RAPPORT POUR L'ASSOCIATION INTERNATIONALE DE DROIT PENAL

L'INTELLIGENCE ARTIFICIELLE ET L'ADMINISTRATION DE LA JUSTICE : LA POLICE ET LA JUSTICE PRÉDICTIVES – PERSPECTIVES FRANÇAISES

Emmanuelle GINDRE[*] *et Margot CHAMBON* [*]

[*] Maître de conférences HDR en droit privé et sciences criminelles, 1. Univ. Polynésie française, GDI EA 4240, Tahiti, Polynésie française; 2. UPPA, IFTJ, EA 7504, Centre de recherche sur la justice pénale et pénitentiaire, Pau, emmanuelle.gindre@upf.pf.

[*]Doctorante en droit privé et sciences criminelles, Aix-Marseille Université, LDPSC EA 4690, Aix-en-Provence, France, margot.chambon@univ-amu.fr.

PREMIERE PARTIE : LA POLICE PREDICTIVE

Margot CHAMBON [*]

1 Pratiques nationales

1.1 Éléments nationaux de définition

Le concept de « police prédictive » reste, en France, sans définition concrète ni théorique. Aucune définition normative ou émanant des autorités publiques n'existe à ce jour, uniquement des essais doctrinaux, des rapports divers ou fondés sur des expériences étrangères permettent de délimiter le champ théorique de la police prédictive. Par exemple, le rapport du Centre des hautes études du ministère de l'Intérieur de mars 2019 a pu préciser la notion :

> « De façon générale, la « police prédictive » consiste pour la police (en France, police ou Gendarmerie) à utiliser des données et autres indicateurs pour calculer la probabilité du risque de survenance d'un crime dans le futur. Il peut également s'agir d'un calcul de probabilité d'une personne, précédemment repérée en raison d'activités suspectées d'illégalité, puisse passer à l'action. De telles informations sont utiles, d'une part, pour prévenir la commission d'infractions et, d'autre part, pour mieux déployer les forces de police »[1].

Le député Cédric Villani avait également tenté de donner des pistes de définitions dans un rapport parlementaire sur l'intelligence artificielle (IA) : « Cette méthode, communément appelée police prédictive, fait référence à l'application des techniques de prévision et d'analyse de données massives (big data) à la prévention de la criminalité »[2].

Les sources de définition de la notion sont donc lacunaires, traduisant la réticence française à adopter et intégrer concrètement la notion de police prédictive, alors que des systèmes fondés sur l'IA sont expérimentés dans le cadre pénal, judiciaire et de prévention policière. En ce sens, le rapport citera certes les rares expérimentations de police prédictive ayant pu avoir lieu en France, mais proposera des extrapolations des normes et exemples actuels concernant les technologies utilisées sur le territoire, qui pourraient s'approcher de la pratique prédictive. En effet, à travers le traitement de données à caractère personnel et les objectifs de prévention de la délinquance et de recherche des infractions poursuivis par les autorités, la police prédictive aurait, dans

[*] Aix-Marseille Université, LDPSC EA 4690, Aix-en-Provence, France, margot.chambon@univ-amu.fr.

[1] Ministère de l'Intérieur, *Rapport final CHEMI, Encadrement des risques techniques et juridiques des activités de police prédictive* (mars 2019).

[2] Mission parlementaire présidée par C. Villani, *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne* (2018).

une certaine mesure, des fondements juridiques similaires aux technologies envisagées dans la pratique existante.

En ce sens, des technologies préexistantes, comme la vidéo « augmentée », la vidéosurveillance, ou la reconnaissance faciale, sont tantôt expérimentées, utilisées ou interdites sur le territoire français. La Commission Nationale Informatique et Libertés (CNIL) donne à ce propos des éléments de définition de ces différentes techniques, bien qu'elle qualifie ces notions de « protéiformes »[3]. La vidéo « augmentée » désigne « des dispositifs vidéo auxquels sont associés des traitements algorithmiques mis en œuvre par des logiciels, permettant une analyse automatique », se distinguant des dispositifs de traitement des données biométriques, notamment la reconnaissance faciale. La vidéo « augmentée » permet à la fois une détection automatisée de certains comportements ou évènements dans l'espace public pour les missions de police, mais également de sécuriser ou mesurer certains phénomènes dans le secteur privé[4].

1.2 Expériences nationales

Les systèmes d'IA ne sont pas directement utilisés à des fins de police prédictive en France. Néanmoins, des expérimentations en la matière ont eu lieu sur le territoire, et certaines technologies fondées sur des systèmes d'IA, utilisées par certaines autorités, tendent à se rapprocher de cette philosophie technique et prédictive.

1.2.1 Essais en Gendarmerie

La Gendarmerie Nationale a pu effectuer, en 2017, des essais sur les logiciels Predvol ou Paved[5], qui ciblent précisément l'analyse des cambriolages et atteintes aux véhicules. Ce système a été élaboré par le Service Central du Renseignement Criminel (SCRC)[6] de la Gendarmerie Nationale, utilisant les informations issues de bases de données fermées du ministère de l'Intérieur relatives aux infractions en question des sept dernières années, ainsi que des données publiques (open data) socio-économiques de l'Institut National de la Statistique et des Études Économiques (INSEE). Le système PAVED se fonde sur la théorie de répétition proche, fréquemment utilisée dans la construction d'algorithmes prédictifs, inspirée du postulat criminologique selon lequel si un acte délinquant est commis dans un lieu, il est statistiquement plus probable que ce type d'acte se reproduise dans cette même zone. Le logiciel produit enfin des cartes présentant

[3] CNIL, *Caméras dites "intelligentes" ou "augmentées" dans les espaces publics*, (2022), 5.
[4] *Ibid*, 6
[5] C. Gode, S. Brion, A. Bohas, « The affordance-actualization process in a predictive policing context : insights from the French military police », *European Conference on Information Systems (ECIS)* (⟨hal-02500125⟩)
[6] Antenne du Ministère de l'Intérieur « *chargé(e) d'apporter des informations et une compréhension précise de la criminalité organisée et de masse afin d'orienter les actions dans la lutte contre la délinquance dans les phases pré-judiciaire et judiciaire* », https://www.gendarmerie.interieur.gouv.fr/pjgn/scrcgn

des hot spots, zones colorées du bleu au rouge en fonction du risque délinquant que présentent ou non certains lieux.

De la même manière, les essais du logiciel Predvol, en septembre 2016, se fondaient sur des données de l'INSEE remontant à 5 ans et eurent lieu dans les Gendarmeries de l'Oise. Ces systèmes n'ont été que peu concluants et sont restés au stade d'expérimentation, faute de résultats pertinents. En effet, les logiciels ne faisaient que reproduire des résultats jusqu'alors connus par les services de la Gendarmerie, et ne présentaient pas de réelle précision en matière de hot spot[7]. L'insuffisance de données fournies explique notamment ce manque de précision : plus l'algorithme reçoit d'informations variées, plus il peut affiner son analyse.

Il n'y a en réalité pas d'unité nationale quant aux essais en matière prédictive. Cependant, bien que l'implantation de logiciels prédictifs sur le territoire français n'ait été que peu concluante, les autorités montrent tout de même un certain intérêt pour l'usage des systèmes fondés sur l'IA dans le travail policier[8]. C'est au niveau local que les différentes expérimentations sont observées, en particulier dans les villes. Ainsi, la ville de Nice a recours aux tests de technologies prédictives lors de rassemblements ou dans le tramway[9].

Pour le moment, les seuls algorithmes s'approchant d'une « police prédictive » restent, dans les unités de Gendarmerie ou de police judiciaire, des systèmes d'aide à la prise de décision policière[10] : création de « divisions d'analyse et d'investigation criminelle » au sein de la Gendarmerie[11], analyse vidéo/vidéosurveillance intelligente, cartographie des lieux « à risque » délinquant[12]. Ces systèmes soutiennent les professionnels dans les procédés d'analyse de données, par exemple pour les investigations ou dans le cadre de la prévention de la délinquance.

1.2.2 Les systèmes et fichiers de traitement de données

En France, l'Unité Information passagers (UIP) a été créée en 2014[13], parallèlement à la transposition de la Directive du 27 avril 2016 relative à l'utilisation des données des dossiers passagers[14], dossier dit PNR (Passenger Name Record). Ce système collecte les

[7] Ministère de l'intérieur, (2019), (n 1), 30

[8] V. ce rapport, troisième partie, droit de la preuve et IA, qui détaille les outils d'investigation numérique des autorités d'enquête.

[9] D. Nakache, « "Two-I", la biopolitique au pouvoir à Nice » (*Médiapart*, 9 janvier 2019).

[10] Aussi appelés systèmes d'analyse décisionnelle.

[11] Sénat, question écrite n°16562 de Mme Marie-Françoise Perol-Dumont, (4 juin 2015), *JO Sénat* 1295.

[12] Ministère de l'Intérieur, (n 1).

[13] Décret n° 2014-1566, portant création d'un service à compétence nationale dénommé "Unité Information Passagers" (UIP) (22 décembre 2014), *JORF*, 24 décembre 2014.

[14] Directive (UE) n° 2016/681, relative à l'utilisation des données passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (27 avril 2016), *JOUE* L 119/132.

données relatives aux passagers aériens au moment de la réservation d'un vol, les informations étant enregistrées par les compagnies aériennes et transmises aux fichiers PNR. Ce dernier est à différencier du fichier API[15] (Advance Passenger Information), qui agrège les données récoltées lors de l'enregistrement du passager, données revêtant alors un caractère plus certain et officiel que lors de la réservation. Ce système PNR est né d'un accord préalable initié par les États-Unis avec l'Union européenne[16], ambition impulsée après les attentats de 2001 à New York. L'UIP, rattachée au ministère français chargé des douanes, a compétence pour gérer le fichier PNR et donc à collecter, enregistrer, traiter, et transmettre ces données relatives aux individus effectuant une réservation auprès d'une compagnie aérienne, puis effectuant l'enregistrement – voire l'embarquement – une fois à l'aéroport de départ. Ce transfert peut être effectué auprès des forces de sécurité nationales[17] ou d'Europol[18] en vue de l'évaluation d'un risque du passager pour la sécurité de l'État de destination. Le système API-PNR a vocation, au-delà de la constatation d'infractions, à anticiper leur commission en vue de l'analyse d'informations pouvant paraître suspectes à propos d'un voyageur.

Les données collectées sont multiples, allant du nom du passager à son numéro de siège, voire comprenant toute donnée « préalable » sur l'individu (API) : le numéro de vol et ses détails, le genre, la date de création et d'expiration de la pièce d'identité par exemple[19]. Les données sensibles[20] sont exclues du spectre de collecte du fichier API-PNR. En revanche, en France, un système de criblage permet d'interconnecter le système avec le fichier des personnes recherchées (FPR), interconnexion qui présente alors un risque de traitement des données sensibles dans la mesure où certaines sous-catégories du FPR contiennent l'inscription d'individus justifiée par des motifs pouvant révéler certaines convictions religieuses ou politiques. Aussi, au vu de l'objectif poursuivi par le système, le fichier API-PNR pourrait relever d'un traitement de police prédictive, en ce qu'il vise à intervenir ou détecter un comportement qui n'aurait pas encore eu lieu, et est ainsi inspiré des systèmes d'évaluation de la dangerosité. En effet, le fichier API-PNT ne se fonde pas sur les données relatives au passé pénal des passagers, aucune distinction n'étant faite entre les individus dans la collecte et l'analyse des données collectées. Force est donc de constater que, malgré la décision d'interdiction de la surveillance généralisée

[15] Directive nº 2004/82/CE concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (29 avril 2004) JOUE L 261/24.
[16] Décision nº 2012/472/UE relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure (26 avril 2012) JOUE L 215/4.
[17] Art. R232-15 du Code de la sécurité intérieure (CSI).
[18] Art. R232-13 CSI.
[19] Les données pouvant être collectées et transmises par les transporteurs aériens à l'UIP sont listées à l'Annexe I de la directive (UE) 2016/681, *op. cit.* (n 14).
[20] Règlement (UE) nº 2016/679, 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 (RGPD) (27 avril 2016), JOUE L 119/1, art. 9 ; Loi nº 78-17, relative à l'informatique, aux fichiers et aux libertés (6 janvier 1978), JOTF, 7 janvier 1978 <www.cnil.fr/fr/la-loi-informatique-et-libertes>, art. 6

par la CJUE[21], son appréhension du PNR paraît différenciée au vu de sa construction même. Il n'en reste pas moins qu'actuellement, seules les données relatives aux passagers à destination de l'Union européenne sont systématiquement collectées. Cette absence de systématicité de collecte des données de voyageurs appartenant à des États membres pourrait disparaître au profit d'une généralisation de l'analyse automatique[22].

1.2.3 Expérience de reconnaissance faciale

Il en est de même pour la technologie de reconnaissance faciale, encore sujette à controverses pour le Parlement, cependant expérimentée dans certaines communes. À ce jour, seule la reconnaissance faciale a posteriori est autorisée[23] à l'aide du TAJ (système de Traitement des Antécédents Judiciaires)[24]. À ce sujet, la ville de Nice a également été le théâtre de l'expérimentation de cette technologie dans l'espace public, à l'occasion du carnaval de la ville, rassemblant plusieurs milliers de personnes. Le dispositif mis en place consistait en un passage d'individus volontaires devant des caméras de vidéosurveillance préexistantes, équipées d'un logiciel créé par la société Confidentia, mais également en l'analyse faciale au sein d'une foule. La reconnaissance faciale permettait d'identifier les personnes dites d'intérêt et de déterminer celles autorisées ou non à pénétrer dans une zone définie, dans un but de protection de l'ordre public. Le rapport final de la Mairie de Nice indique que le contrôle dit « de masse » visait entre autres à identifier les personnes dangereuses et les personnes fichées au Fichier de Surveillance des Personnes Radicalisées au motif de terrorisme (FSPRT)[25]. En ce sens, la technologie de reconnaissance faciale prend une coloration prédictive en ce qu'elle vise dans une certaine mesure à anticiper le comportement délinquant d'individus considérés comme présentant déjà un danger. Le rapport final de la Mairie se félicite du succès de l'outil, notamment testé sur des jumeaux, dont seule la photo de l'un avait été entrée dans le logiciel de reconnaissance faciale, ce dernier identifiant l'individu[26].

Dans ce contexte, la Commission Nationale Informatique et Liberté (CNIL) a été consultée en amont, puis postérieurement aux essais effectués. La CNIL est une autorité administrative indépendante du pouvoir exécutif, créée par la loi Informatique et Libertés de 1978[27], en charge notamment de veiller au respect du droit à la protection des données personnelles dans l'exploitation de traitement automatisé, de fichiers ou tout autre procédé numérique public ou privé. Bien qu'initialement les avis de la CNIL ne

---

[21] CJUE, C-793/19, C-794/19, *Bundesrepublik Deutschland v SpaceNet AG / Telekom Deutschland GmbH*, (2022).

[22] Commission européenne, *Stratégie pour un espace Schengen pleinement opérationnel et résilient* (Communication au Parlement européen et au Conseil, COM/2021/277 final, 2021) 15.

[23] V. notamment art. R.40-26 c. proc. pén., contra art. R.236-2 CSI.

[24] V. Ce rapport, Troisième partie.

[25] Mairie de la ville de Nice, *Rapport sur l'expérimentation de la reconnaissance faciale* (2019) <www.documentcloud.org/documents/6350838-Bilan-Reconnaissance-Faciale.html> consulté le 27 mai 2023, 8

[26] *Ibid*. 10

[27] Loi relative à l'informatique, aux fichiers et aux libertés, *op.cit.* (n 20).

soient pas contraignants, son rôle réside dans les procédés de contrôle, d'alerte, de conseil ou d'information, mais peut aussi sanctionner une entité ou personne qui ne respecterait pas la protection des données à caractère personnel.

À ce titre, elle fut donc consultée en amont des essais à Nice pour lesquels elle exigea aussi un rapport final[28]. Bien que ce dernier détaille les procédés d'étude d'impact effectuée en amont, et fournisse les différents avis des professionnels ayant mis en œuvre l'expérience, peu de détails sont communiqués quant aux éventuels biais, faux-positifs ou encore sur le fonctionnement global du système. Cela pouvant s'expliquer par une protection de la technologie Anyvision par un brevet industriel, il n'en reste pas moins que le rapport n'a pas entièrement satisfait la CNIL, qui a demandé de plus amples précisions à la mairie niçoise. La CNIL a en effet des standards d'exigence en matière de proportionnalité entre les objectifs poursuivis par les autorités et le respect des libertés individuelles. La mairie n'a visiblement pas donné suite à ces demandes[29].

Les gares et les transports publics constituent également un terrain d'expérimentation régulier de technologies prédictives de comportements délinquants. Certains agents des services internes de sécurité des gares du territoire ont ainsi expérimenté l'utilisation de caméras individuelles dans un but préventif, de collecte de preuves ou dans le cadre de procédures judiciaires[30]. À titre d'exemple, certaines communes ont fait appel à des sociétés privées pour détecter les personnes portant ou non un masque dans les transports en commun, lors de la crise sanitaire en 2020[31]. La CNIL s'est formellement opposée à la mise en place de tels systèmes, dans la mesure où les personnes ne pouvaient exercer un droit d'opposition à cette analyse technologique[32]. Néanmoins, la CNIL admet l'utilité technique de la vidéo « augmentée » en ce qu'elle permet « d'une part, d'automatiser l'exploitation des images captées par les caméras, qui était auparavant humaine ; d'autre part, ils offrent une puissance d'analyse de certains paramètres qu'un œil humain ne pourrait pas atteindre »[33].

Finalement, peu de décisions politiques ou officielles ont eu pour but d'interdire l'utilisation de ces technologies. Seul le fait pour les autorités de ne pas avoir donné suite aux tests effectués subsiste aujourd'hui. Les débats parlementaires ont néanmoins fait barrage à l'ouverture à l'utilisation par la Police et la Gendarmerie de certaines

[28] V. par exemple : https://www.lemonde.fr/pixels/article/2019/08/28/reconnaissance-faciale-la-cnil-tique-sur-le-bilan-de-l-experience-nicoise_5503769_4408996.html

[29] *Ibid*.

[30] Décret nº 2016-1862 relatif aux conditions de l'expérimentation de l'usage des caméras individuelles par les agents des services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens, (23 décembre 2016), *JORF*, 27 décembre 2016.

[31] Décret n°2021-269 relatif au recours à la vidéo intelligente pour mesurer le taux de port du masque dans les transports (10 mars 2021) *JORF*, 11 mars 2021.

[32] CNIL, Délibération nº 2020-136 portant avis sur un projet de décret relatif au recours à la vidéo intelligente pour mesurer le taux de port de masque dans les transports, 17 décembre 2020.

[33] CNIL, *Caméras dites "intelligentes" ou "augmentées" dans les espaces publics*, (2022), 7.

technologies[34]. Une décision récente du Parlement européen, qui s'oppose aux systèmes de police prédictive, est ainsi reprise[35].

1.3 Perception et réception de la police prédictive en France

1.3.1 Réticences inspirées par l'expérience étrangère

L'État français n'a donc pas de projet global de déploiement, d'utilisation ou d'expérimentation de la police prédictive à ce jour. Cette frilosité s'explique en partie par le constat de l'expérience étrangère, et notamment américaine. Différentes villes des États-Unis ont, dès les années 2010, mis à disposition des autorités locales des dispositifs de police prédictive, majoritairement spatiotemporels. Certaines villes ont également eu pour ambition de mettre en œuvre des techniques de prédiction du passage à l'acte, et donc des algorithmes de traitement de données relatives à la personne. Des biais discriminatoires ont été allégués par l'organisation Propublica[36], à propos d'un logiciel utilisé par les autorités de Fort Lauderdale. Aucune suite judiciaire n'a cependant été donnée à ces accusations, à l'inverse de la ville de New York qui s'est vue contrainte de rendre compte de l'utilisation du logiciel Palantir Gotham[37], devant les juges américains[38]. Il était effectivement demandé au département de police de préciser quels types de données étaient utilisées, quels systèmes et modèles algorithmiques étaient mis en œuvre, la durée de l'expérimentation et de la conservation, etc. Le manque de transparence de l'initiative new-yorkaise et les risques de biais peu anticipés par les autorités sont des exemples peu engageants, justifiant la réticence française vis-à-vis des technologies de police prédictive[39].

