freedoms. When such treatments deal with sensitive data they must be authorized by a decree adopted in the Council of State after the CNIL has given its opinion.</li> <li>• Article 32: The collection and use of genetic or biometric data on behalf of the State for the authentication or verification of the identity</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					<p>of persons must be authorized by the government by a decree in the Council of State based on the opinion of the CNIL.</p> <ul style="list-style-type: none"> <li>The data subjects have a right of information, a right of access, a right of rectification or deletion, a right of limitation of the treatment (art. 104 et seq.)</li> </ul>
	<p>Law n°95-73 of January 21 1995 (loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité)</p>	<ul style="list-style-type: none"> <li>Security</li> <li>Privacy</li> </ul>	<p>Not applicable</p>	<ul style="list-style-type: none"> <li>Systems set up illegally can be challenged before the administrative judge</li> </ul>	<ul style="list-style-type: none"> <li>Article 10.I: Video-surveillance visual recordings are considered personal information only if they are used to create a personal file. In this case, they are subject to the Data Protection Act.</li> <li>Article 10.II: The transmission and recording of images taken on public roads, by means of video-surveillance, is possible for security purposes provided</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					<p>that the public is clearly and permanently informed of the existence of the video-surveillance system and of the authority or person responsible.</p> <ul style="list-style-type: none"> <li>Article 10.III: The installation of a video surveillance system is subject to authorisation by the representative of the State (prefect) or, in matters of national defense, by a departmental commission chaired by a magistrate. This scheme applies only to recordings which are not intended to be used for the processing of personal data. In the case of the processing of personal data, the Data Protection Act applies.</li> </ul>
	Code of Internal Security ( <i>Code de la sécurité intérieure</i> )	<ul style="list-style-type: none"> <li>Security</li> <li>Privacy and protection of personal data</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>These provisions do not provide for guarantees but enable surveillance</li> </ul>	<ul style="list-style-type: none"> <li>Article L851-1 provides that platforms and internet services providers must communicate, in some</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				<p>services to ask for information</p> <ul style="list-style-type: none"> <li>• Unlawful actions taken by public authorities may be contested before administrative courts</li> </ul>	<p>instances, connection data to intelligence services.</p> <ul style="list-style-type: none"> <li>• Article L851-3 provides that platforms and internet service providers must, in some instances, implement automated processing on their networks to detect connections that could reveal a terrorist threat. This automated processing uses connection data without enabling the identification of the persons concerned. When processing operations detect data likely to characterize the existence of a terrorist threat, the Prime Minister or his delegate may authorize the identification of the persons concerned and the collection of their data. These data are processed within sixty days and destroyed at the end of this period, unless there are</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
Public Administration	Code of relations between the public and the administration ( <i>Code des Relations entre le public et l'administration CRPA</i> )	<ul style="list-style-type: none"> <li>• Privacy and protection of personal data</li> <li>• Transparency of public authorities</li> </ul>	<p>A few amendments were made in order to implement:</p> <ul style="list-style-type: none"> <li>• GDPR 2016/679</li> <li>• Directive 2016/680</li> </ul>	<ul style="list-style-type: none"> <li>• An action may be brought before an administrative court to challenge the legality of the administration's actions</li> <li>• An injunction to release more information can be granted</li> <li>• Compensation for the damage suffered can be awarded</li> </ul>	<p>serious elements confirming the existence of a terrorist threat.</p> <ul style="list-style-type: none"> <li>• The CRPA gathers all the provisions dealing with the relations between citizens and public administrations</li> <li>• The CRPA provides that public administrations can publish the administrative documents they produce or receive (article 312-1). In cases referred to in special provisions, the publication is mandatory.</li> <li>• The provisions of CRPA were modified by the Digital Republic Act n°2016-1321 of October 7, 2016 which implemented two principles: <ul style="list-style-type: none"> <li>- The publication of the source codes of algorithms used by public administrations as part of the "Open Data" policy of the French</li> </ul> </li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<p>government (Art. L300-2)</p> <ul style="list-style-type: none"> <li>- Transparency of algorithmic decision making (Art. L. 312-1-1 CRPA).</li> <li>• The code now provides that the public administrations that practice automated individual decision making are subject to three obligations: <ul style="list-style-type: none"> <li>- Every administration employing more than fifty agents must publish online the rules defining the main processing operations used in the performance of their tasks when they form the basis for individual decisions (article L312-1-3)</li> <li>- They must mention on line and on the documents delivered to</li> </ul> </li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<p>citizens (opinions, notifications) a statement specifying the purposes of the processing operation, a reminder of the right of communication and the procedures for exercising this right (art. L311-3-1).</p> <ul style="list-style-type: none"> <li>- They must provide, at the request of the person concerned: the degree and mode of contribution of the algorithmic processing to decision-making, the data processed and their sources, the processing parameters and their weighting, applied to the situation of the person concerned, the operations carried out by the processing (art. L. 311-3-1-2).</li> </ul>





Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
	Code of tax procedures ( <i>Livre des procédures fiscales</i> )	<ul style="list-style-type: none"> <li>• Transparency of public authorities</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• If the guarantees offered to the taxpayer are not complied with by the tax authorities, the taxpayer may contest the adjustment and have it annulled.</li> </ul>	<ul style="list-style-type: none"> <li>• The code provides for the prerogatives and obligations of the administration in the event of a tax audit</li> <li>• Article 47A III. D provides that the administration informs the taxpayer of the result of the computer processing that gives rise to a tax adjustment.</li> <li>• In 2018, the Council of State<sup>150</sup> (see above § 1.1.6) ruled that the tax administration must transmit to the investigated company the files used for the determination of tax increases, but the administration doesn't have the obligation to communicate the programs, materials and algorithms that were used to produce those files.</li> </ul>

<sup>150</sup> Conseil d'État, 8ème - 3ème chambres réunies, 4 mai 2018, n°410950, accessed 18 March 2020.



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
	Financing Law n°2019-1479 of 28 December 2019 for 2020 (loi n°2019-1470 du 28 décembre 2019 de finance pour 2020)	<ul style="list-style-type: none"> <li>Not fundamental right is protected here</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>Tax procedure not complying with the conditions provided by article 154 may be nullified</li> <li>If the tax administration does not comply with article 154 and the Data Protection Act, complaints may be brought before the CNIL and civil or administrative courts.</li> </ul>	<ul style="list-style-type: none"> <li>Article 154 allows the tax and customs authorities to collect massive amounts of public data on social networks or online sales platforms to combat fraud as part of a three-year experiment</li> <li>three areas are targeted: (fake) tax domiciliation abroad, illegal businesses and hidden professional activities (such as undeclared work)</li> <li>Data can be stored for one year</li> <li>The CNIL released its <a href="#">opinion</a><sup>151</sup> on this project in September and highlighted that the proposed processing operations are likely to infringe the rights and</li> </ul>

<sup>151</sup> Commission Nationale de l'Informatique et des Libertés, 'Délibération N° 2019-114 Du 12 Septembre 2019 Portant Avis Sur Le Projet d'article 9 Du Projet de Loi de Finances Pour 2020' (2019).