1.3.2 Attentes et méfiances du public et des institutions

La CNIL est l'un des garants de la protection des données à caractère personnel et joue un rôle crucial dans le contrôle de l'usage de certaines technologies qui s'apparentent pour certaines de plus en plus à de la police prédictive. En tant que telle, la Commission entretient une réticence quant à l'introduction de ces technologies en France, dans la

---

[34] V. en ce sens les débats parlementaires relatifs au projet de loi sur la responsabilité pénale et à la sécurité intérieure, notamment à propos de l'article additionnel relatif à la reconnaissance faciale, https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000043806985/.

[35] Résolution du Parlement européen n° P9_TA(2021)0405, sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales, (6 octobre 2021).

[36] V. en ce sens : https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. *Propublica* est une organisation non gouvernementale à but non lucratif, spécialisée dans le journalisme d'investigation.

[37] *Palantir* est l'une des entreprises américaines les plus populaires en matière de technologies algorithmiques et de traitement de données proposées aux États et entreprises.

[38] V. en ce sens : https://www.brennancenter.org/our-work/court-cases/brennan-center-justice-v-new-york-police-department

[39] Ministère de l'Intérieur, (2019) *op. cit.*, (n 1) 40,41.

mesure où le cadre juridique est selon elle insuffisant pour permettre un respect des garanties individuelles[40].

Le rapport de la Mairie de Nice consacre quelques pages aux avis collectés auprès du public quant à la perspective d'utilisation de la reconnaissance faciale dans la ville, et l'avis des professionnels ayant participé aux essais. L'avis du public, récolté sur un panel de 821 personnes[41] dont 52,4% sont retraités, 44% actifs et 3,7% étudiants, s'avère plutôt favorable à la mise en œuvre de la reconnaissance faciale dans certaines situations déterminées[42]. Il est précisé que dans ces proportions, les personnes soumises au sondage et favorables à la pérennisation de la technologie sont attentives au manque d'encadrement juridique de cette potentialité. De la même manière, les professionnels – agents de la police municipale – expriment dans différents rapports annexes leurs avis enthousiastes, la technologie garantissant un renforcement de la sécurité publique et pouvant pallier, selon certains, le manque de moyens humains et matériels alloués aux forces de sécurité sur le territoire. Les avis récoltés dans ce rapport sont à aborder avec prudence, dans la mesure où seul un panel réduit a été interrogé. La police prédictive en tant que notion à part entière reste plus une abstraction, voire une fiction pour le public en France. Il serait de ce fait difficile d'interroger la population sur sa perception d'une telle technologie. En revanche, des sondages auprès de la population ont pu être effectués concernant la reconnaissance faciale en 2021[43], montrant que la population reste ouverte à son expérimentation dans l'espace public.

1.3.3 Perception des médias

Si l'on se cantonne uniquement aux systèmes de police prédictive, les médias les présentent, là encore, comme une technologie issue de la fiction, mais s'implantant de plus en plus dans le réel, parfois présentée comme dangereuse pour les garanties individuelles[44]. Les médias français ont plus l'occasion de présenter ces technologies comme des exemples étrangers, tels que les systèmes chinois ou américains. Mais les essais opérés dans les différentes villes de France ont occasionné de vives réactions

[40] V. *infra* sur les pistes d'encadrement juridique.
[41] Mairie de Nice, *op. cit*., (n 25), 13
[42] *Ibid*, 19
[43] J.-M Mis., *Pour un usage responsable et acceptable par la société des technologies de sécurité* (Rapport au Premier Ministre, 2021) <www.vie-publique.fr/rapport/281424-pour-un-usage-responsable-et-acceptable-par-la-societe-des-technologies>, consulté le 27 mai 2023, 32.
[44] V. par exemple : France Culture, « « Police prédictive, LegalTech : les algorithmes font-ils la loi ? » (8 octobre 2021) ; D. Leloup, « A Los Angeles, l'ombre de Palantir sur un logiciel décrié de police prédictive » (*Le Monde*, 9 octobre 2018) ; H. Guillaud, « Police prédictive (1/2) : dépasser la prédiction des banalités ? » et « Police prédictive (2/2) vers une prédiction responsable ? », (*Le Monde*, 24 et 27 septembre 2017).

médiatiques, qui questionnent de plus en plus ce qui est appelé la surveillance de masse[45].

1.3.4 Perception professionnelle et académique

Concernant les professionnels, il semblerait que la poursuite des tests effectués n'ait pas abouti, ou du moins n'ait pas été renouvelée. Une question subsiste cependant concernant la formation en matière technologique, qui reste un problème majeur et peut expliquer la réticence éventuelle de certains corps de la sécurité. Néanmoins, l'analyse décisionnelle ne semble pas totalement rejetée par les forces de sécurité, comme le soulignent les différents rapports de la police niçoise.

En ce qui concerne les cercles doctrinaux, académiques et universitaires, mais également intellectuels, une méfiance générale se remarque. Les réticences et inquiétudes portent principalement sur les atteintes potentielles aux libertés et principes fondamentaux de la procédure pénale. Le Rapport CHEMI sur l'encadrement des risques de la police prédictive rendu en mars 2019 en est un exemple, dans la mesure où les contributions sont toutes issues de professeurs d'universités ou d'écoles françaises[46]. D'autres travaux en la matière adoptent cette même approche[47] réticente.

1.3.5 Problématique de la coopération public-privé

Enfin, il convient de mentionner la tentative de coopération de la Direction Générale de la Sécurité Intérieure (DGSI) avec l'entreprise américaine Palantir, en 2016[48]. L'entreprise étant financée par la Central Intelligence Agency (CIA), des réserves ont rapidement été émises quant à la signature d'un contrat avec l'organe français de sécurité intérieure. La crainte principale résidait dans l'échange de données françaises, voire confidentielles, avec une entreprise entretenant des liens si proches avec un organe fédéral américain. Le système de Cloud, système d'accès aux données à distance, complexifie les processus de protection de ces informations. Le projet de partenariat a été depuis abandonné, une solution de préservation de la souveraineté numérique et de favorisation des entreprises françaises ayant été préférée. Depuis, un groupe de travail dirigé par le Groupement des industries de défense et de sécurité terrestres et aéroterrestres (GICAT) a donné

[45] Terme repris par le Parlement européen, Résolution du Parlement européen, op. cit. (n), §H

[46] Les Professeurs Céline Castets-Renard et Laurent Perrussel enseignent à l'Université Toulouse Capitole, le Professeur Philippe Besse à l'INSA Toulouse et le Professeur Jean-Michel Loubès à l'Université Paul Sabatier.

[47] V. par exemple : B. Benbouzid, « De la prévention situationnelle au predictive policing. Sociologie d'une controverse ignorée » (2015) XII *Champ Pénal* ,<https://doi.org/10.4000/champpenal.9050> consulté le 27 mai 2023.

[48] Assemblée Nationale, Commission de la défense nationale et des forces armées, *Audition de M. Guillaume Poupard* (Compte rendu n°53, 2018) 15.

naissance à une initiative, le Cluster Data Intelligence, regroupant plus d'une vingtaine de sociétés françaises devant collaborer et apporter leur expertise en matière technologique à la DGSI[49].

La Direction Générale des Armées (DGA) a également investi dans la création du projet Architecture de Traitement et d'Exploitation Massive de l'Information multi-Source (ARTEMIS), visant à constituer un big data et le développement de solutions d'IA pouvant servir le secteur des armées[50].

Le besoin sécuritaire et les politiques étant attachées aux systèmes d'IA et de police prédictive sont prégnants. L'exemple des États-Unis montre que le predictive policing, dans sa conception de stratégie policière, s'est développée sur la base de théories managériales institutionnelles, l'exacerbation des politiques sécuritaires et l'intérêt porté au progrès technologique. L'impulsion quant à l'utilisation de ces systèmes émane également d'une concurrence sécuritaire interétatique et technologique. Le rôle que jouent les sociétés privées en matière de spécialisation technique est également un facteur d'incitation auprès des États.

Ainsi, les exemples d'expérimentations nationales et d'encadrement de certaines technologies laissent à penser que les institutions ont pour ambition de développer leur usage dans le cadre de la protection de l'ordre public ou d'appui du travail policier[51]. Pour l'instant les incitations réelles sont plutôt locales, des communes ayant déjà eu l'occasion de tester ces technologies.

Ces réticences et balbutiements en matière prédictive s'expliquent en réalité par les menaces que ces technologies représentent pour les droits et libertés individuelles. Les garanties procédurales et personnelles ne sont, au sens de la réglementation européenne, des exigences de la CNIL voire du Conseil constitutionnel, pas encore suffisamment respectées. Il s'agirait en effet de mener une réflexion plus poussée quant aux encadrements juridiques de ces techniques.

2 Pistes juridiques nationales

2.1 Cadre normatif

Le cadre normatif doit prendre en compte les caractéristiques des outils technologiques utilisés. Les systèmes d'IA utilisés en France sont de plusieurs ordres, qu'il s'agisse de logiciels d'aide à l'enquête policière (Anacrim), d'analyse sérielle (SALVAC) ou de technologies d'analyse audiovisuelle (la reconnaissance faciale, la vidéosurveillance).

[49] V. par exemple : https://www.gicat.com/cluster-data-intelligence/
[50] V. par exemple : https://www.jeunes-ihedn.org/2020/le-defi-du-big-data-et-de-lintelligence-artificielle-pour-le-monde-de-la-defense-2e-partie/
[51] V. par exemple : CNIL, Délibération n°2021-011 portant avis sur une proposition de loi relative à la sécurité globale, (26 janvier 2021).

Les logiciels comme Anacrim ou SALVAC s'apparentent à des systèmes de raisonnement machine, dans la mesure où les données sont triées, ordonnées, optimisées. Ces techniques sont particulièrement utiles pour les crimes sériels ou les enquêtes en matière de criminalité organisée ou trafic de stupéfiants comprenant de nombreux protagonistes et éléments relationnels. En ce sens, il s'agit plus d'un raisonnement machine que d'apprentissage autonome pur qui est utilisé officiellement par les autorités et les forces de sécurité. Si les seuls essais concrets de police prédictive – Predvol et Paved – se concentraient sur des atteintes aux biens, les technologies d'analyse sérielle ont des domaines d'application plus larges et peuvent traiter des atteintes aux personnes.

Concernant les systèmes de reconnaissance faciale, qui ne peuvent être utilisés qu'a posteriori, le raisonnement repose sur l'identification à partir d'images déjà fournies à l'IA, et correspond parfois aux techniques d'identification biométrique. La reconnaissance faciale, qu'elle soit fixe ou attachée à un drone, correspond plus à de l'apprentissage machine par renforcement. En étalonnant ses résultats sur la base de données fournie, l'algorithme évolue et affine l'authentification et la détection des personnes. Dans certains cas, les données sont issues de fichiers de sécurité, d'enquêtes et de procédures pénales passées. Les données dites sensibles, telles que certaines données biométriques, restent hors du champ de la collecte et du traitement[52].

2.1.1 Réglementations et soft law

Il n'existe pas de règles nationales visant spécifiquement et textuellement les systèmes de police prédictive. En revanche, des textes diffus, à valeur législative ou réglementaire, concernent les différentes technologies – drones, vidéosurveillance, reconnaissance faciale – et la protection des données à caractère personnel. Une grande partie de ces textes émanent de l'UE[53], mais prennent également la forme de rapports parlementaires, questions à l'Assemblée nationale, rapports et avis de la CNIL. Ces derniers types de textes, peu contraignants, abordent cependant plus largement l'usage des technologies existantes qui pourraient déboucher sur des enjeux prédictifs.

Certains textes législatifs ou réglementaires récents ont tenté d'insérer dans la pratique française des technologies s'approchant des ambitions prédictives constatées à

[52] Règlement (UE) 2016/679 op.cit. (n 20), art. 9.

[53] V. par exemple : Règlement (UE) 2016/679 *op.cit.* (n 20) ; Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, dite Police-Justice (27 avril 2016), JOUE L 119/89.

l'étranger[54]. Ainsi, la loi Sécurité globale[55] a eu en partie pour projet l'encadrement de l'utilisation de drones par les autorités, notamment dans la ville de Paris, afin d'anticiper les violences lors de rassemblements, de manifestations, ou encore d'actes terroristes[56]. Lors de la crise Covid, le Conseil d'État (CE) avait déjà été confronté à la nécessité de rendre une ordonnance restreignant l'utilisation de cette technologie par la préfecture de police de Paris[57]. Le Conseil enjoignait ainsi l'État français d'encadrer la pratique, considérée comme un outil « pour la réalisation de missions de police administrative »[58]. Un pourvoi demandant l'annulation de ces mesures était néanmoins formé et favorablement accueilli le 22 décembre 2020 par le Conseil d'État[59]. Cette décision catalyse les différentes exigences émises par la juridiction administrative au cours de l'année 2020, et précise notamment qu'il revient au législateur de fixer les conditions d'utilisation d'un tel dispositif[60], afin de ne pas porter atteinte au droit à la protection des données à caractère personnel et du droit au respect de la vie privée.

Après une première tentative d'encadrement du législateur[61], la loi du 24 janvier 2022[62] a finalement introduit l'utilisation des drones dans certaines procédures telles que l'enquête ou l'instruction portant sur un crime ou un délit puni d'au moins trois ans d'emprisonnement, sur la recherche des causes de la mort ou d'une disparition ou la recherche d'une personne en fuite[63]. La police nationale et la Gendarmerie nationale peuvent aussi y recourir dans des buts de prévention des atteintes à l'ordre public.

2.1.2 Jeux Olympiques de Paris 2024.

Récemment, le projet de loi sur la mise en œuvre des dispositifs de sécurité entourant les Jeux olympiques de Paris de 2024 a finalement été voté par l'Assemblée nationale et le

---

[54] V. par exemple le projet de loi relatif à la responsabilité pénale et à la sécurité intérieure faisant suite à la censure du Conseil constitutionnel de l'article 8 de la loi n°2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, visant l'utilisation de drones.

[55] Loi n°2021-646 pour une sécurité globale préservant les libertés (25 mai 2021,) *JORF* n°120 du 26 mai 2021.

[56] *Ibid*. Article 47. La proposition de loi n°3452 visait initialement à introduire deux nouveaux articles L.242-5 et L.242-6 dans le Code de la sécurité intérieure, afin de créer un régime juridique d'encadrement du recours à la captation d'images par des moyens aéroportés.

[57] CE, ord., 18 mai 2020, *La Quadrature du net at a.*, req. n°440441.

[58] *Ibid*, §8.

[59] CE, 22 décembre 2022, *La Quadrature du net*, req. n°446155.

[60] Le Conseil d'État reprend notamment les exigences émises dans un décret n°2020-260 du 16 mars 2020, ou dans un avis du 20 octobre 2020, n°401214.

[61] Le Conseil constitutionnel a déclaré l'article 47 de la loi Sécurité globale non conforme à la Constitution dans une décision n°2021-817 DC du 20 mai 2021.

[62] Loi n°2022-52 relative à la responsabilité pénale et à la sécurité intérieure (24 janvier 2022,) *JORF* n° 20 du 25 janvier 2022.

[63] *Ibid.*, la loi insérant un encadrement de ces pratiques aux articles L.242-1 et suivants du code de la sécurité intérieure et aux articles 230-47 et suivants du code de procédure pénale.

Sénat[64]. Dans son rapport, la Commission mixte paritaire cite le Gouvernement qui estimait nécessaire, à l'occasion de ce projet de loi, « de reporter la création d'un régime juridique commun à l'ensemble des "images de sécurité" »[65] ; l'article 6 unifiant ces cadres de recours à la vidéoprotection. Ce même article substitue par ailleurs les termes de « transmission et enregistrement d'images prises sur la voie publique » par ceux de « système de vidéoprotection » si la finalité poursuivie est antiterroriste. Dans un tel cas, le projet de loi exclut expressément que ce système de récolte et de traitement de données soit soumis au régime de la loi Informatique et Libertés de 1978.

L'article 7 du projet de loi reste l'élément le plus prégnant du projet de loi, visant à instaurer un cadre expérimental du traitement algorithmique couplé à des dispositifs de vidéoprotection et de captation d'images par voie aéroportée. Les caméras « intelligentes » ne sont en effet pas utilisées actuellement sur le territoire français, exception faite des expérimentations effectuées dans les transports publics[66]. Cet essai étant circonscrit dans le temps[67], il est également soumis au régime juridique du RGPD et de la loi Informatique et Libertés. Outre ce cadre général, il est à noter que le texte interdit tout de même le recours à l'identification biométrique ou à la reconnaissance faciale[68]. L'ensemble de l'article 7 établit ainsi les conditions dans lesquelles un tel système pourra être mis en œuvre lors des manifestations sportives ou rassemblements publics. Sans être exhaustifs, nous citerons certaines de ces dispositions :

> Une information préalable du public devra être mise en œuvre, par tout moyen – laissant en suspens la question de ces moyens employés : signalisation visuelle, sonore, permanente …
>
> Le système permettant le signalement d'évènements particuliers prédéterminés par le responsable de traitement, ce signalement ne peut fonder une décision individuelle ni un acte de poursuite. La décision humaine reste maîtresse.
>
> La CNIL est désignée comme autorité de contrôle au même titre qu'elle l'est à l'article 8 de la loi Informatique et Libertés. L'Agence nationale de la sécurité des systèmes d'information assure quant à elle le respect des exigences de cybersécurité, que le développement du traitement soit assuré par l'État ou un tiers.

[64] Loi n° 2023-380 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (19 mai 2023), *JORF* n° 116 du 20 mai 2023.
[65] Assemblée Nationale, Rapport n°496 sur le projet de loi modifié relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, (4 avril 2023).
[66] V. supra p.5
[67] Débutant au jour de publication du texte, ce dernier fixe le terme de l'expérimentation au 31 mars 2025.
[68] V. ce rapport, troisième partie : Droit de la preuve et IA.

Une analyse d'impact doit être menée pour toute initiative d'expérimentation de cette technique, concernant en particulier les garanties présentées en matière de protection des données à caractère personnel.

Enfin, le texte prévoit également les exigences qui devront entourer les données d'entraînement de l'algorithme ; données qui pourront notamment relever de la collecte autorisée à l'article L.252-1 du code de la sécurité intérieure.

Ce texte est à ce jour la perspective française approchant le plus concrètement les prémices de techniques s'apparentant à la technologie prédictive. Si le terme de prévention est toujours privilégié quant au but mené par ce recours algorithmique, la loi mentionne également la détection, floutant de ce fait les lignes de démarcation qui circonscrivent ces technologies et leurs capacités en matière pénale.

2.2 Jurisprudence

Les essais effectués s'approchant de systèmes de police prédictive n'ayant pas été effectués dans un cadre officiel, les autorités, la Cour de cassation, le Conseil d'État ou le Conseil constitutionnel n'ont pas eu l'occasion de rendre de décisions en ce sens. Précisons une nouvelle fois que la CNIL, autorité administrative, est l'organe ayant cependant rendu régulièrement des avis et rapports concernant ces technologies de surveillance s'apparentant à l'aide à l'anticipation de la délinquance[69].

La CNIL considère ainsi les différentes technologies (drones, reconnaissance faciale), comme des traitements de données à caractère personnel au sens du RGPD. À ce titre, un tel traitement doit être encadré par des dispositions législatives ou réglementaires précises. La commission rappelle également que les autorités doivent être particulièrement vigilantes lorsque les données en cause sont des données dites sensibles. La collecte et le traitement des données à caractère personnel doivent de plus respecter les différents principes du droit pénal et de la procédure pénale.

Ce type de décisions émanant des autorités régulatrices a pu être rendu concernant des systèmes tels que les drones, par exemple[70].

2.3 Garanties de fond

Les garanties telles que la fiabilité, l'impartialité et l'efficacité ne sont pas expressément prévues par des textes ou normes internes. Les textes européens transposés en France, ou des lois relatives à la sécurité intérieure, à travers leurs dispositions, impliquent le

[69] V. par exemple : CNIL Délibération n° SAN-2021-003 du 12 janvier 2021, sur l'utilisation des drones, notamment lors du confinement et la mise en œuvre des mesures dans le cadre de la crise sanitaire.
[70] Cons. const. n°2021-817 DC du 20 mai 2021.

respect de certaines de ces garanties telles que le traitement licite, loyal et transparent des données à caractère personnel[71].

De même, dans la mesure où les technologies décrites ne peuvent pour l'instant pas fonder de décision pénale individuelle[72], aucune indemnisation d'individus qui seraient éventuellement concernés n'est pour l'instant prévue. Cependant, une telle interdiction de traitement automatisé individuel étant issue de la directive dite « Police-Justice » du Parlement européen, transposée en droit français[73], cette dernière considère tout de même qu'un dommage subi du fait d'un traitement automatisé devrait ouvrir droit à réparation :

> « Tout dommage qu'une personne pourrait subir du fait d'un traitement qui constitue une violation des dispositions adoptées en vertu de la présente directive devrait être réparé par le responsable du traitement ou toute autre autorité compétente en vertu du droit des États membres. (…) Lorsqu'il est fait référence à un traitement illicite ou qui constitue une violation des dispositions adoptées en vertu de la présente directive, cela concerne aussi un traitement qui constitue une violation des actes d'exécution adoptés en vertu de la présente directive. Les personnes concernées devraient recevoir une indemnisation complète et effective pour le dommage subi. »[74]

En effet, les technologies automatisées utilisées par le système pénal et policier engendrant des décisions pénales (l'exemple le plus classique étant celui de la détection des infractions routières, du dépassement de vitesse maximale autorisée par exemple), sont toujours susceptibles de voies de recours.

2.4 Labellisation des systèmes développés par les entreprises

Si aucun texte français n'est à l'initiative de certifications ou labels à l'égard des systèmes basés sur l'IA, le Règlement Général sur la Protection des données[75], applicable directement en France, conseille « la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement ».[76] Une attention est

[71] Loi Informatique et Liberté modifiée par l'Ordonnance n°2018-1125 du 12 décembre 2018, art. 4. L'article 4 reprends les termes de l'article 5 du Règlement général sur la protection des données du 27 avril 2016.
[72] Directive (UE) 2016/680 *op.cit* (n 53), Article 11
[73] Loi n° 2018-493 relative à la protection des données personnelles (20 juin 2018), *JORF* n° 141 du 21 juin 2018.
[74] Directive UE) 2016/680 *op.cit* (n 53), Considérant 88
[75] Règlement (UE) 2016-679 *op.cit*.(n 53).
[76] *Ibid*, art. 42

également portée sur la cybersécurité des données et de ces systèmes. Nous pourrions donc entrevoir, en France, des exigences de brevets certifiant qu'une technologie est sûre en matière de cybersécurité. Le concept de « privacy by design » est également recherché par un nombre croissant d'entreprises et notamment des sociétés françaises qui ont vocation à s'associer avec l'État français[77]. Ce concept de protection des données dès la conception ou par défaut, est textuellement prévu par l'article 5 du RGPD :

> « Compte tenu de l'état des connaissances, des coûts de mise en œuvre de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ».

Ces différents éléments issus des exigences européennes permettent de présumer de la construction juridique des labélisations de technologies prédictives par les entreprises qui les proposeraient aux services de sécurité français. Cela n'a néanmoins pas encore permis d'aperçus en matière d'engagement de la responsabilité des entreprises qui fourniraient à l'État de tels dispositifs. Qui plus est, cela impliquerait de composer avec la responsabilité de l'État dans la mesure où de telles technologies prédictives – voire les technologies actuelles – se fonderaient sur des données issues de fichiers pénaux et utilisées par les autorités et forces de sécurité françaises.

3 Principes généraux du droit

Le droit à l'égalité reste un principe fondamental en procédure pénale, régissant ainsi une potentielle utilisation de techniques de police prédictive.

Ces discussions existent en France, non pas à des fins de police prédictive, mais pour toute technologie utilisée à des fins pénales et celles s'en approchant – les derniers débats en date portant sur la surveillance par drones ou la reconnaissance faciale.

La protection tient au type de données collectées – données à caractère personnel, données sensibles – à la durée de la conservation des données, au traitement et aux fins du traitement.

[77] J-M. Mis (2021) *op. cit.* (n 43), 13

La protection des données à caractère personnel est intimement – si ce n'est nécessairement – liée au droit au respect de la vie privée. C'est donc par le truchement de ce dernier que le cadre juridique de la protection des données personnelles se crée en France. La Cour européenne des droits de l'Homme rattache ainsi ce droit au fondement de l'article 8. D'un point de vue interne, la valeur constitutionnelle du droit à la vie privée a pu être expressément reconnue dès 1982[78].

L'atteinte au droit à la vie privée en matière pénale a récemment été discutée concernant les durées de conservation de ces données dans le FNAEG (Fichier national automatisé des empreintes génétiques)[79]. Dans ce cadre-là, les individus concernés par la collecte disposent de voies de recours afin d'obtenir leur effacement, sous certaines conditions. Des délais de conservations légaux sont prévus[80], mais la personne concernée par le fichage peut adresser une demande anticipée d'effacement de ses données au procureur de la République[81]. Si ce dernier refuse, le justiciable peut s'adresser au juge des libertés et de la détention puis, en dernier recours, au président de la chambre de l'instruction. Des voies de contestations existent donc dans ce cadre-là, qui pourraient être transposées ou adaptées à l'utilisation de technologies prédictives.

Au-delà du droit à la vie privée, l'utilisation de telles technologies questionne quant au respect du droit à l'égalité[82] et plus généralement quant à la conciliation entre libertés et sécurité. En matière pénale, les corolaires de l'égalité de traitement sont le principe de l'égalité des armes, l'une des exigences du droit à un procès équitable[83]. Ces techniques ne doivent pas impacter le respect de l'exercice des droits au procès ni leur équilibre entre parties – au risque d'aller à l'encontre des dispositions de l'article préliminaire du code de procédure pénal[84].

En réalité, l'utilisation de la police prédictive et de systèmes fondés sur l'IA renvoie classiquement à la question de la conciliation entre exercice des droits, respect des libertés, et sécurité. En ce sens, le principe de proportionnalité est cardinal en procédure pénale, se retrouvant dès l'article préliminaire du code de procédure pénale. Ainsi, à titre d'exemple, « au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction »[85]. Le Conseil

[78] Cons. constit. n°82-148 DC, 14 décembre 1982.
[79] Crim. 8 décembre 2021, n°20-84.201 ; CEDH 22 juin 2017, n°8806/12, *Aycaguer c/ France*
[80] Art. R.53-14 C. pr. pén.
[81] Art. 706-54-1 C. pr. pén.
[82] Art. 6 CEDH.
[83] Art. 6§1 CEDH.
[84] « *I. – La procédure pénale doit être équitable et contradictoire et préserver l'équilibre des droits des parties. (…) Les personnes se trouvant dans des conditions semblables et poursuivies pour les mêmes infractions doivent être jugées selon les mêmes règles* ».
[85] Art. prél., III, C. pr. pén.

constitutionnel exige donc de l'usage de telles technologies, soit qu'il soit nécessaire pour atteindre certains objectifs de maintien de l'ordre public (lutte contre la criminalité et sa prévention, recherche d'infractions), soit qu'il se concilie de manière proportionnée avec le respect des droits et libertés individuelles – droit à la vie privée, liberté d'aller et venir par exemple[86].

Le droit à la présomption d'innocence pourrait également être menacé par l'utilisation de technologies de police prédictive. Ces mêmes principes de proportionnalité et de nécessité, tels que reconnus par le Conseil constitutionnel, s'exercent donc dans une certaine mesure à l'égard du respect de la présomption d'innocence, principe cardinal de la procédure pénale[87].

3.1 Doctrine

De manière générale, la doctrine – tout comme la CNIL – reste méfiante quant à la mise en œuvre concrète de la technologie prédictive au vu des risques d'atteinte au droit à la vie privée que font déjà courir certains dispositifs[88], également mis à mal par certains acteurs privés qui se sont vus sanctionnés par la CNIL[89]. Celle-ci, en formation restreinte, a en effet un pouvoir sanctionnateur en cas de manquement au RGPD ou à la Loi « Informatique et Libertés ». Les sanctions prononcées vont du rappel à l'ordre à la prononciation d'une amende dont le montant peut s'élever jusqu'à 20 millions d'euros dans certains cas[90].

3.2 Perspectives

La police prédictive représente l'ensemble des systèmes basés sur des techniques d'IA poursuivant un objectif plus poussé que le simple travail policier de prévention et de résolution. Il est nécessaire de définir précisément la technique et les limites de son champ d'application dans le cadre de son utilisation par les forces de sécurité. La France entretient aujourd'hui une certaine réticence à l'utilisation de ces technologies par les forces de police du territoire, les expériences étrangères n'étant pas exemplaires en

[86] Cons. constit. n°80-127 DC du 20 janvier 1981 ; Cons. constit. n°2003-467 DC du 13 mars 2003 ; Cons. constit. n°2008-562 DC du 21 février 2008.
[87] Cons. constit. n°81-127 DC du 20 janvier 1981.
[88] V. par exemple : C. Mequesne Roth, « Pour un encadrement démocratique de la reconnaissance faciale », (2020), *Recueil Dalloz*, 1568.
[89] CNIL, 17 octobre 2022, délib. n° SAN-2022-019. En effet la CNIL, après une mise en demeure, a sanctionné la société Clearview utilisant la technologie de reconnaissance faciale dans le cadre de l'exploitation de son moteur de recherche. Il lui était reproché de ne pas avoir déterminé de base légale pour ce traitement, qui permettrait aux usagers l'exercice des droits d'accès et d'effacement de leurs données de la plateforme.
[90] Art. 83 RGPD.

matière de conciliation avec le respect des droits et libertés fondamentaux. Il n'en reste pas moins que la compétitivité sécuritaire interétatique est largement entretenue par les possibilités technologiques actuelles, voire exacerbée par l'immixtion des sociétés de sécurité dans de tels domaines. L'exemple de la reconnaissance faciale et de son expérimentation diffuse montre bien que l'usage de ces dispositifs ne pourra être repoussé indéfiniment, mais qu'il serait plus judicieux d'anticiper son utilisation par le droit. De grands axes peuvent être posés en amont, tel que la protection de l'anonymat dans l'espace public, ou la sauvegarde du consentement à l'exploitation de certaines données.

Un premier temps consisterait par exemple dans le fait d'encadrer ce type d'essai localisé. La CNIL exige une analyse d'impact relative à la protection des données antérieurement à la mise en œuvre d'un outil de traitement, devant comprendre le détail technique et opérationnel de l'outil, la description juridique du respect que l'outil présente vis-à-vis des droits et libertés fondamentaux ainsi que les risques qu'il pourrait présenter pour la protection des données et de la vie privée. C'est sur ce dernier point que les précisions ont pêché dans le cadre des essais niçois. En ce sens, il faut effectuer un travail plus poussé de coopération et de transparence avec les entreprises productrices de logiciels au service des autorités publiques. Sans pouvoir exiger la publication totale des algorithmes créés, du fait de la protection de certains brevets, une transparence minimale devrait être respectée quant aux types de techniques utilisées, ce qu'elles impliquent en matière de données utilisées, si cela nécessite une conservation prolongée, etc.

La souveraineté numérique est primordiale, dans la mesure où la collaboration avec des entreprises françaises sera plus sereine dans l'exploitation des données – l'exemple de la société Palantir, proche de la CIA, en est une preuve.

Une difficulté réside également dans le fait que l'interconnexion des fichiers de police est la plupart du temps interdite[91]. Celle-ci doit être préservée, dans la mesure où le recours à certaines technologies telle que la police prédictive, pour être plus performantes, pourraient demander l'interconnexion et la circulation de données entre fichiers et systèmes de traitement. Cela peut se faire par une évaluation et un suivi régulier, tant des technologies déjà utilisées que de celles qui seraient expérimentées. De la même manière, une vraie réflexion doit être menée quant à la formation des professionnels qui seraient amenés à utiliser ces technologies, voire que ceux-ci accompagnent leur développement dès les premiers essais non officiels. La coopération entre le secteur privé et le secteur public pourrait ainsi être harmonieuse.

Enfin, plus concrètement, ces technologies, tant pour être efficaces que non discriminatoires, ne devraient pas s'appliquer uniquement à certains quartiers déjà ciblés

[91] L'article 230-17 du code de procédure pénale interdit des utilisations à des fins administratives.

par la délinquance, et devraient élargir le spectre des infractions considérées. Par exemple, certains actes de la criminalité économique et financière, très présente sur les plateformes numériques, sont tout aussi sujets à la détection algorithmique et à l'anticipation.

DEUXIEME PARTIE : JUSTICE PREDICTIVE

Emmanuelle GINDRE *

1 Questions générales

1.1 Définition de la notion de justice prédictive en France

Si la notion de justice prédictive, dans une acception contemporaine, semblait exister dans d'autres États dès les années cinquante (aux États-Unis notamment, sous le nom de jurimetric ou legalmetric)[92], elle n'est que d'apparition plus récente en France. Son utilisation et son étude croissante sont datées de l'adoption de la Loi pour une République numérique du 7 octobre 2016[93], instaurant l'open data des décisions de justice. Cette loi ne définit pas pour autant la justice prédictive, qui n'en est qu'une conséquence, et il n'existe actuellement en France aucune définition normative ou jurisprudentielle de la notion de justice prédictive.

En revanche, la notion de justice pénale prédictive a une autre acception, plus ancienne, qui renvoie à la doctrine des positivistes italiens du XIXème siècle et à cette anticipation du crime résultant d'un « calcul probabiliste de récidive »[94]. Mireille Delmas-Marty la décrivait comme une application du principe de précaution: « Avec la fonction « prédictive », la dangerosité se substitue à la culpabilité, la punition est supplantée par la prévention des risques ou même la précaution face aux risques incertains (risques de risques). »[95]. Ainsi définie, la justice pénale prédictive apparaît plus circonscrite que la notion contemporaine, ne visant qu'à « prédire », pour prévenir, la récidive. Elle implique également un changement de paradigme, la justice prédictive s'opposant ici à la justice rétributive.

Ce n'est pas l'acception qui transparaît dans les réflexions actuelles sur la justice prédictive en France, même appliquée à la justice pénale. Il s'agit plus de prévoir l'issue d'un procès à partir des solutions passées, que de prédire des situations futures. Certains auteurs préfèrent alors parler de « justice prévisible »[96] ou de « prédiction judiciaire par

* 1. Univ. Polynésie française, GDI EA 4240, Tahiti, Polynésie française; 2. UPPA, IFTJ, EA 7504, Centre de recherche sur la justice pénale et pénitentiaire, Pau, emmanuelle.gindre@upf.pf .

[92] S. Lebreton-Derrien, « La justice prédictive, Introduction à une justice « simplement » virtuelle », (2018) *Arch. phil. droit* n°60, 3.

[93] Loi n° 2016-1321 pour une République numérique (7 octobre 2016), *JORF* 8 octobre 2016.

[94] J.-M. Brigant, « Les risques accentués d'une justice pénale prédictive », (2018) *Arch. phil. Droit* n°60, 46.

[95] M. Delmas-Marty, « Vers une justice pénale prédictive », in *Mélanges en l'honneur de Geneviève Giudicelli-Delage, Humanisme et Justice* (Dalloz 2017), 58.

[96] J.-M. Brigant, (2018), *op. cit.* 47 « d'autant plus que la prévisibilité est une exigence qui découle notamment de l'article 7 de la Convention européenne des droits de l'Homme ». V. aussi A. Coletta, *La prédiction judiciaire par les algorithmes*, (2022) Thèse sous la direction de G. Cerqueira, Université de Nîmes ;

les algorithmes »[97]. La Commission Nationale Consultative des Droits de l'Homme (CNCDH) préconise même l'usage de l'expression générique « systèmes algorithmiques d'aide à la décision » pour désigner les systèmes d'intelligence artificielle[98].

Un engouement doctrinal pour le sujet a pu être constaté après l'adoption de la loi précitée, qui ne masque pas la faiblesse de la recherche juridique en ce domaine[99], et plusieurs définitions nouvelles sont apparues après 2016. La terminologie « justice prédictive » a même fait son entrée dans le Lexique des termes juridiques 2018-2019 de S. Guinchard et Th. Debard[100]. Les définitions et terminologies relevées dans la doctrine varient sensiblement d'un auteur à l'autre, tant dans la nature que dans les fonctions de la justice prédictive.

1.1.1 Nature de la justice prédictive

La plupart des auteurs définissent la justice prédictive comme un outil ou un ensemble d'outils. Certains l'assimilent à « des instruments d'analyse de la jurisprudence et des écritures des parties »[101], d'autres à « un outil informatique, reposant sur une base de données jurisprudentielles », des algorithmes de tri voire des réseaux neuronaux[102].

Le rapport de la Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, sous la présidence de Loïc Cadiet, retient également cette nature: « Ensemble d'instruments développés grâce à l'analyse de grandes masses de données de justice » et utilisant notamment les probabilités[103].

D'autres auteurs définissent la justice prédictive comme une méthode : « méthode de résolution judiciaire des contentieux qui s'appuie sur le traitement de masse de données jurisprudentielles par des algorithmes. »[104].

Enfin, A. Coletta retient dans sa thèse la terminologie « prédiction judiciaire par les algorithmes » afin de désigner à la fois l'opération réalisée et les techniques employées[105].

T. Cassuto, « La justice à l'épreuve de sa prédictibilité », (2017) *AJ Pén.*, 334 : la justice doit être prévisible en application du principe de sécurité juridique.

[97] A. Coletta, (2022), *op. cit.* note 5, § 4 à 8.

[98] CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, (2022) A-2022-6, 4.

[99] Ibid. § 11 et 12.

[100] S. Guinchard, Th. Debard, *Lexique des termes juridiques 2018-2019* (Dalloz 2018).

[101] B. Dondero, « Justice prédictive : la fin de l'aléa judiciaire ? », (2017) *D.*, 532.

[102] R. Boucq, « La justice prédictive en question », (2017) *Dalloz actualités*, 14 juin https://www.dalloz-actualite.fr/chronique/justice-predictive-en-question , consulté le 14 nov. 2022.

[103] Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, *L'open data des décisions de justice* (Rapport à Madame la Garde des sceaux, Ministre de la Justice sous la présidence de L. Cadiet, 2017), 14.

[104] S. Guinchard, Th. Debard (2018) *op. cit.* note 9.

[105] A. Coletta, (2022), *op. cit.* note 5 § 6.

Quelle que soit la définition retenue, la justice prédictive est celle qui s'appuie sur des algorithmes, et principalement des algorithmes d'intelligence artificielle.