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
Justice	Code of the Organization of Justice (COJ)	<ul style="list-style-type: none"> <li>• Privacy and protection of personal data</li> <li>• Transparency of the judicial system</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• Unlawful action taken by public authorities may be challenged before administrative courts and give rise to compensation</li> </ul>	<p>freedoms of the data subjects</p> <ul style="list-style-type: none"> <li>• The Digital Republic Act n°2016-1321 of October 7, 2016 launched the Open Data policy, especially for judicial decisions and modified accordingly article L. 111-13 of the Code of the Organization of Justice (and article 10 of the Code of Administrative Justice)</li> <li>• Article L 111-13 now provides that judicial decisions are made available to the public in electronic form free of charge</li> <li>• Article L111-13 also provides that the surname and forenames of the natural persons mentioned in the decision, whether they are litigants or third parties must be removed prior to publication</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					<ul style="list-style-type: none"> <li>This provision also provides that the identity of judges and members of the Court's Registry may not be used in order to assess, analyse, compare or predict their actual or alleged professional practices, under penalty of criminal sanctions</li> </ul>
	<p>Data Protection Act (<i>loi n°78-17 Informatique et Libertés</i>) of January 6th 1978, as modified by Law n°2018-493 of 20 June 2018 on the protection of personal data and the Ordinance n° 2018-1125 of December 12 2018</p>	<ul style="list-style-type: none"> <li>Due process</li> </ul>	<p>Yes (in part). The law was voted in 1978 but was amended in order to implement:</p> <ul style="list-style-type: none"> <li>Directive 95/46</li> <li>GDPR 2016/679</li> <li>Directive 2016/680</li> </ul>	<ul style="list-style-type: none"> <li>The judicial decision would be void</li> <li>The person concerned would be compensated</li> </ul>	<ul style="list-style-type: none"> <li>Article 47 and article 95: No judicial decision involving an assessment of a person's conduct may be based on automated processing of personal data intended to evaluate certain personal aspects relating to that person.</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
	Law of 16 November 2016 ( <i>Loi n°2016-1547 du 16 novembre 2016 de modernisation de la justice du XXI<sup>e</sup> siècle</i> )	<ul style="list-style-type: none"> <li>• Due process</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• The arbitration decision or the result of the conciliation or mediation would be void</li> <li>• The person concerned would be compensated</li> </ul>	<ul style="list-style-type: none"> <li>• Article 4.3 : online conciliation, mediation or arbitration services cannot be based solely on algorithmic or automated processing of personal data</li> </ul>
	Decree n° 2020-356 of March 27, 2020 on the DataJust system	<ul style="list-style-type: none"> <li>• Right to be compensated for personal injury</li> </ul>	Not applicable	<ul style="list-style-type: none"> <li>• Unlawful actions taken by the Ministry of Justice may be challenged before administrative courts.</li> <li>• Damages could be awarded.</li> </ul>	<ul style="list-style-type: none"> <li>• The Decree authorizes the Ministry of Justice to implement an algorithm that will process past decisions rendered on compensation for personal injury. Specifically, the algorithm will process data relating to the amounts awarded by the courts, for each type of personal injury.</li> <li>• The aim of the Datajust project is to draw up an indicative reference system for compensation of</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					personal injury based on case law data.
Health Services	Code of Public Health ( <i>Code de la santé publique</i> )	<ul style="list-style-type: none"> <li>• Liberty and right to give an informed consent</li> <li>• Transparency of medical procedures</li> <li>• Protection of personal data</li> </ul>	Some provisions were amended because of GDPR implementation	<ul style="list-style-type: none"> <li>• In case of infringements, patients can be compensated by an award of damages</li> </ul>	<ul style="list-style-type: none"> <li>• The code provides for the rights of patients: <ul style="list-style-type: none"> <li>- Every patient has a right to be informed of his state of health and to give an informed consent (Articles L.1110-5, L. 1111-2 and L. 1111-4): this requirement implies that the patient's consent is necessary in order to use any AI tool in the medical process (though it is not expressly stated)</li> <li>- Every patient has a right to privacy and to the secrecy of information about him/her (Article 1110-4)</li> </ul> </li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<ul style="list-style-type: none"> <li>- Every patient has a right of access to his or her data and medical records (article L1111-7)</li> <li>• The code includes provisions restricting or prohibiting the creation or use of health data processing, among which:               <ul style="list-style-type: none"> <li>- Article 4113-7: the creation and use of files containing data from medical prescriptions or information for the purposes of commercial prospecting or promotion is prohibited, as long as these files make it possible to directly or indirectly identify the prescribing professional.</li> <li>- Combined with article L 113-1 of the Code of insurance, article 1141-1 provides that insurers</li> </ul> </li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
					<p>cannot deny the subscription of an insurance contract on the basis of the results of predictive genetic tests meant to detect a disease which has not yet broken out. Nor can they reproach subscribers for not disclosing such a predisposition if the disease had not yet manifested itself at the time of subscription<sup>152</sup>.</p> <ul style="list-style-type: none"> <li>The code provides for the possibility of creating health data files with or without the patient's consent, under the conditions provided for by the Data Protection Act.</li> </ul>
	Data Protection Act ( <i>loi n°78-17 Informatique et Libertés</i> ) of January	<ul style="list-style-type: none"> <li>Transparency</li> <li>Liberty and right to give an informed consent</li> </ul>	Yes (in part). The law was voted in 1978 but was	<ul style="list-style-type: none"> <li>Any person or association may submit a complaint to the</li> </ul>	<ul style="list-style-type: none"> <li>Article 6 prohibits health data processing subject to exceptions</li> </ul>