1.1.2 Fonctions de la justice prédictive

La justice prédictive est également définie par ses fonctions. Pour certains, elle a une fonction très générique et permet « de prédire ce que sera la jurisprudence future »[106]. Pour d'autres, sa fonction est plus précise et orientée en ce qu'elle permet « de prévoir autant qu'il est possible l'issue d'un litige. »[107], « d'anticiper quelles seront les statistiques de succès de tel ou tel argument juridique »[108], « annoncer le sens de la décision d'un juge sur une affaire donnée »[109].

La plupart des auteurs s'accordent sur le fait que la justice prédictive ne peut avoir pour fonction de déléguer à l'intelligence artificielle le fait de rendre une décision de justice, cette fonction devant rester une prérogative du juge. Pourtant, c'est cette fonction de rendre la justice qui semble ressortir de la définition de MM. Guinchard et Debard (« méthode de résolution judiciaire des contentieux »)[110].

Certains préfèrent alors parler de justice analytique[111] ou de justice algorithmique, insistant sur le fait que ce n'est pas la justice qui prédit mais qui serait prédite par des algorithmes : « la justice prédictive n'existerait donc pas en tant que telle, seul existerait l'outil algorithmique prédictif et, partant le(s) résultat(s) du calcul effectué. »[112].

Elle est également qualifiée d'outil d'aide à la décision ou « d'outil statistique de quantification des risques d'un litige »[113], en ce qu'elle permet de calculer les probabilités de succès d'une partie, le montant moyen de l'indemnité habituellement accordée, ou encore selon certains arguments commerciaux, d'identifier les arguments les plus convaincants. À cet égard, la justice prédictive apparaît davantage comme un outil d'aide à la décision pour les avocats et les parties, plutôt qu'un outil d'aide à la décision du juge.

Il découle de ces tentatives de définitions deux catégories de justice prédictive mises en évidence par M.-C. Lasserre[114]. La justice prédictive quantitative d'une part, permet « l'exploitation de données afin de délivrer une réponse juridique mais dépourvue d'une capacité de raisonnement humain autonome » : l'intelligence artificielle permet ici de

---

[106] B. Dondero (2017) *op. cit*. note 10.

[107] Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice (2017), *op. cit.*

[108] R. Boucq (2017), *op. cit.* note 11.

[109] A. Coletta, (2022), *op. cit.* note 5 § 7.

[110] S. Guinchard, Th. Debard (2018) *op. cit.* note 9.

[111] C. Guillard, « La justice prédictive et l'IA dans le procès pénal : risques et opportunités », (2020) *OJP* https://www.justicepenale.net/post/la-justice-prédictive-et-l-ia-dans-le-procès-pénal-risques-et-opportunités , consulté le 14 nov. 2022.

[112] S. Lebreton-Derrien, (2018), *op. cit.* note 1, 4.

[113] *Ibid.* 5.

[114] M.-C. Lasserre, « L'intelligence artificielle au service du droit : la justice prédictive, la justice du futur ? », (2017) *LPA* 30 juin (130), 6.

déterminer des probabilités, des tendances statistiques ou de chiffrer le montant d'un préjudice[115]. D'autre part, la justice prédictive cognitive, qui relève encore du domaine de la fiction, « renvoie à la délivrance d'une solution juridique par une machine mais suivant un raisonnement humain développé par l'intelligence artificielle. Dans ce cas, la justice prédictive se substitue à l'homme, engendrant la naissance d'un « juge-robot » »[116].

1.2 Pratique de la justice prédictive en matière pénale

Si la loi pour une République numérique, qui permettra à l'horizon 2025 une diffusion publique de l'ensemble des décisions de justice (les décisions pénales étant les dernières à être concernées), favorise le développement de start-ups et autres entreprises dites « legaltech » proposant des outils d'analyse et d'exploitation des décisions de justice, les outils informatiques ne sont pas une nouveauté dans le monde judiciaire.

En matière pénale, l'informatisation des juridictions, bien que longue et laborieuse[117], a permis d'implémenter certains logiciels développés au niveau local ou national par le Ministère de la Justice, proposant une aide à la rédaction, voire à la décision des magistrats. Ainsi, les tribunaux de grande instance, désormais tribunaux judiciaires, disposaient d'applications pénales nationales telles Micro-pénale, Mini-pénale et EPWIN ou des développements locaux (INSTRU, WINSTRU, WINEURS)[118], remplacés peu à peu à partir de 2009 par le logiciel de traitement des informations pénales Cassiopée[119]. Le traitement Cassiopée « permet d'assurer notamment la gestion des audiences, l'élaboration des décisions des juridictions de jugement et des pièces associées, la gestion des voies de recours et des recours en grâce, la gestion des requêtes, la gestion des scellés et des objets en gardiennage, la gestion de l'exécution des peines, la gestion des agendas, les systèmes d'alertes /relances, le système d'édition des documents, l'archivage électronique, les recherches/consultation intra et inter-juridictions. »[120]. En permettant l'enregistrement informatique de toute la chaîne pénale, l'application permet des recherches, des statistiques, des rapprochements notamment, qui assurent une meilleure

---

[115] E. Rottier, « Quelle prévisibilité pour la justice ? », (2018) *Arch. phil. Droit* n°60, 189.

[116] M.-C. Lasserre, (2017) *op.cit*. note 23.

[117] Cour des comptes, *Améliorer le fonctionnement de la justice, Point d'étape du plan de transformation numérique du Ministère de la Justice* (Communication à la Commission des finances du Sénat, janvier 2022).

[118] Sénat, *Rapport général sur la Justice* (n° 74 de M. Roland du LUART, fait au nom de la commission des finances, 2004), not. 130, L'informatique pénale.

[119] Chaîne Applicative Supportant le Système d'Information Opérationnel pour le PÉnal et les Enfants, traitement automatisé de données à caractère personnel, comprenant l'application dite « bureau d'ordre national automatisé des procédures judiciaires », qui peut avoir pour objet l'exploitation des informations recueillies à des fins de recherches statistiques, C. proc. pén. art. 48-1 et R. 15-33-66-4 et suivants.

[120] CNIL, Délibération n°2009-170 du 26 mars 2009 portant avis sur un projet de décret en Conseil d'État relatif au bureau d'ordre national automatisé des procédures judiciaires et au traitement dénommé « Cassiopée ». Nous soulignons.

information des magistrats ou des acteurs autorisés à consulter l'application et donc une prise de décision éclairée. Ce logiciel a été développé dès la fin 2003 par la société Atos et son installation a commencé dans les parquets dès 2008, puis dans les cabinets d'instruction et dans les tribunaux de grande instance. Il n'a été étendu aux Cours d'appel qu'en 2019[121].

Des perspectives de développement de ces traitements de données peuvent également s'appuyer sur le plan de transformation numérique du Ministère de la Justice, pour la période 2018-2022[122]. Le renforcement des systèmes d'informations, notamment Cassiopée, ou APPI[123] en matière pénale, permettra d'affiner les statistiques du Ministère de la Justice relatives au traitement des affaires pénales.

Cependant, la France accuse un réel retard dans le traitement numérique des informations judiciaires[124], et les logiciels comme Cassiopée rencontrent des difficultés de mise en œuvre qui font douter d'un déploiement à court terme d'applications de justice prédictive en matière pénale[125]. Notons que les applications actuellement utilisées par les magistrats et les acteurs de la chaîne pénale sont des solutions logicielles développées sous le contrôle du Ministère de la Justice.

De manière connexe, signalons également la création d'un traitement automatisé de données à caractère personnel, dénommé « DataJust »[126], ayant pour finalité le développement d'un algorithme relatif aux indemnisations des préjudices corporels (y compris ceux découlant d'une infraction pénale mais dans le cadre d'un recours porté devant les juridictions civiles[127]). Ce traitement automatisé a été autorisé par le décret de création pour deux ans en 2020 au profit du Ministère de la Justice. Il permettait la réalisation d'évaluations rétrospectives et prospectives des politiques publiques en matière de responsabilité civile ou administrative ; l'élaboration d'un référentiel indicatif d'indemnisation des préjudices corporels ; l'information des parties et l'aide à

---

[121] G. Thierry, « 2019 : l'année Cassiopée », (2019) *Dalloz actualité*, 23 janvier, https://www.dalloz-actualite.fr/flash/2019-l-annee-cassiopee , consulté le 22 mars 2022.

[122] Cour des comptes, (2022) *op. cit*. note 26.

[123] Application des Peines, Probation et Insertion, traitement automatisé de données à caractère personnel, qui a également pour finalité l'exploitation des informations recueillies à des fins de recherches statistiques et qui peut être mis en relation avec Cassiopée.

[124] Cour des comptes, (2022) *op. cit*. ; Assemblée nationale, *Rapport d'information sur les carences de l'exécution des peines et l'évaluation de l'application Cassiopée*, (n° 3177 présenté par E. Blanc, 2011).

[125] Assemblée nationale, (2011) *op. cit*. ; G. Thierry, (2019), *op. cit.* <https://www.dalloz-actualite.fr/flash/2019-l-annee-cassiopee> ; L. Le Devin, « Chez les magistrats, Cassiopée frôle la nullité », *Libération*, (Paris,10 novembre 2017) <https://www.liberation.fr/france/2017/11/10/chez-les-magistrats-cassiopee-frole-la-nullite_1609375/> consulté le 14 mars 2022 ; V. *infra,* §1.3.1 et 1.3.2.

[126] Décret n° 2020-356 portant création d'un traitement automatisé de données à caractère personnel dénommé « DataJust » (27 mars 2020), *JORF* n°77 du 29 mars 2020.

[127] *Ibid.* L'article 2 prévoit que les données nécessaires sont extraites des décisions de justice rendues en appel entre le 1er janvier 2017 et le 31 décembre 2019 par les juridictions administratives et les formations civiles des juridictions judiciaires dans les seuls contentieux portant sur l'indemnisation des préjudices corporels.

l'évaluation du montant de l'indemnisation à laquelle les victimes peuvent prétendre afin de favoriser un règlement amiable des litiges ; l'information ou la documentation des juges appelés à statuer sur des demandes d'indemnisation des préjudices corporels. À ces fins, l'algorithme recensait les montants demandés et offerts par les parties, les évaluations proposées dans le cadre de procédures de règlement amiable des litiges et les montants alloués aux victimes pour chaque type de préjudice, ainsi que de nombreuses données et informations énumérées par le décret qui l'instaure[128]. Son contenu n'était accessible qu'à des agents du ministère de la justice, affectés au service chargé des développements informatiques du secrétariat général du ministère de la justice, individuellement désignés par le secrétaire général, ainsi qu'aux agents du bureau du droit des obligations, individuellement désignés par le directeur des affaires civiles et du sceau. Ce traitement automatisé, bien que validé par le Conseil d'État[129], n'a cependant pas été prorogé par le Ministère de la Justice, pour des raisons tenant apparemment à la complexité de sa mise en œuvre[130].

Enfin, il existe une justice automatisée en matière de sécurité routière. La loi renforçant la lutte contre la violence routière[131], a permis le développement d'un contrôle radar automatisé et la délivrance automatique d'amendes par l'Agence Nationale du Traitement Automatisé des Infractions (ANTAI)[132]. L'intelligence artificielle a permis de développer en 2019 une solution « IA Flash », qui devait être intégrée dans les radars automatiques en 2020, afin de renforcer la fiabilité de ce traitement automatisé. Un algorithme de reconnaissance d'images permet de détecter une plaque d'immatriculation qui ne correspond pas au modèle du véhicule enregistré dans le système national d'immatriculation des véhicules (en cas d'usurpation de plaque par exemple), et ainsi de bloquer l'envoi de la contravention[133].

Les legaltechs, sociétés privées, proposent quant à elles des solutions davantage à destination des avocats et des entreprises. La plupart des solutions éventuellement applicables en matière pénale, utilisent la jurisprudence française en open data. L'accessibilité à toutes les décisions pénales étant encore réduite, ces applications sont pour l'heure peu utilisées dans ce domaine, même si elles ne l'écartent pas expressément.

---

[128] *Ibid*. Article 2

[129] CE 30 décembre 2021, n° 440376.

[130] E. Marzolf, « Le ministère de la Justice renonce à son algorithme DataJust », *Acteurs publics*, 14 janvier 2022.

[131] Loi n° 2003-495 renforçant la lutte contre la violence routière (12 juin 2003), JORF n° 135 du 13 juin 2003.

[132] Art. 529-11 C. proc. pén.

[133] Application développée dans le cadre du programme Entrepreneur d'intérêt général, https://eig.etalab.gouv.fr/defis/ia-flash/ ; V. aussi https://www.permisapoints.fr/securite-routiere/intelligence-artificielle-venir-aide-radars-automatiques#:~:text=L'intelligence%20artificielle%20va%20venir,usurpations%20de%20plaques%20d'immatriculation.

Ces applications sont essentiellement des moteurs de recherche, qui peuvent également proposer des services de veille juridique ou d'analyse juridique de documents. Cette dernière fonctionne en scannant les documents (par exemple les écritures de la partie adverse) afin d'en rechercher les fondements textuels et jurisprudentiels et les afficher à destination de l'auteur de la requête. Certaines applications calculent également les probabilités de résolution d'un litige et estiment le montant des indemnités susceptibles d'être prononcées au regard de l'analyse statistique de la jurisprudence rendue dans le même domaine (Predictice, Case Law Analytics)[134].

Ces outils se fondent sur des modélisations mathématiques ou statistiques, conçues à partir d'un grand nombre de décisions de justice permettant de mettre en évidence les critères sur lesquels se fondent les magistrats pour prendre une décision. Certains auteurs soulignent que par définition, un modèle est faux « puisqu'il est une simplification de la réalité »[135]. Il est en effet impossible de prendre en compte tous les critères interférant dans la décision d'un juge, certains n'étant pas du tout juridiques[136]. Il est donc nécessaire de connaître les limites de ces outils.

L'application Supra Legem, ciblant la jurisprudence administrative a été présentée comme utilisant des algorithmes prédictifs. Créée en 2016, cette application utilisait l'intelligence artificielle afin d'analyser les décisions des juridictions administratives et déterminer le sens possible d'un litige au regard de la thématique de la décision, de la nature du demandeur et celle du défendeur. L'application permettait également de fournir des statistiques et des représentations graphiques de la tendance de chaque juge pour un type de contentieux donné. Le concepteur vantait la possibilité d'anticiper son juge et de concourir ainsi à une justice plus impartiale[137]. Ce logiciel pouvait trouver application dans le champ pénal entendu au sens large, notamment en matière pénitentiaire lorsque les décisions de l'administration pénitentiaire sont susceptibles d'un recours, ou dans le cadre d'un recours à l'encontre de conditions de détention indignes. Le site internet de l'application a cependant été rendu inaccessible et le législateur a introduit de nouvelles dispositions dans le code de l'organisation judiciaire et le code de justice administrative par la loi n° 2019-222 du 23 mars 2019 de programmation et de réforme pour la justice[138], interdisant la réutilisation des données d'identité des magistrats et agents de greffe, en particulier pour le profilage ou le

[134] V. l'inventaire réalisé par L. Tavitian, « Justice prédictive où en est-on ? », (2016), <https://www.village-justice.com/articles/Justice-predictive-est-jurimetrie,22683.html> , consulté le 12 mars 2022.

[135] J. Levy-Véhel, « L'office du juge: un éclairage via la modélisation mathématique », (2020), *Cahiers de la Justice*, 4, 744.

[136] Danziger, S., Levav, J., & Avnaim-Pesso, L., *« Qu'a mangé le juge à son petit-déjeuner ? » De l'impact des conditions de travail sur la décision de justice*, (2015), *Les Cahiers de la Justice*, 579.

[137] V. La présentation sur le site gouvernemental, <https://www.data.gouv.fr/fr/reuses/supra-legem/>

[138] Amendement n° 1425 du 15 novembre 2018 déposé sur le texte de la commission examiné en première lecture à l'Assemblée Nationale et adopté le 11 décembre 2018.

ranking, ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées[139].

Le développement de l'intelligence artificielle est encouragé par les pouvoirs publics, y compris en matière de justice. Ainsi, en 2016, la Direction de l'information légale et administrative a créé un prix « DILA - le droit ouvert - jurisprudence » destiné à récompenser des projets innovants, notamment des applications, services, produits ou visualisation de données juridiques ou facilitant leur réutilisation[140]. La société Prédictice en a été le lauréat[141]. Il en est de même du programme Entrepreneur d'intérêt général du Ministère de la transformation et de la fonction publiques qui a permis le développement d'une solution d'intelligence artificielle pour renforcer la fiabilité du traitement automatisé des infractions routières[142].

Par ailleurs, bien que ne concernant pas pour l'heure la justice pénale, certaines applications proposées par les legaltechs font l'objet d'une diffusion croissante s'appuyant sur des institutions juridiques reconnues et sur l'enseignement supérieur et la recherche pour assoir leur notoriété. Ainsi, Case Law Analytics a pour partenaire la société d'édition Dalloz et des modules de formation sont dispensés à l'École Nationale de la Magistrature, à l'École Nationale du Barreau ainsi que dans certaines universités[143]. De même, la société Prédictice propose d'accompagner des projets pédagogiques innovants en mettant sa plateforme gratuitement à disposition des étudiants et des universitaires souhaitant s'engager dans ce type de démarche[144].

[139] Art. L. 10 du Code de la justice administrative et L. 111-13 du code de l'organisation judiciaire.

[140] Arrêté du 4 novembre 2016 *relatif à la création et dotation du prix de la direction de l'information légale et administrative « DILA - le droit ouvert - jurisprudence »*, *JORF* n° 268 du 18 novembre 2016.

[141]<https://www.dila.premier-ministre.gouv.fr/actualites/toutes-les-actualites/open-case-law-2016-remise-des-prix-le-droit-ouvert-jurisprudence>

[142] V. Note 42.

[143]<https://www.caselawanalytics.com/wp-content/uploads/2021/06/Catalogue-de-formations-2021-Case-Law-Analytics.pdf>

[144] <https://blog.predictice.com/le-programme-predictice-pour-lenseignement-et-la-recherche>

Principales applications de l'intelligence artificielle en droit pénal

NOM	Date de création	Utilisateurs ciblés	Fonctionnalités	Domaines du droit couverts	Sources et natures des données	Technologies utilisées
Juri'Prédis (SAS Juri'Prédis)	2018	Étudiants, cabinets d'avocats, directions juridiques, juristes d'entreprise, services juridiques de collectivités ou du secteur banque-assurance, notaires, huissiers, experts-comptables	Moteur de recherche de jurisprudence à partir d'une problématique juridique, solutions supplémentaires de veille juridique et d'analyse jurisprudentielle de documents (Juri'détect) pour les avocats	Tous	Décisions issues de l'open data, jurisprudences françaises de l'ordre judiciaire (Cour de cassation, cours d'appel, tribunaux de première instance), de l'ordre administratif, et du Conseil Constitutionnel	IA Machine learning
Doctrine.Fr (Forseti SAS)	2016	Avocats, entreprises	Moteur de recherche, veille juridique, analyse juridique de documents (Analyzer)	Tous	Jurisprudence française	IA (intelligence juridique)

Principales applications de l'intelligence artificielle en droit pénal

Moteur de recherche de l'open data judiciaire	2021	Tout public	Moteur de recherche	Tous	Jurisprudence de la Cour de cassation	IA
Supra-legem (M. Benesty) Désormais inaccessible	2016	Citoyens	Moteur de recherche, analyse prédictive permettant de déterminer les chances du succès d'un recours, ainsi que la position de chaque juge et son degré d'impartialité	Droit administratif (peut concerner les litiges en matière pénitentiaire)	Jurisprudence administrative	IA, algorithmes prédictifs, machine Learning, moteur de recherche permettant de chercher selon : la thématique de la décision, la nature du demandeur, la nature du défendeur et le sens du dispositif; calculs de statistiques par juge ou par cours

Principales applications de l'intelligence artificielle en droit pénal

Jurisdata Analytics (LexisNexis)	2016	Professionnels du droit	Moteur de recherche et d'analyse, outil d'aide à la décision, recherche de décisions comparables pour définir des stratégies juridiques, évaluer le montant d'une indemnité	Hors pénal à ce jour	Décisions de justice indexées de l'analyse Jurisdata	Data-visualisation active et analyse de corrélation

1.3 Représentations de la justice predictive

1.3.1 Représentations de la doctrine

Les travaux de recherche menés sur la justice prédictive sont encore récents et peu nombreux, surtout en matière pénale145. Ils recèlent cependant une tendance à la méfiance envers les prédictions judiciaires par algorithmes, peut-être de manière encore plus prononcée en matière pénale.

La justice prédictive est abordée principalement sous l'angle du fantasme[146], d'une justice « simplement » virtuelle par opposition à actuelle[147], alors que la matière pénale est pour l'heure exclue des développements technologiques[148]. Les commentaires s'appuient cependant sur des expériences, américaines notamment, bien réelles.

Certains auteurs, partisans d'une justice formelle, voient dans l'IA une opportunité de renforcer la sécurité juridique par une meilleure cohérence des décisions de justice[149]. D'autres considèrent que les algorithmes permettraient de renforcer l'efficacité du procès par son automatisation, sa désincarnation et sa rapidité (et même son anticipation)[150]. Les appréciations positives sont cependant rares et rapidement écartées au profit des nombreux doutes émis.

---

[145] Pour un inventaire, V. A. Coletta, (2022), *op. cit.* § 11. Ajoutons spécifiquement en droit pénal, la thèse en préparation depuis 2018 de Sarah Cherqaoui, *L'intelligence artificielle en matière pénale*, sous la direction de O ; Decima, Bordeaux, et celle de Emily Mongaillard, *Étude de la contribution de l'intelligence artificielle à l'évolution du droit : l'exemple du droit pénal des affaires*, sous la direction de C. Mascala, Toulouse depuis 2019. L'ENM finance également des programmes de recherche : E. Vergès, G. Vial, 'L'impact des algorithmes sur les décisions de justice des magistrats au pénal et au civil', (2022); les mêmes chercheurs s'intéressent à la pratique des juges et au raisonnement probatoire.
Des congrès internationaux ou nationaux ont également pu aborder le sujet en matière pénale: J.-B. Hubin, H. Jacquemin, B. Michaux (dir.), 'Le juge et l'algorithme: juges augmentés ou justice diminuée ?' (Larcier 2019) ou enfin un congrès en ligne sous la direction de P. Mistretta et J. Alix, 'Intelligence artificielle et justice pénale', 12 march 2021, https://lexradio.fr/emission/1-27-COLLOQUE-INTELLIGENCE-ARTIFICIELLE-ET-JUSTICE-PENALE-EN-LIGNE-LE-12-MARS-2021.
Voir aussi les essais écrits par des universitaires : S. Desmoulin-Canselier, D. Le Métayer, 'Décider avec les algorithmes, quelle place pour l'Homme, quelle place pour le droit ?', (Dalloz, 2020); F. G'Sell, 'Justice numérique, (Dalloz, 2021); ou par des juges : E. Poinas, 'Le tribunal des algorithmes: juger à l'ère des nouvelles technologies', (Berger-Levrault, 2019).

[146] Dondero B., « Justice prédictive: la fin de l'aléa judiciaire ? », (2017), *D.*, 532.

[147] S. Lebreton-Derrien, 'La justice prédictive, Introduction à une justice "simplement" virtuelle,' (2018) *Arch. phil. droit* no. 60, 21.

[148] J.-M. Brigant, 'Les risques accentués d'une justice pénale predictive', (2018) *Arch. phil. Droit* no. 60, 46.

[149] Guillaume Zambrano, « Précédents et prédictions jurisprudentielles à l'ère des *big data* : parier sur le résultat (probable) d'un procès », (2015), <hal-01496098>

[150] J-B Duclercq, « Les algorithmes en procès », (2018), *RFDA*, 131.

Une partie de la doctrine se montre sceptique quant à la possibilité de systématiser nos règles de droit, dans le cadre de notre système juridique de droit écrit, par opposition aux systèmes de Common law. Si « le droit apparaît comme un système « logique » »[151], permettant de prévoir les conséquences juridiques d'un acte, il conserve une part d'incertitude liée à l'humanité des rapports qu'il gère, et aux situations de fait qui ne sont pas réductibles à l'énoncé d'une norme abstraite et générale[152]. Toutes les notions appliquées en droit ne sont pas définies par la loi, permettant à l'appréciation souveraine des juges du fond d'adapter les solutions à une dimension politique et sociale qui ne figure pas dans les textes, de déterminer « la règle d'application de la règle »[153] de droit. Le jugement semble donc ne pas pouvoir se passer d'un juge pour interpréter et appliquer la règle de droit[154].

Certains auteurs doutent que les algorithmes soient fiables et de qualité car ils sont fondés sur une petite partie de l'information. En effet, en matière pénale, les décisions des juges du fond sont encore largement inaccessibles, tandis que se développent des alternatives aux poursuites qui ne seraient pas prises en compte par les algorithmes[155].

Certains auteurs soulignent alors les choix arbitraires des concepteurs d'algorithmes, qui sont donc forcément limités et à utiliser avec précaution[156] : « Appliqués aux décisions de justice, les modèles mathématiques peinent à rendre compte de l'entière réalité qu'ils prétendent décrire et ne peuvent se prêter qu'imparfaitement à des finalités prédictives ou actuarielles ». Une décision de justice est bien plus complexe qu'un simple syllogisme et les algorithmes, qui se limitent à des corrélations, des liens lexicaux, ne fournissent pas une analyse assez fine impliquant le comportement d'un juge. Les applications créées sur cette base ne proposent donc que des explications faussées des décisions de justice, « une sorte de mémoire myope de la justice, dépourvue d'une analyse fine des véritables éléments causatifs des décisions de justice qu'elle prétend restituer »[157], car il reste une part d'imprévisibilité. C'est d'ailleurs pour pallier cette critique que certains auteurs militent pour le profilage des juges, qui permettrait d'assurer une véritable prédiction judiciaire et partant assurer la prévisibilité de l'application du droit[158].

---

[151] Boucq R., « La justice prédictive en question », (2017), *Dalloz actualités*, 14 juin, <https://www.dalloz-actualite.fr/chronique/justice-predictive-en-question>

[152] V. Vigneau, « Le passé ne manque pas d'avenir, Libres propos d'un juge sur la justice prédictive », (2018) *D.*, 1095

[153] Garapon A., « Les enjeux de la justice prédictive », (2017) *JCP G* n°1-2, 9 janvier, doctr. 31.

[154] Dondero B., « Justice prédictive : la fin de l'aléa judiciaire ? », (2017) *D.*, 532; V. Vigneau, (2018) *op. cit*., cite quant à lui le doyen Cornu: « le juge est asservi par la loi à la création du droit, laquelle ne prendra corps véritablement que par l'apport du juge » (G. Cornu, Cours de doctorat 1970-1971. L'apport des réformes récentes du code civil à la théorie du droit civil, p. 167.).

[155] J.-M. Brigant, (2018) *op. cit.* note 57.

[156] Y. Meneceur, C. Barbaro, « Intelligence artificielle et mémoire de la justice : le grand malentendu »,(2019) *Les Cahiers de la Justice*, 277.

[157] B. Dondero (2017), *op. cit.*

[158] A. Coletta, 'La prédiction judiciaire par les algorithmes', (2022), *op. cit.* note 5, § 20, 24.

De même, les statistiques obtenues peuvent être faussées si aucune hiérarchie n'est faite entre les décisions de justice utilisées, par exemple entre les décisions de la Cour de cassation, celles des cours d'appel ou celles des juridictions de première instance.

De nombreuses craintes sont exprimées face à la justice prédictive. La première est le risque performatif, mis en évidence notamment par Antoine Garapon[159], c'est-à-dire le risque que la solution prédite par les algorithmes devienne la norme. La marge d'interprétation et donc la liberté des juges disparaîtrait au profit d'un conformisme impliquant une pression sur le jugement dans le sens imposé par le standard virtuel. Un juge qui souhaiterait s'éloigner des standards devrait motiver davantage, mettant en jeu une responsabilité nouvelle. L'homogénéisation de la jurisprudence ainsi obtenue implique à son tour le risque de reproduire des stigmas sociaux et de figer les décisions sur des solutions dépassées puisque les algorithmes s'appuient sur la jurisprudence passée[160]. En matière d'individualisation de la peine, le recours à l'IA pourrait faire rejaillir l'opposition entre l'individualisation humaniste de la peine (Saleilles, Ancel) et l'individualisation scientifique fondée sur une évaluation statistique de la dangerosité de l'individu (Ecole positiviste italienne).

Plusieurs craintes sont liées au respect des principes généraux du droit. Certains auteurs évoquent la remise en cause du principe du contradictoire, face à des arguments voire des solutions dictées par les algorithmes. Pour certains, « le recours aux algorithmes dans le cadre du procès soulève la question de la conformité de cette pratique aux traités internationaux et à la Constitution, notamment du point de vue du droit à un procès équitable ou encore du principe d'indépendance de la justice. »[161]. La qualité du procès est fragilisée, du fait de la remise en cause de l'indépendance du magistrat, tant à l'égard des autres magistrats, des justiciables, des experts, du pouvoir politique, que des machines elles-mêmes. La qualité du procès est également fragilisée du fait de la diminution de l'acceptabilité sociale du procès si les justiciables ne sont plus face à des hommes mais à des machines[162]. Et lorsque la solution prédite est défavorable, c'est l'évitement du procès qui peut être préconisé[163].

La doctrine réfractaire dénie alors à la jurisprudence de la Cour de cassation la possibilité de constituer le fondement d'un algorithme, au nom de la liberté et de l'indépendance du juge. Le juge du fond peut s'émanciper de la jurisprudence non obligatoire de la Cour de cassation, et ses décisions ne sont pas figées au nom de la sécurité juridique[164].

---

[159] Garapon A., (2017), *op. cit*.note 62.
[160] B. Dondero, (2017) *op. cit*. note 63.
[161] J-B Duclercq, « Les algorithmes en procès », (2018) RFDA, 131.
[162] *Ibid*.
[163] S. Lebreton-Derrien, 'La justice prédictive, Introduction à une justice "simplement" virtuelle,' (2018) *Arch. phil. droit* no. 60, 13.
[164] V. Vigneau, (2018) *op. cit*.

Certains auteurs tempèrent cependant les craintes avancées, en accueillant de manière bienveillante la possibilité d'une autre justice. La justice prédictive suppose une intervention humaine pour prospérer, ce qui donnerait aux acteurs l'occasion d'être créatifs pour se protéger d'une domination du virtuel[165]. Elle permettrait par exemple l'avènement d'un nouveau principe directeur du procès : « un principe de candeur du juge qui devrait avoir à cœur de réserver aux plaideurs un regard neuf, vierge de tout préjugé et libre de toute pression prédictive »[166]. Ou bien elle favoriserait la médiation et donc « une meilleur acceptation de la solution en participant au processus de contractualisation de la procédure »[167].

La doctrine propose alors des solutions pour conserver la dimension humaine inhérente à la justice. Il apparaît d'abord nécessaire que les juristes comprennent les différentes dimensions des outils de justice prédictive créés, par l'intermédiaire d'une formation technique, permettant de rendre intelligibles les algorithmes utilisés. Il convient par ailleurs de développer des normes éthiques permettant une responsabilisation des acteurs dans l'utilisation des algorithmes[168].

Certains auteurs dénoncent enfin la « logique capitalistique entrepreneuriale »[169] au fondement de l'évolution qui se dessine et qui tend à transformer profondément la profession d'avocat, et au-delà une « remise en cause radicale des formes actuelles du droit, des juristes et de la justice »[170]. Le rapport de la mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice soulignait d'ailleurs la reconfiguration possible du marché des entreprises juridiques, la compétitivité des Legaltechs françaises risquant de se heurter aux entreprises étrangères plus puissantes[171]. Il prévoyait également une mutation du travail des professionnels du droit, nécessitant un cadre juridique et éthique[172].

1.3.2 Représentations par les praticiens

Les pratiques de la justice prédictive par les magistrats restent très rares et circonscrites à des expérimentations de logiciels de traitement de bases de données de jurisprudence. Une étude a été menée dans le cadre de l'expérimentation du logiciel Predictice par les

[165] S. Lebreton-Derrien, (2017) *op. cit*., 12.
[166] A. Garapon, J. Lassègue, *Justice digitale,* (Paris PUF 2018), 259.
[167] S. Lebreton-Derrien, (2017) *op. cit*., note 72, 14.
[168] Ibid., p. 17
[169] B. Dondero, 'Justice prédictive: la fin de l'aléa judiciaire?' (2017), *D.*, 532.
[170] A. Garapon, « Les enjeux de la justice prédictive », (2017) JCP G n°1-2, 9 janvier, doctr. 31.
[171] Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, *L'open data des décisions de justice*(Rapport à Madame la Garde des sceaux, Ministre de la Justice sous la présidence de L. Cadiet, novembre 2017), 28.
[172] *Ibid*., 30.

Cours d'appel de Rennes et de Douai au printemps 2017[173]. Cette étude visait notamment à recueillir la perception des magistrats confrontés à cet outil d'intelligence artificielle, ainsi qu'à analyser les répercussions sur le travail du magistrat dans la fabrication des décisions de justice et sur la représentation de l'activité de jugement.

Le logiciel Predictice est présenté comme une plateforme d'aide à la décision judiciaire basée sur les données de la jurisprudence des cours d'appel, devenues open data. L'application analyse les décisions figurant dans la base selon les critères sélectionnés par l'auteur de la requête et indique le sens des décisions rendues dans des affaires similaires, ainsi que, le cas échéant, le montant des indemnités allouées. Ce logiciel a été expérimenté au même moment par une quinzaine de cabinets d'avocats pilotes.

L'accueil par les magistrats a été plutôt mitigé voire hostile, pour des raisons tenant à la méfiance envers une application qui remettrait en cause leur autonomie, ainsi que pour des difficultés d'ordre technique, les systèmes informatiques des juridictions étant souvent obsolètes. L'expérimentation ne s'est pas déroulée de la façon dont le développeur l'avait envisagé, de manière collective dans un cadre « d'innovation participative »[174], chaque magistrat impliqué continuant à travailler de manière solitaire face au logiciel, ce qui est courant chez les magistrats du siège. À l'inverse, les Parquets ont développé depuis quelques années des méthodes de travail plus collaboratives, mais comme la matière pénale a été exclue de l'expérimentation, ils n'y ont pas participé.

L'accueil mitigé peut également s'expliquer par la préexistence d'outils « artisanaux » d'aide à la décision. L'étude précitée fait ainsi référence à des trames informatiques de jugement pour les contentieux simples et répétitifs, des grilles d'indemnisation en matière de licenciement, ou encore un référent devenu national, bien que critiqué, en matière d'indemnisation des préjudices corporels[175]. En matière pénale, l'application Cassiopée fournit une aide à l'élaboration des décisions des juridictions de jugement, en mettant par exemple à disposition des trames de décisions ou une liste préétablie de motifs, à sélectionner lors de la rédaction des jugements de première instance[176].

Apparaît alors une tension entre d'un côté « l'indépendance revendiquée du juge (et de fait, son autonomie au sens de la sociologie du travail) et de l'autre la nécessité de mettre en cohérence les décisions judiciaires »[177]. Les magistrats « bricolent » des outils, en interne, mais résistent à la standardisation et aux logiciels développés en externe par des

[173] C. Licoppe et L. Dumoulin. « Le travail des juges et les algorithmes de traitement de la jurisprudence. Premières analyses d'une expérimentation de « justice prédictive » en France », (2019) *Droit et société*, vol. 103, n°3, 535.
[174] C. Licoppe et L. Dumoulin, (2019), *op. cit.*
[175] *Ibid*. ainsi que les références citées.
[176] G. Thierry, « 2019: l'année Cassiopée », (2019) *Dalloz actualité*, 23 janvier, <https://www.dalloz-actualite.fr/flash/2019-l-annee-cassiopee >, *op. cit.*
[177] *Ibid*.

entreprises privées. Ils peuvent ainsi conserver le contrôle de ces outils, ce qui n'est pas le cas avec les logiciels de justice prédictive.

Un désaccord est également apparu entre magistrats quant à la possibilité de diffuser leurs outils aux avocats, notamment les barèmes et référentiels. En effet, la crainte de certains magistrats était de se trouver liés par leur outil ou encore de donner l'impression que la décision était déjà rendue. D'autres en revanche considèrent que ces barèmes ne sont qu'indicatifs mais permettent aux avocats de mieux formuler leurs demandes. Finalement, le référentiel d'indemnisation a été communiqué au public afin de permettre des transactions directes entre les parties, sans recours au tribunal, dans un objectif de limiter le contentieux[178].

Par ailleurs, l'étude précitée souligne l'utilisation réflexive du logiciel Predictice par les magistrats, qui souhaitent évaluer leurs décisions au regard de la moyenne. Cette possibilité d'analyser les décisions d'un magistrat, également par les avocats, fait craindre là encore la standardisation des jugements, la tentation de ne pas s'écarter de la moyenne et donc la remise en cause de l'indépendance du juge.

1.4 Évaluation de la fiabilité, de l'impartialité, de l'égalité, de l'adaptabilité

L'expérimentation décrite ci-dessus a fait l'objet d'une évaluation par les utilisateurs eux-mêmes, c'est-à-dire les magistrats, qui ont été plutôt déçus de l'application. D'après les informations disponibles, l'évaluation portait davantage sur sa fiabilité que sur son impartialité. La dimension pénale de l'activité des cours d'appel n'était pas concernée.

Si la modernité de l'outil a été saluée, les magistrats ne lui reconnaissaient cependant pas la plus-value escomptée au regard des moteurs de recherche dont ils disposaient déjà[179]. Le logiciel devait en outre être amélioré, et l'analyse affinée, car elle pouvait produire des résultats aberrants, selon les magistrats interrogés, comme le calcul d'une indemnité de licenciement qui peut se trouver faussé par le fait que le logiciel ne distingue pas les cadres des autres salariés[180]. Suite à cette expérimentation, l'utilisation de l'outil a cessé.

---

[178] *Ibid*.

[179] Réponse du Ministère de la Justice, publiée dans le JO Sénat du 28/12/2017 - page 4694, à la Question écrite n° 01823 de M. Jérôme Durain, publiée dans le JO Sénat du 02/11/2017 - page 3392, <https://www.senat.fr/questions/base/2017/qSEQ171101823.html>

[180] L'utilisation de l'outil Predictice déçoit la cour d'appel de Rennes, Interview de X. Ronsin, premier président de la cour d'appel de Rennes, *Dalloz Actualité*, 16 octobre 2017, <https://www.dalloz-actualite.fr/interview/l-utilisation-de-l-outil-predictice-decoit-cour-d-appel-de-rennes> . Pour relativiser l'échec dont la presse s'est fait l'écho, V. C. Licoppe et L. Dumoulin, « Le travail des juges et les algorithmes de traitement de la jurisprudence. Premières analyses d'une expérimentation de « justice prédictive » en France », (2019) *Droit et société*, vol. 103, no. 3, 535.

D'autres études ont été réalisées ou sont en cours. Le blog de Predictice mentionne des travaux de l'Université de Paris Dauphine sur l'effet performatif de son application[181].