<sup>152</sup> Tribunal de Grande Instance de Nanterre, 25 Octobre 2019.





Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
	<p>6th 1978, as modified by Law n°2018-493 of 20 June 2018 on the protection of personal data and the Ordinance n° 2018-1125 of December 12 2018</p>	<ul style="list-style-type: none"> <li>• Fairness</li> </ul>	<p>amended in order to implement:</p> <ul style="list-style-type: none"> <li>• Directive 95/46</li> <li>• GDPR 2016/679</li> <li>• Directive 2016/680</li> </ul>	<p>CNIL. The CNIL can carry out controls on its own initiative, but it can also act following complaints and reports from users. The control may result in a formal notice to comply with the law or in a sanction provided for in article 45 of the Data Protection law which may be pecuniary (fine) or non-pecuniary (public warning, order to stop the treatment). In the event of a sanction, an appeal may be made to the Council of State.</p>	<ul style="list-style-type: none"> <li>• Article 64 states the right of access provided for by article L1111-7 Code of public health</li> <li>• Article 65 to 71 provide for the general regime applicable to health data processing: <ul style="list-style-type: none"> <li>- if the file is merely a "repository" of health data, patient's consent is required. The authorization of the CNIL is necessary for files created without the consent of patients, whose public interest must then be established.</li> <li>- if the data are reused for research, studies or evaluations on the basis of the collected data, then the data controller should make a commitment to comply with a reference methodology developed by the CNIL. In the absence of</li> </ul> </li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				<ul style="list-style-type: none"> <li>The person injured by unlawful data processing may be awarded damages by civil courts. Class actions are possible.</li> <li>Criminal penalties: data controllers who do not comply with their obligations may incur criminal penalties as provided for by articles 226-16 et seq. of the Penal Code (see above). Penalties range up to 5 years' imprisonment and a fine of up to €300,000, in</li> </ul>	<p>compliance with these standards, an authorisation from the CNIL must be obtained (Article 66 III).</p>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies if rights violated	Description
				particular for breaches of fairness in data processing or breaches of data security and confidentiality.	
Education	Code of Education	<ul style="list-style-type: none"> <li>• Transparency</li> </ul>		<ul style="list-style-type: none"> <li>• Unlawful actions taken by public higher education institutions can be contested before administrative courts.</li> <li>• Injunctions to disclose more information can be granted</li> <li>• Damages can be award</li> </ul>	<ul style="list-style-type: none"> <li>• Article L. 612-3 deals with the national procedure for pre-enrolment in higher education.</li> <li>• Candidates may be provided with information on the examination criteria and arrangements implemented by higher education institutions as well as the pedagogical reasons justifying the decision taken with regard to them.</li> <li>• Access to the documents relating to the algorithmic processing used by higher education institutions for the examination of applications shall be</li> </ul>



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<p>restricted to applicants who so request, after the decision concerning them has been taken, and solely for information relating to the criteria and arrangements for examining the application of the person's concerned. Third parties may not request that such criteria and procedures be communicated to them.</p> <ul style="list-style-type: none"> <li>The Council of State<sup>153</sup> ruled that student unions do not have the right to be informed of the criteria used by institutions of higher education in making decisions on students' applications. However, the Council of State has also highlighted that the Decree of 19 March 2019 (which is now in effect) provides that higher education</li> </ul>

<sup>153</sup> Le Conseil d'État, 'Conseil d'État, 12 juin 2019, Université des Antilles, n°427916 & 427919', 12 June 2019,



Sector	Title in English (unofficial)	Fundamental rights addressed	EU law basis	Remedies rights violated	if Description
					<p>institutions must release the general criteria used in their selection process</p> <ul style="list-style-type: none"> <li>On April 3<sup>rd</sup> 2020<sup>154</sup>, the Constitutional Council ruled that article 612-3 is constitutional while making a reserve of interpretation. According to the Council, higher education institutions must publish the criteria used to review applications at the end of the national pre-registration procedure. The report must specify the extent to which algorithmic processing was used to carry out this examination and respect the privacy of applicants.</li> </ul>

<sup>154</sup> Conseil Constitutionnel, Décision 2020-834 QPC, 3 avril 2020.

### 3 Future development

This country research has shown that AI is considered as a major challenge by the French government. AI is increasingly used by both public bodies and private companies, and many French research institutes and universities are involved in AI-development and in research into the effects of AI on human beings and society as a whole. The various policy documents, norms and guidelines described in this report show that there is significant awareness of both the opportunities and risks of AI for fundamental rights and public values.

Some general tendencies can be distilled from the various policy briefs and documents that are relevant to the future development of AI in France:

- The French Government is determined to achieve the digital transition of the French administration by using the latest technologies.
- The French Government deeply wants France to be a leader in AI and allocates significant amounts of money to AI research projects. By the year 2024, 70 million euros per year should be dedicated to the creation of new start-ups via Bpifrance, 400 million euros should be allocated to financing innovation challenges or industrial projects dedicated to AI and 800 million euros should be devoted to nanoelectronics research. Within this context, health and transports are the government's priority.
- The French local authorities also want to benefit from the opportunities created by AI, as illustrated by the success of facial recognition and predictive policing projects.
- The French agencies, like the CNIL, are very much aware of the challenge raised by AI, especially when it comes to protecting privacy and fundamental freedoms.
- In addition to this, it is evident that many private actors are actively involved in developing and using AI. Some of them have formed alliances, coalitions and public-private partnerships and developed a variety of ethical codes and guidelines for the responsible use of AI.

The future developments in the next few months or years will certainly deal with the use of AI in the healthcare system and various experiments launched by the French government:

- The law on bioethics is currently being discussed in parliament. This law will soon be adopted and will probably include provisions relating to the use of AI in medicine. In particular, this law will probably impose the obligation to inform the patient if an algorithmic treatment is used and provide that no medical process should be performed without a human intervention.
- The French government is implementing a 3 years experiment to detect tax evasion and frauds with AI tools which process data collected on social networks

- The French government is about to launch an experiment regarding facial recognition in the public space which may lead to the implementation of new systems.

## 4 References

### **Official reports**

Assemblée Nationale, *Intelligence artificielle: l'urgence d'une ambition européenne*, Rapport d'information de MM. André GATTOLIN, Claude KERN, Cyril PELLEVAL et Pierre OUZOULIAS, fait au nom de la commission des affaires européennes n° 279 (2018-2019) - 31 janvier 2019

S. Benhamou et L. Janin, *Intelligence artificielle et travail*, rapport à la ministre du Travail et au secrétaire d'État chargé du Numérique, France Stratégie, mars 2018

CERNA (Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene), *Éthique de la recherche en apprentissage machine*, juin 2017

CERNA ((Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene), *Numérique et santé: quels enjeux éthiques pour quelles régulations?* Novembre 19, 2018

Commission Nationale Informatique et Libertés (CNIL), *Comment garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, Décembre 2017; in English: [How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence](#)

Conseil d'Etat, *Le numérique et les droits fondamentaux*, La documentation française, 2014

Conseil d'Etat, *Puissance publique et plateformes numériques: accompagner l'ubérisation*, La documentation française, 2017