Une recherche est également menée dans le cadre d'un appel à projet de la Mission de recherche droit et justice[182], sur la période novembre 2020-février 2023 sur « droit et intelligence artificielle: quelle régulation du marché pour des outils de justice prévisionnelle dignes de confiance ? », sous la direction de Agnès Delaborde, Aurore Hyde, Christian Licoppe. Cette étude s'intéresse au développement d'outils de justice prévisionnelle, aux conditions auxquelles les résultats de ces outils peuvent devenir des sources du droit, à la réglementation ou la régulation privée ou publique à mettre en œuvre pour encadrer leur utilisation, ainsi qu'à la fiabilité et à l'impartialité des outils choisis comme illustration de la recherche[183].

Faute d'expérimentation, il n'existe pas de données permettant d'apprécier la fiabilité ou l'impartialité des logiciels de justice prédictive en matière de justice pénale.

2 Cadre normatif, réglementation et soft law

Il n'existe pas, en France, de cadre juridique propre à l'utilisation de systèmes basés sur l'IA à des fins de justice prédictive. Comme indiqué ci-dessus, une recherche est actuellement en cours afin d'étudier la nécessité et l'opportunité d'adopter un tel cadre[184]. Cependant, d'autres corpus législatifs ou règlementaires sont susceptibles de s'appliquer à ces systèmes, notamment en matière de traitement automatisé de données à caractère personnel. La Commission Nationale de l'Informatique et des Libertés (CNIL) rappelle qu'une grande partie des enjeux et des questions posées par l'intelligence artificielle se sont déjà posées en 1978 à propos de l'informatisation de l'État et trouvent déjà des réponses dans la législation existante. La CNIL invite en outre à considérer la possibilité d'une régulation par les acteurs, à côté de la réglementation étatique, et l'adoption de chartes éthiques est un exemple de régulation possible[185].

2.1 Cadre législatif et règlementaire applicable

2.1.1 La loi informatique et libertés

[181] <https://blog.predictice.com/le-programme-predictice-pour-lenseignement-et-la-recherche-souffle-sa-première-bougie> ; nous n'avons cependant pas trouvé de compte-rendu de cette expérimentation.
[182] Désormais l'Institut des Études et de la Recherche sur le Droit et la Justice.
[183] <http://www.gip-recherche-justice.fr/publication/droit-et-intelligence-quelle-regulation-du-marche-pour-des-outils-de-justice-previsionnelle-dignes-de-confiance/ >
[184] *Ibid*.
[185] CNIL, *Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, (2017), 44.

La loi informatique et libertés[186] énonce dans son premier article les principes sur lesquels repose l'utilisation des données personnelles par les algorithmes : « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

Elle encadre la création et l'utilisation de traitement de données à caractère personnel et particulièrement les conditions de collecte et de conservation des données et en confie le contrôle à la CNIL. Elle écarte cependant de son champ d'application les traitements réutilisant les données des décisions de justice disponibles en open data depuis la Loi pour une République numérique. L'article 44 de la Loi informatique et liberté exclut en effet « 5° Les traitements portant sur la réutilisation des informations publiques figurant dans les décisions mentionnées à l'article L. 10 du code de justice administrative et à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que ces traitements n'aient ni pour objet ni pour effet de permettre la ré-identification des personnes concernées (…) ».

L'article 46 permet quant à lui aux réutilisateurs des données figurant dans les décisions de justice en open data de traiter des informations en matière pénale: « Les traitements de données à caractère personnel relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne peuvent être effectués que par : (…) 5° Les réutilisateurs des informations publiques figurant dans les décisions mentionnées à l'article L. 10 du code de justice administrative et à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la ré-identification des personnes concernées. »

L'article 42 exclut également du champ d'application de la loi Informatique et Libertés les traitements de données à caractère personnel effectués « 3° Par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces ». Cette disposition autoriserait ainsi l'usage par les magistrats de logiciels prédictifs fondés par exemple sur la probabilité de récidive. Elle est cependant tempérée par l'article 47 qui dispose qu'« 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 la personnalité de cette personne. »

La Loi informatique et libertés interdit en effet qu'une machine puisse prendre seule, sans intervention humaine, des décisions ayant des conséquences importantes pour les personnes, notamment les décisions judiciaires. Elle interdit ainsi depuis son origine les algorithmes de profilage, particulièrement dans le cadre juridictionnel. De même,

[186] Loi relative à l'informatique, aux fichiers et aux libertés, no 78-17, 6 janvier 1978, JORF, 7 janvier 1978 <www.cnil.fr/fr/la-loi-informatique-et-libertes>.

« 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 », à part quelques exceptions encadrées par la suite de l'article 47.

Ces dispositions font également référence au règlement européen 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[187]. Le RGPD, d'application directe dans les États membres de l'Union européenne, permet de limiter l'utilisation de certaines données dans le cadre d'application de justice prédictive. Ainsi, le traitement des données personnelles relatives aux condamnations pénales et aux infractions est encadré par l'article 10 du RGPD, qui impose que ce traitement soit réalisé sous le contrôle de l'autorité publique. De même, la loi informatique et libertés renvoie à l'article 22 du RGPD qui encadre le profilage.

Enfin, la loi informatique et libertés organise l'exercice de leurs droits par les personnes à l'égard des données les concernant, ainsi que le droit d'être informé sur le fonctionnement de l'algorithme[188].

Nous pouvons souligner avec certains auteurs que « Littéralement, la loi Informatique et libertés ne défend pas au juge de se fonder sur des algorithmes de profilage maniant des données dépourvues de caractère personnel » ni « de se fonder sur des algorithmes autres que ceux de profilage, qui sont légions. »[189].

2.1.2 Code de l'organisation judiciaire (COJ) et Code la justice administrative (CJA)

Le code de l'organisation judiciaire et celui de la justice administrative règlementent et organisent le fonctionnement des juridictions judiciaires et des juridictions administratives. Les juridictions judiciaires comprennent celles ayant compétence en matière pénale, tandis que les juridictions administratives peuvent être saisies d'affaires concernant l'application du droit pénal, comme en matière d'exécution des peines en cas de litige avec l'administration pénitentiaire, ou en cas de contestation de la légalité d'un règlement pris en application de la loi pénale.

Les articles L 111-13 COJ et 10 CJA organisent la mise à disposition du public des décisions rendues par les juridictions judiciaires et administratives, sous réserve de leur anonymisation. Ils interdisent également la réutilisation des données d'identité des magistrats et des membres du greffe « ayant pour objet ou pour effet d'évaluer,

---

[187] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, dit RGPD, *op. cit.* (n 20).

[188] Loi relative à l'informatique, aux fichiers et aux libertés, no 78-17, 6 janvier 1978, JORF, 7 janvier 1978 <www.cnil.fr/fr/la-loi-informatique-et-libertes>, art. 48 et s.

[189] J.-B. Duclercq, « Les algorithmes en procès », (2018), *RFDA* 131.

d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées. La violation de cette interdiction est punie des peines prévues aux articles 226-18, 226-24 et 226-31 du code pénal[190], sans préjudice des mesures et sanctions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. ». Une telle disposition interdit donc le développement d'applications comme SupraLegem[191].

2.1.3 Code des relations entre le public et l'administration (CRPA)

Le CRPA a, comme son nom l'indique, vocation à régir les relations entre le public et l'administration de l'État, notamment en matière de documents administratifs, de communication d'informations ou d'accès aux informations personnelles. Il règlemente la procédure administrative non contentieuse et peut donc à ce titre également intéresser la matière pénale dès lors qu'une administration chargée d'appliquer les lois et règlementations pénales est concernée.

Les articles L 321-1 et suivants du code des relations entre le public et l'administration énoncent les règles de réutilisation des informations publiques, elles-mêmes soumises à la loi informatique et libertés.

De manière plus précise, l'article L. 311-3-1 du même code énonce les règles applicables à l'utilisation d'un traitement algorithmique. Ainsi, toute décision individuelle prise sur le fondement d'un traitement algorithmique doit comporter une mention explicite qui en informe l'intéressé. Celui-ci peut demander à l'administration de lui communiquer les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre.

Les article R 311-3-1-1 et R 311-3-1-2 définissent le contenu de la mention informative, ainsi que le contenu des informations sur le traitement algorithmique qui peuvent être fournies à l'intéressé. Ces informations doivent être intelligibles pour l'intéressé et portent sur 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, ainsi que sur les opérations effectuées par le traitement.

2.2 Les sources non contraignantes

Le Conseil National des Barreaux (CNB), à l'issue d'une étude sur les technologies développées par les Legaltechs, a adopté le 9 octobre 2020, une Charte sur la transparence

[190] Délit puni de 5 ans d'emprisonnement et 300 000 euros d'amende.
[191] V. *Supra,* point 1.2.

et l'éthique de l'utilisation des données judiciaires[192]. Case Law Analytics et Doctrine ont été les premières Legaltechs à la signer en octobre et décembre 2020.

Cette Charte comporte, d'après son préambule, « un ensemble de principes visant à garantir l'autorégulation des acteurs tant s'agissant des algorithmes utilisés pour l'exploitation de la base de données des décisions de justice que de la réutilisation des informations qu'elle contient. ». Elle s'adresse aux acteurs de la Legaltech et les invite à proposer des outils respectueux des principes qu'elle énonce.

Les principes de bienfaisance et de non malfaisance engagent les concepteurs d'algorithmes de justice prédictive à préserver les libertés et droits fondamentaux et non à rechercher la performance. Le principe de loyauté oblige les acteurs concernés à afficher les conflits d'intérêts qui les concernent. Le principe d'explicabilité oblige le concepteur à fournir une information claire concernant le fonctionnement de l'algorithme, sa nature, sa fonction, sa logique décisionnel, l'objectif recherché. Le principe de transparence suppose la communication à l'utilisateur de toute information concernant d'éventuels biais décelés dans l'utilisation de l'outil. Le principe de compétence et d'égalité : permet d'associer des juristes dans les équipes de conception, ainsi qu'assurer la parité et la mixité des équipes afin de prévenir la reproduction de préjugés. Le principe de protection vise à garantir l'égal accès de tous à la technologie proposée. Le principe d'accessibilité, qui rejoint le précédent, permet une technologie inclusive, générale avec des options activantes pour s'adapter au public cible. Le principe de responsabilité du concepteur s'impose de manière inéluctable. Le principe de prévisibilité et d'évaluation vise à évaluer les actions de l'outil, mesurer les effets et prévenir les risques. Le principe de minimisation, de remédiation et de compensation agit en cas de défectuosité et d'effets négatifs pour l'utilisateur. Le principe de neutralité technologique et de sécurité permet d'éviter l'effet performatif et de protéger les données.

Ces principes visent notamment à garantir une information complète sur les algorithmes utilisés, à éviter la reproduction de préjugés par une composition adéquate des équipes de production des algorithmes, ou encore à instaurer une évaluation régulière des applications.

Bien que non contraignante, notons l'influence qui peut être exercée par la charte éthique de l'utilisation de l'intelligence artificielle adoptée par la Commission européenne pour l'efficacité de la justice (CEPEJ) du Conseil de l'Europe, en décembre 2018. Cette charte énonce 5 grands principes éthiques : respect des droits fondamentaux, non-discrimination, qualité et sécurité, transparence, neutralité et intégrité intellectuelle, maîtrise par l'utilisateur. Ces principes se retrouvent dans la charte adoptée par le CNB.

[192] Annexée au rapport du groupe de travail Legaltech, « Legaltechs du domaine de la jurimétrie, préconisations d'actions », 9 octobre 2020.

2.3 La Jurisprudence

Les juridictions pénales n'ont, à notre connaissance pas été confrontées à des systèmes basés sur l'IA et utilisés à des fins de justice prédictive, les systèmes existants étant appliqués hors champ pénal.

En revanche, le Conseil d'État a confirmé la conformité du décret instituant le traitement automatisé DATAJUST[193] à la Constitution, à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, à la Charte des droits fondamentaux de l'Union européenne, ainsi qu'au RGPD et à la loi informatique et liberté. Dans sa décision du 30 décembre 2021, il a en effet considéré que les droits à la protection des données personnelles sont suffisamment garantis par ce traitement automatisé, qui vise à développer un algorithme d'analyse des indemnités allouées en matière de préjudice corporel par les juridictions administratives et judiciaires, qui n'a qu'un caractère expérimental et qui n'est pas destiné à être mis à disposition ni des magistrats ni des parties. La particularité des finalités du traitement attaqué explique une appréciation souple du Conseil d'État, notamment quant à la minimisation des données: en effet, la finalité de développement d'un algorithme explique qu'il soit difficile de déterminer avec précision les données à collecter qui sont strictement nécessaires à la finalité du traitement[194]. La CNIL avait d'ailleurs émis un avis favorable à l'égard de la création de DATAJUST[195]. L'expérimentation a cependant pris fin prématurément en janvier 2022, la mise en œuvre étant jugée trop complexe[196].

Par ailleurs, la CNIL a autorisé le Ministère de la Justice à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la connaissance statistique de la réponse pénale apportée aux infractions à caractère raciste et l'analyse statistique des jugements comportant au moins une infraction commise en raison de l'origine, la nationalité, la religion, la race, réelles ou supposées, des victimes[197]. L'analyse a pour objectif d'évaluer la réponse pénale apportée à ces infractions et d'en tirer des statistiques. L'accès aux données ainsi collectées est restreint et sécurisé. Il ne s'agit donc pas d'un outil développé dans un objectif de justice prédictive, mais davantage dans le cadre d'une évaluation (et adaptation éventuelle) de la politique pénale à l'égard d'une catégorie d'infractions. Cependant, la base de données ainsi constituée serait la même pour une application de justice prédictive.

---

[193] Décret n° 2020-356 *op. cit*. (n 125).

[194] La nécessaire souplesse d'interprétation du Conseil d'État ici a notamment été relevée par Belkacem N., « Secteur public, affaires régaliennes et intelligence artificielle - décisions de justice et développement d'un algorithme », (2022), *Communication Commerce électronique* n° 2, Février, comm. 14.

[195] Délibération n° n° 2020-002 portant avis sur un projet de décret en Conseil d'État portant création d'un traitement automatisé de données à caractère personnel dénommé « DataJust » (9 janvier 2020, demande d'avis n° 19020148), JORF n° 77 du 29 mars 2020.

[196] V. *supra* § 1.2; V. égal. CNCDH, (2022) *op. cit.* § 30 ; E. Marzolf, (2022), *op. cit*.

[197] Délibération n°2017-186 du 15 juin 2017.

Enfin, notons que la CNIL n'a pas à autoriser les traitements algorithmiques développés dans un but de justice prédictive dans la mesure où ces traitements ne s'appuient pas sur des données à caractère personnel, mais sur la réutilisation de données anonymisées, déjà mises à disposition du public.

2.4 Les garanties de fond

La fiabilité, l'impartialité, l'égalité et l'adaptabilité des outils de justice prédictive ne sont pas garanties par un cadre législatif spécifique. Le rapport de la mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice recommandait d'ailleurs de « prévenir par un cadre juridique adapté la constitution de bases de données de décisions de justice s'affranchissant des exigences, contraintes et garanties recommandées par le présent rapport »[198]. Ces principes sont cependant garantis par la Charte éthique de l'utilisation de l'intelligence artificielle du Conseil de l'Europe et la Charte sur la transparence et l'éthique de l'utilisation des données judiciaires du Conseil National des Barreaux[199]. Ces textes non contraignants peuvent servir à la régulation de l'utilisation de la justice prédictive, voire inspirer si nécessaire un cadre réglementaire propre à assurer la protection de ces principes.

La transparence du fonctionnement et de l'utilisation des algorithmes est également une préoccupation de la mission d'étude conduite par Loïc Cadiet. Son rapport préconise en effet de « réguler le recours aux nouveaux outils de justice dite « prédictive » par l'édiction d'une obligation de transparence des algorithmes, la mise en œuvre de mécanismes souples de contrôle par la puissance publique, et l'adoption d'un dispositif de certification de qualité par un organisme indépendant. »[200].

Un principe de transparence à l'égard du public est donc posé par les articles L. 311-3-1 et R. 311-3-1-1 et -2 du code des relations entre le public et l'administration[201], ce qui peut permettre d'en déceler le manque de fiabilité, d'impartialité ou d'égalité.

Dans la mesure où un système basé sur l'IA et utilisé à des fins de justice prédictive ne s'appuie pas sur des données à caractère personnel, la législation française n'exige pas d'autorisation pour sa commercialisation, « sous réserve que les traitements mis en œuvre n'aient ni pour objet ni pour effet de permettre la ré-identification des personnes concernées »[202]. De même, aucune obligation n'est imposée aux producteurs de ces outils, ni technique ou technologique, ni quant à la méthodologie de conception et la nécessité d'associer des juristes. Seule la Charte éthique du CNB le préconise dans le cadre du

---

[198] Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, *L'open data des décisions de justice*, Rapport à Madame la Garde des sceaux, Ministre de la Justice sous la présidence de L. Cadiet, novembre 2017, Recommandation n°19.

[199] V. *Supra*, § 2.2.

[200] Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, *op. cit*. Recommandation n° 20.

[201] V. *Supra*, § 2.1.3.

[202] Art. 44 et 46 de la Loi n° 78-17 *op. cit*. (n 187).

principe de compétence[203]. Notons cependant que les sociétés françaises proposant des outils de justice prédictive comptent des juristes, notamment des avocats, parmi leurs associés ou collaborateurs.

Par ailleurs, bien que préconisée[204], la certification ou la labellisation des outils de justice prédictive n'est pas encore proposée ni imposée en France.

S'agissant de la responsabilité des producteurs d'algorithmes, ou de la formation des utilisateurs, là encore ces garanties de fonds ne sont évoquées que dans la Charte éthique du CNB précitée et n'ont donc pas de valeur contraignante.

3 Principes généraux du droit

Les discussions autour des principes généraux du droit, et plus particulièrement des principes du droit pénal, restent essentiellement doctrinales. Plusieurs instances se saisissent cependant de la question depuis peu. La CNIL, dans son rapport Comment permettre à l'homme de garder la main, aborde ainsi certains enjeux « éthiques » intéressants les principes généraux du droit[205]. Le défenseur des droits s'est également saisi des problématiques en matière de discriminations liées à l'IA[206]. À son tour, la Commission Nationale Consultative des Droits de l'Homme (CNCDH) a rendu un avis sur l'impact de l'intelligence artificielle sur les droits fondamentaux[207], en proposant des modifications de la proposition de règlement européen relatif à l'intelligence artificielle[208]. Elle rappelle en outre que pour être considérée comme légitime, l'atteinte apportée par un système d'IA à une liberté doit être « adaptée, nécessaire et proportionnée »[209]. À cette fin, elle préconise une évaluation de l'impact sur les droits

---

[203] V. *Supra,* §2.2.

[204] V. not. A. Louvaris, « La justice prédictive entre être et devoir-être » in *La justice prédictive* (Paris, Dalloz thèmes et commentaires 2018) 36, ainsi que le rapport de la Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, *L'open data des décisions de justice*, (2017), *op. cit*. Recommandation n°20.

[205] CNIL, *Comment permettre à l'homme de garder la main, Les enjeux éthiques des algorithmes et e l'intelligence artificielle*, Synthèse du débat public (2017).

[206] Défenseur des droits, *Algorithmes, prévenir l'automatisation des discriminations*, (2020). L'institution s'est également saisie de la question de la reconnaissance faciale : *Technologies biométriques : l'impératif respect des droits fondamentaux*, (2021) et a participé avec Equinet (European Network of Equality Bodies) à la rédaction d'un avis établissant des recommandations et des principes essentiels pour la future législation européenne portant sur l'intelligence artificielle, intitulé *Pour une IA européenne protectrice et garante du principe de non-discrimination,* (2021).