Conseil National du Numérique, Rapport du groupe de travail co- piloté par R. Hindi et L. Janin, *Anticiper les impacts économiques et sociaux de l'intelligence artificielle*, 2017

C. de Ganay et D. Gillot, *Pour une intelligence artificielle maîtrisée, utile et démystifiée* - n° 464 tome I (2016-2017) - 15 mars 2017



CSA, Capacité à informer des algorithmes de recommandation, Une expérience sur le service YouTube, novembre 2019

C. Gosselin, La police prédictive, Enjeux soulevés par l'usage des algorithmes en matière de sécurité publique, Institut d'aménagement et d'urbanisme d'Ile de France, avril 2019

Gouvernement français, *Une stratégie pour la France en matière d'intelligence artificielle*, mars 2017

Ministère de l'Economie et des Finances, "[Intelligence artificielle: état de l'art et perspectives pour la France](#)", 2019

OPECST, rapporteurs C. de Ganay et D. Gillot, Pour une intelligence artificielle maîtrisée, utile et démystifiée, 29 mars 2017

Cédric Villani, *Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne*, 2018; in English: <https://www.aiforhumanity.fr/en/>

C. Villani, Les algorithmes au service de l'action publique: le cas du portail admission post bac, février 2018, n°671 (Assemblée Nationale), n°305 (Sénat).

C. Villani et G. Longuet, L'intelligence artificielle et les données de santé, mars 2019, n°1795 (Assemblée Nationale), n°401 (Sénat)

## **Legal Scholarship**

### **Books:**

A.Bensamoun et G. Loiseau (dir.), *Traité de l'intelligence artificielle*, Lextenso, 2019

Ch. Feral-Schuhl, *Cyberdroit 2020-2021*, 8th edition, Dalloz Action, 2020

F. G'sell (dir.), *Le Big Data et le Droit*, Dalloz, 2020

### **Articles:**

Laurent Archambault et Léa Zimmerman, "La réparation des dommages causés par l'intelligence artificielle: le droit français doit évoluer", *Gaz Pal* 6 mars 2018, n°9, p. 17

Boris Barraud, "L'algorithmisation de l'administration", *RLDI* 2018, n° 150, p. 42

Emmanuel Barthe, "Les outils de l'intelligence artificielle pour le droit français", JCP G n° 14, 2019, doct. 381

Delphine Bauer, "Intelligence artificielle: qui sera responsable?", Petites Affiches, 29 mai 2018, n°107, p. 3

Alexandra Bensamoun, "Des robots et du droit...", Dalloz IP/IT 2016 p.281

Alexandra Bensamoun, "Stratégie européenne sur l'intelligence artificielle: toujours à la mode éthique..." D. 2018 p.1022

Alexandra Bensamoun et Grégoire Loiseau, "La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité" JCP G n° 46, 2017, doct. 1203

Alexandra Bensamoun et Grégoire Loiseau "L'intelligence artificielle: faut-il légiférer?", D. 2017 p. 581

Alexandra Bensamoun et Grégoire Loiseau, "L'intelligence artificielle à la mode éthique", D. 2017, 1371

Alexandra Bensamoun et Grégoire Loiseau "L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun: questions de temps", Dalloz IP/IT 2017 p.239

Alexandra Bensamoun et Grégoire Loiseau, "L'intégration de l'intelligence artificielle dans certains droits spéciaux", Dalloz IP/IT 2017 p.295

Charly Berthet, "Vers une politique de l'intelligence artificielle?", D. 2018 p.1640

Antoine Bolze, "Accès aux décisions judiciaires et Legaltech", Dalloz actualité, 20 février 2019

Danièle Bourcier et Primavera De Filippi, "Transparence des algorithmes face à l'*open data*: quel statut pour les données d'apprentissage?", RF adm. publ. 2018. 525

Magali Bouteille-Brigant, "Intelligence artificielle et droit: entre tentation d'une personne juridique du troisième type et avènement d'un "transjuridisme"", Petites Affiches, 27 mars 2018, n°62, p. 7