[207] CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, (2022), n° A-2022-6 du 7 avril.

[208] Proposition de règlement du parlement européen et du conseil *établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union*, com/2021/206 final

[209] CNCDH (2022), *op. cit*., §25. Si la Cour européenne des droits de l'Homme vérifie que la restriction aux libertés est prévue par une loi, le droit français l'impose déjà à l'article 4 de la Déclaration des Droits de

fondamentaux des applications utilisant l'IA, préalablement à leur mise en œuvre, accompagnée d'une consultation des parties prenantes. L'avis détaille les modalités et le contenu de l'étude d'impact ainsi souhaitée, comportant notamment l'identification des droits fondamentaux susceptibles d'être affectés et les mesures d'atténuation des risques envisagées. La CNCDH invite également à une vigilance continue tout au long de la durée d'utilisation de ces applications[210].

3.1 Égalité et lutte contre les discriminations

La CNIL attire l'attention sur les risques de biais et de discriminations pouvant découler de la conception d'un algorithme, en prenant notamment comme exemple l'application COMPAS (Correctional Offender Management Profile for Alternative Sanction) visant à produire un score de risque de récidive pour les auteurs d'infractions mais révélant des dérives racistes des résultats[211]. L'autorité propose d'étendre le principe de loyauté formulé par le Conseil d'État en 2014[212], « un algorithme loyal ne devrait pas avoir pour effet de susciter, de reproduire ou de renforcer quelque discrimination que ce soit, fût-ce à l'insu de ses concepteurs »[213]. Par ailleurs, toutes les dispositions normatives interdisant toutes formes de discrimination sont applicables, sur le fondement du principe d'égalité devant la loi pénale, principe constitutionnel garanti par l'article 6 de la Déclaration des droits de l'homme et du citoyen de 1789[214].

---

l'Homme et du Citoyen (1789) ayant valeur constitutionnelle. Le Conseil Constitutionnel et le Conseil d'État contrôlent alors la proportionnalité de l'atteinte aux libertés à la lumière du triple test emprunté au droit allemand, V. CC, 21 février 2008, Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental, n° 2008-562 pt. 13 ; M. Guyomar, « Le passeport biométrique au contrôle : empreintes et cliché », (2012) *Actualité Juridique Droit Administratif*, 35 ; J.-M. Sauvé, « Le principe de proportionnalité, protecteur des libertés », Institut Portalis, (2017), Aix-en-Provence, <https://www.conseil-etat.fr/publications-colloques/discours-et-interventions/le-principe-de-proportionnalite-protecteur-des-libertes>

[210] CNCDH, (2022), Recommandations n° 9, 10,11 not.

[211] CNIL *Comment permettre à l'homme de garder la main, Les enjeux éthiques des algorithmes et e l'intelligence artificielle*, *op. cit.*, 32.

[212] Conseil d'État, *Le Numérique et les droits fondamentaux*, (2014), 273 et 278,281.

[213] CNIL, *Comment permettre à l'homme de garder la main, Les enjeux éthiques des algorithmes et e l'intelligence artificielle*, Synthèse du débat public, (2017), 49.

[214] Not. L'article 225-1 du Code pénal qui incrimine toute discrimination entre personnes physiques fondée sur « leur origine, de leur sexe, de leur situation de famille, de leur grossesse, de leur apparence physique, de la particulière vulnérabilité résultant de leur situation économique, apparente ou connue de son auteur, de leur patronyme, de leur lieu de résidence, de leur état de santé, de leur perte d'autonomie, de leur handicap, de leurs caractéristiques génétiques, de leurs mœurs, de leur orientation sexuelle, de leur identité de genre, de leur âge, de leurs opinions politiques, de leurs activités syndicales, de leur capacité à s'exprimer dans une langue autre que le français, de leur appartenance ou de leur non-

De même, le Défenseur des droits préconise la vigilance et la sanction à l'égard des décisions discriminatoires issues de traitements algorithmiques[215]. Il attire cependant l'attention sur l'inefficacité des protections existantes face au manque de transparence des systèmes et au caractère souvent invisible des discriminations qu'ils emportent.

3.2 Droit à un procès équitable

Le droit à un procès équitable est consacré par l'article 6§1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales d'abord comme le droit d'accès au juge : « Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi (…) ». Il est complété par la jurisprudence de la Cour européenne des droits de l'homme, notamment par le principe du contradictoire, le droit à un recours effectif ou celui d'égalité des armes.

Les risques d'atteinte à ces droits fondamentaux par des outils de justice prédictive (d'aide à la décision ou de prise de décision) sont mis en évidence par la doctrine[216] et par les autorités administratives indépendantes (AAI)[217]. La justice prédictive, en fournissant des statistiques ou des probabilités sur l'issue d'un procès, peut conduire à résoudre des litiges en dehors du juge[218]. Un auteur souligne ainsi les limites des algorithmes qui peuvent conduire les justiciables à renoncer à un procès sur le fondement de statistiques biaisées, alors que le renoncement à un droit protégé par la CEDH doit être libre et éclairé[219].

De même, les principes d'indépendance et d'impartialité du juge sont menacés par le recours à des outils de justice prédictive, au regard de la neutralité des algorithmes utilisés. La doctrine[220], tout comme les praticiens[221], ont souligné le risque performatif des logiciels prédictifs: le juge peut être conduit à suivre la solution adoptée par la majorité

---

appartenance, vraie ou supposée, à une ethnie, une Nation, une prétendue race ou une religion déterminée. »

[215] Défenseur des droits, *Algorithmes : prévenir l'automatisation des discriminations*, (2020).

[216] S. Amrani Mekki, « Le point de vue d'une universitaire », in *La justice prédictive*, sous la direction de l'Ordre des avocats au Conseil d'État et à la Cour de cassation, (Paris, Dalloz, Thèmes et commentaires, 2018), 49 ; V. aussi S.-M. Ferrié, « Les algorithmes à l'épreuve du droit au procès équitable », (2018) *La Semaine Juridique Edition Générale* n° 11, 12 Mars, doctr. 29.

[217] V. not. CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, (2022), *op. cit*, note 116.

[218] S. Amrani Mekki, « Le point de vue d'une universitaire », (2018) *op. cit.* 58.

[219] S.-M. Ferrié, « Les algorithmes à l'épreuve du droit au procès équitable », (2018) *op.cit,* note 125.

[220] V. *Supra* et A. Garapon 'Les enjeux de la justice prédictive,' (2017) *JCP G* no. 1-2, 9 janvier, doctr. 31.

[221] V. not. l'intervention de J.-M. Sauvé à l'occasion du colloque « La justice prédictive », organisé à l'occasion du bicentenaire de l'Ordre des avocats au Conseil d'État et à la Cour de cassation le 12 février 2018., https://www.conseil-etat.fr/publications-colloques/discours-et-interventions/la-justice-predictive, consulté le 6 avril 2022.

et renforce à son tour cette majorité[222]. Malgré la recommandation d'ériger en principe la neutralité des algorithmes[223], ce risque de préjugé porte atteinte à l'indépendance et à l'impartialité du juge et saurait difficilement être résolu par la procédure de récusation, voire le renvoi pour cause de suspicion légitime si les magistrats ont accès aux mêmes outils de justice prédictive[224].

La CNCDH, à son tour, doute de l'impartialité d'un juge qui serait tenté de reprendre quasi-systématiquement les résultats fournis par le logiciel de prédiction judicaire par algorithmes « au regard de la charge de travail qui pèse actuellement sur les magistrats »[225].

La doctrine souligne quant à elle la difficulté de qualifier un algorithme de tribunal au sens de l'article 6§1 CEDH, du moins de sa faculté à offrir toutes les garanties attachées à cette notion. Ajouté au fait que l'algorithme syllogistique ne rend pas compte de la réalité et de la complexité d'une décision de justice, ce constat fait douter de la conformité des outils de justice prédictive avec le droit à un procès équitable[226].

3.3 Droit d'accès à un juge humain et droit de recours contre les algorithmes

La CNIL souligne que, malgré l'interdiction formulée par la loi Informatique et libertés de fonder une décision entraînant des effets juridiques à l'égard d'une personne sur le seul fondement d'un traitement automatisé de données à caractère personnel, l'automatisation des décisions se répand, et l'interprétation de la loi s'assouplit[227]. Elle propose alors de penser l'intervention de l'humain non pas au niveau de chaque décision individuelle, ce qui anéantirait le rôle d'optimisateur de l'algorithme, mais à un niveau collectif : « On pourrait, par exemple, assurer que des formes de délibération humaine et contradictoire encadrent et accompagnent l'utilisation des algorithmes en examinant et en interrogeant le paramétrage mais aussi tous les effets – directs et indirects – du système. Cette supervision pourrait ainsi porter, non pas sur chaque décision individuelle, mais de loin en loin sur des séries plus ou moins nombreuses de décisions. »[228].

---

[222] S.-M. Ferrié, « Les algorithmes à l'épreuve du droit au procès équitable », (2018) *op.cit*.

[223] Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, *L'open data des décisions de justice*, (2017) *op. cit*. Recommandation n° 20.

[224] Articles 668 et 662 C. Proc. pén., V. J.-M. Brigant, « Les risques accentués d'une justice pénale prédictive », (2018) *Arch. phil. Droit* no. 60, 57.

[225] CNCDH, (2022) op. cit., note 116, §29.

[226] S.-M. Ferrié, « Les algorithmes à l'épreuve du droit au procès équitable », (2018) *op.cit*, note 125.

[227] CNIL, *Comment permettre à l'homme de garder la main, Les enjeux éthiques des algorithmes et e l'intelligence artificielle*, (2017) *op. cit*., 52.

[228] *Ibid*.

La CNCDH recommande quant à elle l'information systématique des personnes faisant l'objet d'une décision se fondant en tout ou partie sur un traitement algorithmique. De la même façon elle recommande de garantir à la personne concernée un droit au réexamen, par un être humain, de toute décision individuelle fondée totalement, ou même en partie, sur un traitement algorithmique, dès lors qu'elle emporte des conséquences significatives pour elle[229].

La question des voies de recours, en revanche, ne fait pas l'objet de discussion particulière. Les possibilités de recours contre les traitements automatisés de données à caractère personnel prévus par la loi Informatique et Libertés semblent suffisantes en l'état actuel. Cependant, la loi ne s'applique pas en dehors de l'utilisation de données personnelles. En matière pénale, l'exemple peut être cité du traitement automatisé des infractions routières constatées par les radars automatiques, pour lequel un recours est possible devant le tribunal de police[230].

S'agissant de la réalité d'un second degré de juridiction lorsque la juridiction d'appel use des mêmes logiciels prédictifs, elle ne semble pas évoquée, cette possibilité étant encore simplement virtuelle, encore plus en matière pénale.

3.4 Principes constitutionnels

Outre le principe d'égalité[231], d'autres principes constitutionnels sont menacés par la justice prédictive.

Il s'agit d'abord du principe de légalité criminelle, consacré par l'article 7 de la Déclaration des droits de l'homme et du citoyen, menacé par l'avènement d'algorithmes fondés sur les précédents judiciaires plus que sur la règle de droit elle-même[232]. La conception des algorithmes par des entreprises privées peut également mettre en question le rôle du législateur dans la définition du droit pénal.

S'agissant du principe d'interprétation stricte de la loi pénale, corollaire du principe de légalité, s'il proscrit l'interprétation par analogie, il n'empêche pas la jurisprudence de recourir au raisonnement téléologique, recherchant la finalité du texte propre à l'adapter au contexte social de l'infraction. Or, la reproduction des décisions, induite par les algorithmes et un raisonnement mathématique qui n'intégrerait pas cette vision humaine

[229] CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, (2022) n° A-2022-6 du 7 avril, recommandations n° 17 et 18.
[230] art. 529-11 C. Proc. pén.
[231] V. *Supra* § 3.1.
[232] J.-M. Brigant, « Les risques accentués d'une justice pénale prédictive », (2018) *op. cit*., 52.

de l'application de la loi, annihilerait toute possibilité de revirements de jurisprudence[233].

Il en est de même du principe de nécessité des peines, consacré quant à lui par l'article 8 de la Déclaration des droits de l'homme et du citoyen. Ce principe a pour corollaire le principe d'individualisation des peines inscrit à l'article 132-1 du Code pénal : « Toute peine prononcée par la juridiction doit être individualisée. / Dans les limites fixées par la loi, la juridiction détermine la nature, le quantum et le régime des peines prononcées en fonction des circonstances de l'infraction et de la personnalité de son auteur ainsi que de sa situation matérielle, familiale et sociale, conformément aux finalités et fonctions de la peine énoncée à l'article 130-1. ». Or « la barémisation automatique des peines applicables pour les infractions commises »[234] contreviendrait non seulement au principe d'individualisation, mais aussi à l'exigence de motivation qui concerne aujourd'hui toutes les peines prononcées[235].

En revanche, bien que l'utilisation des outils actuariels d'évaluation des risques de récidive soit étudiée, notamment au regard des expériences étrangères, les auteurs ne s'interrogent pas sur le respect de la présomption d'innocence par ces outils[236].

[233] *Ibid*., p. 53 : l'auteur constate qu'une justice algorithmique n'aurait sans doute pas permis l'immunité du salarié pour le vol de documents au préjudice de son employeur.
[234] *Ibid*. p. 54.
[235] Art. 132-19 et 132-20 C. pén. en matière correctionnelle et contraventionnelle, art. 365-1 C. pén. en matière criminelle.
[236] V. Par exemple P.-L. Déziel, « L'utilisation de renseignements personnels dans le contexte de la justice prédictive : le cas des outils actuariels d'évaluation des risques de récidive", (2018) *Arch. Phil. Droit* 60, 253.

TROISIEME PARTIE : DROIT DE LA PREUVE ET INTELLIGENCE ARTIFICIELLE

Emmanuelle GINDRE *

À titre liminaire, il convient de définir les notions utilisées dans ces développements, telles qu'elles sont appréhendées par les services enquêteurs notamment. L'intelligence artificielle est envisagée ici comme un outil qui va soit permettre de collecter, soit permettre de produire des indices. Ces indices ne deviennent des preuves pénales que par la force probante qui y sera attachée par le juge et qui doit emporter son intime conviction. La preuve judiciaire doit ainsi être distinguée de la preuve scientifique, qui, elle, est irréfutable, même si le résultat n'est qu'une probabilité.

En France domine le système de la liberté de la preuve en matière pénale. L'article 427 du code de procédure pénale autorise tout mode de preuve que le juge accueille selon son intime conviction. Les preuves collectées ou produites au moyen de l'intelligence artificielle sont donc en principe admises, avec les seules restrictions tenant à la licéité et à la loyauté applicables aux autorités d'enquête et sous réserve de l'autorisation, le cas échéant, des algorithmes utilisés.

1 Collecte d'indices grâce à des systèmes basés sur l'IA

1.1 Pratiques nationales

Plusieurs systèmes basés sur l'IA sont utilisés en France pour collecter des indices qui pourront être utilisés comme preuves dans le cadre judiciaire. Ces systèmes sont majoritairement utilisés par les autorités de police judiciaire, mais peuvent également être déployés dans le cadre d'enquêtes internes, de contrôle de conformité au sein des entreprises ou encore, dans le cadre du contrôle du respect de leur règlementation par certaines administrations.

1.1.1 Utilisation de systèmes de collecte d'indices basés sur l'IA par les services de police judiciaire

Les fichiers d'analyse sérielle.

Les fichiers d'analyse sérielle utilisent des logiciels de traitement automatisé de données personnelles, qui permettent de « rassembler les preuves et d'identifier les auteurs, grâce à l'établissement de liens entre les individus, les événements ou les infractions »[237]. Ainsi,

* 1. Univ. Polynésie française, GDI EA 4240, Tahiti, Polynésie française; 2. UPPA, IFTJ, EA 7504, Centre de recherche sur la justice pénale et pénitentiaire, Pau, emmanuelle.gindre@upf.pf .

[237] Art. 230-12 C. proc. pén.

le logiciel SALVAC (Système d'Analyse des Liens de la Violence Associée aux Crimes) est un logiciel d'analyse sérielle, importé du Canada, utilisé depuis 2003 par la police et la Gendarmerie nationales. Il permet d'opérer des rapprochements entre des affaires criminelles de violence (homicides, viols, agressions sexuelles et tentatives). Il intègre également des données relatives aux disparitions supposées criminelles, aux découvertes de cadavres inconnus, ainsi que des données de procédure (mode opératoire, horaire des faits, habitudes des victimes, propos tenus par les auteurs des crimes). Depuis sa mise en service, le logiciel a mémorisé plus de 15 000 dossiers, dont les informations sont réparties en plus de 150 rubriques, étudiées par 11 analystes spécialisés[238]. Le logiciel est également utilisé par d'autres pays européens, comme la Belgique, le Royaume-Uni, la Suisse et l'Allemagne, ce qui permet des recoupements d'informations lorsque des crimes similaires ont lieu dans ces pays.

L'utilisation de l'IA par ce logiciel reste pour l'heure limitée : il s'agit d'une base de données, donnant une représentation visuelle des liens entre dossiers, encore alimentée par les enquêteurs eux-mêmes, et dont les résultats sont également analysés par l'intelligence humaine. Une évolution est cependant envisagée pour exploiter plus largement les progrès de l'IA dans l'analyse de masses de données, tant pour l'automatisation de la collecte des données que pour l'utilisation d'algorithmes dans l'analyse de ces données[239].

D'autres logiciels d'analyse sérielle sont utilisés à des fins d'aide à l'enquête et pourront également, à brève échéance sans doute, être rendus plus efficaces par l'IA.

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
BABCO (base atteintes aux biens et criminalité organisée)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Identifier les auteurs, co-auteurs ou complices de faits sériels nationaux et transfrontaliers pour toutes les infractions sérielles afférentes aux atteintes aux biens (VAMA, vols quelle que soit la nature du butin, cambriolages, recels en tout genre) punies d'une peine d'emprisonnement d'au moins 5 ans

[238] V. E. Paolini, « Tueurs en série : comment le logiciel enquêteur Salvac «assemble les pièces du puzzle» » (16 octobre 2021), *Le Figaro*, https://www.lefigaro.fr/faits-divers/tueurs-en-serie-comment-le-logiciel-enqueteur-salvac-assemble-les-pieces-du-puzzle-20211016 .