Céline Castets-Renard, "Régulation des algorithmes et gouvernance du machine learning: vers une transparence et "explicabilité" des décisions algorithmiques?", Revue Droit & Affaires n° 15, Décembre 2018, 1

Sylvie Chassagnard-Pinet, "Les usages des algorithmes en droit: prédire ou dire le droit?", Dalloz IP/IT 2017, p. 495

Raja Chatila "Intelligence artificielle et robotique: un état des lieux en perspective avec le droit", Dalloz IP/IT 2016 p.284

Anne-Sophie Choné-Grimaldi et Philippe Glaser, "Responsabilité civile du fait du robot doué d'intelligence artificielle: faut-il créer une personnalité

robotique?" Contrats Concurrence Consommation n° 1, Janvier 2018, alerte 1

Marc Clément, "Les juges doivent-ils craindre l'arrivée de l'intelligence artificielle?", Recueil Dalloz 2017 p.104

Lucie Cluzel-Métayer et Emilie Debaets, "Le droit de la protection des données personnelles: la loi du 20 juin 2018", RFDA 2018, p. 1101

Georgie Courtois, "Robots intelligents et responsabilité: quels régimes, quelles perspectives?", Dalloz IP/IT 2016 p.287

Xavier Delpech, "Intelligence artificielle: le droit (des contrats) a aussi son mot à dire", AJ Contrat 2018, p.145

Bruno Dondero, "Justice prédictive: la fin de l'aléa judiciaire?", Recueil Dalloz, D. 2017. 532

Bruno Dondero et Bernard Lamon, "Juristes humains contre IA. À propos de l'étude LawGeex", JCP G 2018, 1201

Sarah Dormont, "Quel régime de responsabilité pour l'intelligence artificielle?" Communication Commerce électronique n° 11, Novembre 2018, étude 19

Thibault Douville, "Parcoursup à l'épreuve de la transparence des algorithmes", Dalloz IP/IT 2019, p. 390

Jean-Baptiste Duclercq, "Le droit public à l'ère des algorithmes", RD publ. 2017. 1401

Scarlett May Ferrié, "Les algorithmes à l'épreuve du droit au procès équitable", JCP 2018, n° 11, p. 498

Nathalie Fricero, "Algorithmes et nouvelle génération de droits humains. À propos de la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement", JCP G n° 51, 2018, 1331

Antoine Garapon, "Les enjeux de la justice prédictive", RPPI 2016. Dossier 4

Edouard Geffray, "Quelle protection des données personnelles dans l'univers de la robotique", in *Robots, intelligence artificielle et droit*, Dalloz IP/IT 2016, p. 295

Lêmy Godefroy, "La performativité de la justice "prédictive": un pharmakon?", D 2018, 1979

Lêmy Godefroy, "Le code algorithmique au service du droit", D. 2018, 734

Julie Groffe, "Robot et droit d'auteur", in *Les robots - Objets scientifiques, objets de droits*, dir. A. Bensamoun, Mare et Martin, coll. "PUS", 2016, p. 201

Lucile Hennequin-Marc, "Pour l'harmonisation de la réparation du préjudice extrapatrimonial par le recours à la base de données publique" Droit Administratif n° 6, Juin 2019, étude 10

Aurore-Angélique Hyde, "Vers une cyberéthique de la justice "prédictive"", Dalloz IP/IT 2019 p. 324

Sophie Lacour, "Intelligence artificielle: les solutions algorithmiques permettent de définir plus précisément les profils des clients", Juris tourisme 2019, n°220, p.13

Stéphane Larrière, "Confier le droit à l'intelligence artificielle, le droit dans le mur?", Revue Lamy Droit de l'Immatériel, n°34, 1er février 2017

Jacques Larrieu, "Robot et propriété intellectuelle", Dalloz IP/IT 2016 p.291

Jacques Larrieu, "Le robot et le droit d'auteur," in *Mélanges en l'honneur du professeur André Lucas*, LexisNexis, 2014, p. 465

Marie-Cécile Lasserre, "L'intelligence artificielle au service du droit: la justice prédictive, la justice du futur?", Petites Affiches n°130 30 juin 2017, p. 6

Audrey Lebois, "Quelle protection juridique pour les créations des robots journalistes", Communication Commerce Electronique, décembre 2015, Étude 2

Caroline Lequesne-Roth, "La sciences des données numériques au service du contrôle fiscal français, Réflexions sur l'algocratie", in A. Pariente (dir.), *Les chiffres en finances publiques*, Paris, éd. Mare & Martin, 2019

Grégoire Loiseau, "Les responsabilités du fait de l'intelligence artificielle", Communication Commerce électronique n° 4, Avril 2019, comm. 24

Grégoire Loiseau, "Responsabilité", in *Intelligence artificielle et santé*, Journal de Droit de la Santé et de l'Assurance Maladie, 2017, n° 17, p. 21

Grégoire Loiseau, "Intelligence artificielle et droit du travail", Bulletin Joly Travail, avril 2019, n°4, p. 5

Engerrand Marique et Alain Strowel, "Gouverner par la loi ou les algorithmes: de la norme générale de comportement au guidage rapproché des conduites", Dalloz IP/IT 2017, 517

Nathalie Martial-Braz, "Le profilage", Communication Commerce Electronique 2018, Étude 15

Fabrice Melleray, "La justice administrative doit-elle craindre la "justice prédictive"?", AJDA 2017. 193

Alexandra Mendoza-Caminade, "Le droit confronté à l'intelligence artificielle des robots: vers l'émergence de nouveaux concepts juridiques?", Recueil Dalloz 2016 p.445

Yannick Meneceur, "Les enseignements des éthiques européennes de l'intelligence artificielle", JCP G n° 12, 2019, doct. 325

Florence Meuris-Guerrero, "Quelques illustrations contemporaines de l'intelligence artificielle", Communication Commerce électronique, n° 12, Décembre 2018, alerte 96

Elise Mouriesse, "L'opacité des algorithmes et la transparence administrative", RFDA 2019, 45

Martine Quenillet, "Droit et Intelligence Artificielle: mythes, limites et réalités", Petites Affiches, 3 juin 1994, n°66, 3 juin 1994

Jean-Baptiste Racine, "La résolution amiable des différends en ligne ou la figure de l'algorithmes médiateur", D. 2018. 1700

Alain Rallet, Fabrice Rochelandet, Philippe Pucheral et Celia Zolynski, "La *privacy by design*: une fausse bonne solution aux problèmes de protection des données personnelles", Légipresse 2016, p. 330

Thibault de Ravel d'Esclapon, "Intelligence artificielle: nouvelle résolution du Parlement européen", Dalloz actualité, 20 février 2019

Judith Rochfeld, "L'encadrement des décisions prises par algorithmes", Dalloz IP/IT 2018, p. 474

Frédéric Rouvière, "La justice prédictive, version moderne de la boule de cristal", RTD civ. 2017. 527

Frédéric Rouvière "Jus ex machina: la normativité de l'intelligence artificielle", RTD Civ. 2019 p.217

Jean-Baptiste Thierry, "La loi n° 2019-222 du 23 mars 2019, loi de réforme pour la justice numérique?", JCP G n° 19, 2019, doct. 524

Elise Untermaier-Kerléo, "Les nouveaux visages de la décision administrative: d'une administration assistée à une administration automatisée", JCP éd. Administration et Collectivité Territoriales, 2018, 2339

Alexandre Vial, "La qualification juridique de l'intelligence artificielle: du silicium à la personne?", Revue Droit & Affaires n° 15, Décembre 2018, 4

Michel Vivant, "Intelligence artificielle et propriété intellectuelle", Communication Commerce électronique n° 11, Novembre 2018, étude 18

Léo Wada, "De la machine à l'intelligence artificielle: vers un régime juridique dédié aux robots", *Petites Affiches*, 26 décembre 2018, n°257-258, p. 7

Guillaume Zambrano "Essai de catégorisation des *Legaltech*", *JCP G* n° 27, 2019, 725