[239] S. Pétroff, « La police judiciaire à l'épreuve de la donnée massive : Moore a rendez-vous avec Locard » (octobre 2022), *La jaune et la rouge*, n° 778, https://www.lajauneetlarouge.com/la-police-judiciaire-a-lepreuve-de-la-donnee-massive-moore-a-rendez-vous-avec-locard/

BAM (base anti-mafia)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Identifier les auteurs, co-auteurs ou complices de faits sériels régionaux et transfrontaliers pour toutes les infractions afférentes aux phénomènes mafieux et de criminalité organisée au sein de la RGPACA punies d'une peine d'emprisonnement d'au moins 5 ans
Base de l'OCLDI (office central de lutte contre la délinquance itinérante)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Analyser, exploiter et transmettre toute documentation relative aux faits et infractions liés à la délinquance itinérante et punis d'une peine d'emprisonnement d'au moins 5 ans
Base escroqueries	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Identifier les auteurs, co-auteurs ou complices de faits sériels nationaux et transfrontaliers pour toutes les infractions sérielles afférentes aux escroqueries en tout genre punies d'une peine d'emprisonnement d'au moins 5 ans
Base Harpie (base Harpie du COMGEND Guyane)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Lutte contre l'orpaillage illégal, infractions relatives à des exploitations minières illicites susceptibles de causer des dommages écologiques sévères punies d'une peine d'emprisonnement d'au moins 5 ans
CALIOPE (base de comparaison et analyse logicielles des images d'origine pédopornographiques)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Trier et rapprocher les éléments relatifs à l'exploitation sexuelle de mineurs, fournir des contenus illicites utilisés lors des actions de « cyberpatrouille »
FPNID (fichier des personnes non identifiées ou disparues)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Retrouver et identifier les personnes disparues et les victimes lorsque celles-ci ont fait l'objet d'infractions à caractère sériel afférentes aux homicides, enlèvements, séquestrations, actes de tortures et de barbarie commis en tous lieux et punis d'une peine d'emprisonnement d'au moins 5 ans
PITEH (base personnes impliquées dans la traite des êtres humains)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Identifier les auteurs, co-auteurs ou complices de faits sériels nationaux et transfrontaliers pour toutes les infractions sérielles afférentes à la traite des êtres humains, dans toutes ses composantes (sexuelle, économique, frauduleuse, …) commis en tous lieux et punis d'une

			peine d'emprisonnement d'au moins 5 ans
SALVAC (système d'analyse des liens de la violence associée aux crimes)	DGPN (DCPJ)	Décret n° 2009-786 du 23 juin 2009	Faciliter la constatation des crimes et délits portant atteinte aux personnes et présentant un caractère sériel, rassembler les preuves et identifier les auteurs, grâce à l'établissement de liens entre les individus, les événements ou les infractions pouvant mettre en évidence ce caractère sériel
SERAFIM (système d'exploitation, de recherche et d'analyse sur les filières d'immigration)	DGPN (DCPAF)	Engagement de conformité du 28 janvier 2014 au décret cadre du 22 novembre 2013 relatif aux bases d'analyse sérielle	Mettre à disposition de l'ensemble des enquêteurs des services d'investigation de la DCPAF, les données judiciaires inhérentes à la lutte contre les filières d'immigration irrégulière issues des enquêtes judiciaires en cours, en vue d'effectuer des recoupements

Les logiciels de rapprochement judiciaire.

Créés en 2011[240], ils sont « destinés à faciliter l'exploitation et le rapprochement d'informations sur les modes opératoires »[241] pour faciliter le rassemblement des preuves et la recherche des auteurs d'infractions. Les logiciels d'analyse criminelle, dits ANACRIM, appartiennent à cette catégorie, et utilisent la suite logicielle Analyst's Notebook (ANB). Le fonctionnement est assez proche de SALVAC, consistant en une base de données dont les entrées peuvent être liées entre elles. Le degré d'IA reste donc limité, mais, de même que pour SALVAC, les possibilités de développement s'accroissent avec les progrès de l'IA.

Ces logiciels sont les suivants :

- ANACRIM – ATRT est un traitement d'exploitation automatisée de relevés bancaires et de documents téléphoniques (facturation détaillée, localisation de relais, etc.), obtenus

[240] Loi n°2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure (14 mars 2011), JORF n° 62 du 15 mars 2011.
[241] Art. 230-20 C. proc. pén.

sur réquisitions judiciaires, afin de mettre en évidence les liens entre les données collectées ;

- ANACRIM-ANB est un logiciel permettant l'analyse et la représentation visuelle de données sous forme de graphiques relationnels ou événementiels ;

- ANACRIM ANG permet, en complément du précédent, la gestion des données d'enquête pour les affaires complexes, notamment celles mettant en cause une multiplicité de faits ;

- ANACRIM – IVC est un traitement destiné à faciliter la gestion des données dans le cadre des procédures d'identification des victimes de catastrophes.

Analyse des données de téléphonie.

MERCURE est un logiciel d'investigation, utilisé depuis 2009 en France, permettant aux services de police judiciaire d'analyser et de traiter, dans tous les cadres d'enquêtes judiciaires, les données de téléphonie difficilement exploitables de façon manuelle. Il permet d'analyser les factures détaillées, les trafics sur antennes GSM, d'extraire les données des mémoires et cartes SIM des téléphones, mais aussi des disques durs d'ordinateurs[242]. Il intervient notamment dans le traitement des données transmises par la plate-forme nationale des interceptions judiciaires[243].

Extractions et décryptage des données d'un appareil mobile.

S'agissant de l'extraction des données, jusqu'à présent, les téléphones saisis devaient être envoyés dans l'un des centres spécialisés de la police technique et scientifique, ce qui pouvait allonger les délais d'investigation. Cependant, depuis 2019 et la signature d'un marché avec l'entreprise israélienne Cellebrite, le ministère de l'Intérieur équipe les commissariats d'un boîtier Cellebrite UFED, capable d'extraire les données des téléphones chiffrés ou verrouillés en quelques minutes, ce qui permettra un recueil de preuves beaucoup plus rapide[244], bien que toujours soumis à autorisation.

---

[242] https://ockham-solutions.fr/site/produits/mercure/mercure-v4.html

[243] Décret n° 2014-1162 relatif à la création de la « Plate-forme nationale des interceptions judiciaires », (9 octobre 2014), *JORF* n°236 du 11 oct. 2014 ; V. Aussi l'avis de la CNIL, Délibération n° 2014-009 portant avis sur un projet de décret autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires » (16 janvier 2014), *JORF* n°236 du 11 oct. 2014.

[244] V. https://www.liberation.fr/checknews/2019/11/28/les-commissariats-francais-vont-ils-s-equiper-d-un-outil-qui-permet-d-aspirer-les-donnees-des-teleph_1765867/ ; V. Aussi la présentation sur le site de l'entreprise: https://cellebrite.com/wp-content/uploads/2021/03/ProductOverview_Cellebrite_UFED_A4_fr_web.pdf

1.1.2 Utilisation de systèmes de collecte d'indices par les entreprises privées

Des solutions de collecte de preuves basées sur l'IA sont également développées à destination des entreprises. L'analyse forensic, au sens d'investigation numérique, est ainsi proposée par des cabinets d'avocats ou d'audit afin d'assister les entreprises dans le cadre d'un audit interne, d'une mise en conformité (dans le cadre de programmes anti-corruption ou anti-blanchiment) ou de poursuites pénales. Ces cabinets s'appuient sur des logiciels développés par des entreprises françaises, comme Théolex, start-up française spécialiste de l'analyse juridique des données[245], ou par des entreprises étrangères, comme RelativityOne[246]. L'IA utilisée est de type Machine Learning, voire Deep Learning[247], et permet d'analyser une grande quantité de données pour les classer, les regrouper par thème, pour rechercher des indices de fraudes dans des milliers de documents et de courriers électroniques, ou encore par comparaison, pour élaborer une stratégie de défense face au risque pénal.

1.1.3 Utilisation de systèmes de collecte d'indices par les administrations

L'administration fiscale a développé depuis 2021 le recours à l'IA dans le cadre de la lutte contre la fraude fiscale et l'exploitation des bases de données (datamining). Ce sont désormais près de 50% des contrôles fiscaux qui sont ainsi réalisés, les algorithmes permettant, à partir de modèles, de déterminer des probabilités de fraude[248].

L'IA est également utilisée sur les images fournies par l'Institut national de l'information géographique et forestière (IGN). Un système de reconnaissance d'image permet d'identifier les immeubles bâtis et les piscines et de croiser ces informations avec les bases de données des déclarations pour déterminer si les propriétés bâties sont correctement imposées. Les résultats sont très positifs pour l'administration fiscale depuis le lancement de l'expérimentation[249].

---

[245] V. https://www.decideurs-magazine.com/droit/40789-enquetes-penales-transfrontalieres-la-legaltech-francaise-gagne-du-terrain.html

[246] https://www.relativity.com/ediscovery-software/relativityone/

[247] https://www.grantthornton.fr/fr/insights/articles-et-publications/2022/relativityone-une-boite-a-outils-forensic/

[248] F. Perrotin, « Comment Bercy utilise l'intelligence artificielle pour cibler ses contrôles fiscaux » (19 octobre 2022) *Lextenso, Actu-juridique.fr*, https://www.actu-juridique.fr/fiscalite/fiscal-finances/comment-bercy-utilise-lintelligence-artificielle-pour-cibler-ses-controles-fiscaux/, consulté le 19 mai 2023.

[249] X. Martinage, « Des milliers de piscines repérées par le fisc grâce à l'intelligence artificielle » (22 mars 2023), *Capital*, https://www.capital.fr/votre-argent/des-milliers-de-piscines-reperees-par-le-fisc-grace-a-lintelligence-artificielle-1463704.

1.2 Cadre normatif

1.2.1 Les outils d'investigation numérique utilisés par les services d'enquête judiciaire.

Les systèmes traitant des données ou informations à caractère personnel qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté doivent être autorisés après avis motivé de la Commission Nationale de l'Informatique et des Libertés qui en vérifie la conformité avec la loi dite « Informatique et libertés » de 1978[250]. La collecte de preuves dans le cadre d'une procédure pénale et leur traitement est encadrée par le code de procédure pénale. Ce dernier régit ainsi des fichiers d'investigation, des fichiers d'identification ainsi que l'utilisation de logiciels de rapprochement judiciaire[251]. Tous ces outils, on l'a vu, s'appuient ou pourront s'appuyer à court terme, sur l'intelligence artificielle.

Les fichiers d'analyse sérielle.

Le premier logiciel d'analyse sérielle, SALVAC, a d'abord été utilisé dès 2003 en dehors de tout cadre légal, avant d'être encadré par la loi du 12 décembre 2005[252] et le décret du 23 juin 2009[253]. La loi du 12 décembre 2005 créé un régime dérogatoire pour le recueil des informations alimentant les logiciels d'analyse sérielle, puisqu'il suffit de raisons sérieuses, et non pas seulement d'indices graves ou concordants, de soupçonner qu'une personne a commis ou tenté de commettre un crime ou un délit grave pour figurer dans SALVAC[254]. De même, le logiciel peut mémoriser l'identité d'une personne simplement citée dans une procédure, ou conserver, sur prescription du procureur de la République, les informations relatives à une personne alors qu'elle en aura demandé l'effacement et que l'auteur a été condamné[255]. La durée de conservation des données dans ce logiciel est de quarante ans[256].

---

[250] Loi n° 78-17 *op. cit.* (n 187), art. 31 et 32.

[251] D'après la classification présentée par J. Buisson, « Preuve » (oct. 2020) *Répertoire de droit pénal et procédure pénale, Dalloz*, n° 84s. V. Aussi la Circulaire du 18 août 2014 relative aux fichiers d'antécédents judiciaires, *BOMJ* n°2014-08 du 29 août 2014.

[252] Loi n° 2005-1549 relative au traitement de la récidive des infractions pénales (12 décembre 2003), *JORF* n° 289 du 13 décembre, Art. 30 insérant un art. 21-1 dans la loi n° 2003-239 pour la sécurité intérieure (18 mars 2003), *JORF* n° 66 du 19 mars 2003.

[253] Décret n° 2009-786 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « Système d'analyse des liens de la violence associée aux crimes » (23 juin 2009), *JORF* n° 145 du 25 juin 2009.

[254] Loi n° 2005-1549 relative au traitement de la récidive des infractions pénales, Art. 30, *op. cit.* (n 251) V. aujourd'hui Art. 230-13 2° C. proc. pén.

[255] Art. 230-15 C. Proc. Pén., art. 6 du Décret n° 2009-786 *op. cit.* (n 252).

[256] Art. R. 40-36 C. proc. Pén. En revanche, la durée de conservation des données dans les bases d'analyse sérielle de police judiciaire est plus courte : 15 ans pour les délits, 20 ans pour les crimes, à compter de la date de clôture de l'enquête et de sa transmission au magistrat, V. Décret n°2013-1054 relatif au traitement

Les fichiers d'analyse sérielle sont aujourd'hui régis par les articles 230-12 à 230-18, R. 40-35 à R. 40-37 du Code de procédure pénale, et le décret-cadre n° 2013-1054 du 22 novembre 2013 relatif au traitement automatisé de données à caractère personnel dénommé « bases d'analyse sérielle de police judiciaire ». Ils regroupent des informations à caractère personnel concernant des suspects, des victimes, des témoins ou des personnes faisant l'objet d'une enquête pour recherche des causes de la mort ou de la disparition[257]. Leur utilisation, portant atteinte à la vie privée, est donc strictement encadrée. Ainsi, ces fichiers peuvent être utilisés dans le cadre d'enquêtes préliminaires, de flagrance ou d'investigations exécutées sur commission rogatoire, mais ne concernent que les crimes et délits présentant un caractère sériel et sanctionnés d'au moins cinq ans d'emprisonnement. En outre, le code de procédure pénale restreint les personnes habilitées à utiliser ces fichiers aux seuls personnels spécialement habilités de la police et de la Gendarmerie nationales, à certains personnels de l'État, ainsi qu'aux magistrats du parquet et magistrats instructeurs dans la limite des infractions dont ils sont saisis[258]. Il précise par ailleurs la durée de conservation des données recueillies[259] et les conditions auxquelles les personnes concernées peuvent en obtenir l'effacement ou la rectification[260]. Un droit de recours est prévu contre les décisions du procureur ou du magistrat compétent.

L'utilisation de l'IA dans ce cadre, bien qu'encore peu développée, est donc encadrée par la législation relative à la protection des données personnelles, garantissant un accès strictement limité à ces données et un droit à leur effacement ou rectification.

Les logiciels de rapprochement judiciaire.

Ils sont régis par d'autres dispositions du code de procédure pénale, les articles 230-20 à 230-27 et R. 40-39 à R. 40-41 du code de procédure pénale. Tous les logiciels utilisés doivent être préalablement autorisés par un décret en Conseil d'État, après avis de la CNIL.

Seuls les personnes habilitées chargées d'une mission de police judiciaire[261] ainsi que le service placé sous l'autorité du ministre du budget chargé d'effectuer des enquêtes judiciaires, peuvent mettre en œuvre ces traitements, en utilisant uniquement les

automatisé de données à caractère personnel dénommé « bases d'analyse sérielle de police judiciaire » (du 22 novembre 2013), *JORF* n° 273 du 24 novembre.

[257] Art. 230-12 C. proc. pén.

[258] Art. 230-10 et 230-16 C. proc. pén.

[259] Art. R. 40-27 C. proc. pén. pour le TAJ.

[260] Art. 230-8, 230-9, 230-11, 230-15 et 230-18 C. proc. pén.

[261] Les agents des services de la Police nationale, de la Gendarmerie nationale, les magistrats du parquet ou magistrats instructeurs dans le cadre de l'enquête pour laquelle ils sont saisis, le Procureur de la République et le magistrat chargé du contrôle, art. 230-25 C. proc. pén.

données déjà détenues dans le cadre des procédures[262]. L'identité d'une personne ne peut être révélée qu'à l'issue de l'opération de rapprochement, et les données personnelles doivent être effacées à la clôture de l'enquête ou à l'expiration d'un délai de 3 ans. La mise en œuvre des logiciels de rapprochement judiciaire, ainsi que l'autorisation qui l'accompagne, est mentionnée dans la procédure[263]. L'utilisation est réalisée sous le contrôle du Procureur de la République qui peut demander à ce que les données soient effacées, complétées ou rectifiées. La rectification en cas de requalification judiciaire est de droit pour la personne concernée qui la demande.

L'article 230-27 précise en outre que les décrets autorisant les logiciels de rapprochement judiciaire doivent indiquer les modalités selon lesquelles les personnes intéressées peuvent exercer leur droit d'accès.

Extraction et décryptage des données de téléphonie.

S'agissant de l'extraction et du décryptage des données d'un appareil mobile, le cadre juridique est fourni par les articles 230-1 à 230-5 C. Proc. pén. Constituant un chapitre intitulé « De la mise au clair des données chiffrées nécessaires à la manifestation de la vérité ». Cette procédure technique ne concerne que les données saisies ou obtenues lors d'une enquête ou d'une instruction. Sa mise en œuvre doit faire l'objet d'une autorisation: « le procureur de la République, la juridiction d'instruction, l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir l'accès à ces informations, leur version en clair ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire ».

Les résultats du décryptage sont communiqués à l'autorité mandante avec les indications techniques utiles à la compréhension et à leur exploitation ainsi qu'une attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis[264]. Tous les éléments obtenus sont consignés dans un procès-verbal versé au

[262] Le Conseil constitutionnel a apporté une réserve d'interprétation aux articles 230-20 et suivants : « Les dispositions des art. 230-20 s. n'ont pas pour objet et ne sauraient avoir pour effet de permettre la mise en œuvre d'un traitement général des données recueillies a l'occasion des diverses enquêtes mentionnées a l'art. 230-20. Les logiciels de rapprochement judiciaire ne pourront conduire qu'à la mise en œuvre, autorisée par le procureur de la République ou la juridiction compétente, de traitements de données a caractère personnel particuliers, dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations. Partant, ces dispositions ne sont pas contraires a la Constitution. », Cons. const. 10 mars 2011, n° 2011-625 DC ; *D*. 2012. Pan. 1638, obs. Bernaud et Jacquinot; *Dr. pénal* 2012. Chron. 2, obs. Garçon et Peltier.

[263] Art. R. 40-40 C. proc. Pén.

[264] Article 230-3 C. Proc. Pén.

dossier de la procédure, qui peut ensuite être consulté par la défense selon les règles de droit commun.

Le droit pénal s'est également enrichi depuis 2001 d'une incrimination spécifique sanctionnant le refus de remettre sur réquisition la convention secrète de chiffrement d'un moyen de cryptologie[265], dont les peines ont été renforcées en 2016, afin de faciliter la collecte de preuves numériques.

1.2.2 Les outils d'investigation numérique utilisés par les entreprises

Depuis l'entrée en vigueur du RGPD, la plupart des formalités de déclaration ou de demande d'autorisation à la CNIL ont disparu. Les entreprises doivent désormais respecter le RGPD et la protection des données personnelles, notamment des salariés à l'égard desquels serait mis en œuvre un traitement automatisé visant à collecter des preuves de leurs agissements illicites. La CNIL peut cependant contrôler la proportionnalité du traitement des données ou informations à caractère personnel relatives aux salariés, au regard de l'objectif du traitement et vérifier que l'atteinte à la vie privée n'est donc pas disproportionnée[266]. En outre, le salarié doit être informé des outils de surveillance mis en œuvre[267]. À défaut, la preuve recueillie sera considérée comme illicite[268].

En dehors du respect du cadre législatif de la protection des données personnelles, les applications d'investigation numérique développées au service des entreprises ne font pas l'objet d'un encadrement juridique spécifique.

1.3 Contrôle jurisprudentiel de la mise en œuvre des systèmes d'investigation numérique

1.3.1 Conservation des données de connexion et accès à ces données

La jurisprudence française s'est développée, récemment et tardivement, en matière de données de connexion (résultats d'un traitement par l'intelligence artificielle), sous l'influence de la jurisprudence de la Cour de Justice de l'Union européenne appliquant

[265] Article 434-15-2 C. Pén. : « Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale. »
[266] Article 9 C. civ., Art. 8 Conv. EDH, art. L. 1121-1 C. trav.
[267] Art. L 1224-4 C. trav.
[268] Cass. soc. 4 juillet 2012 n°11-30.266.

les directives dites ePrivacy[269]. Le Conseil Constitutionnel et la Cour de cassation sont venus préciser le cadre juridique de la conservation des données de connexion, ainsi que de l'accès à ces données.

La conservation généralisée et indifférenciée des données de trafic et de géolocalisation, permise par l'article L. 34-1 du code des postes et des communications électroniques, a été mesurée au motif qu'elle porte une atteinte disproportionnée au respect de la vie privée[270]. La seule exception européenne permettant une conservation généralisée concerne les cas de menaces graves pour la sécurité nationale. La Cour de cassation définit alors la sécurité nationale, par référence aux atteintes aux intérêts fondamentaux de la nation et au terrorisme (les deux premiers titres du livre IV du Code pénal), et considère dans le même temps que les réquisitions judiciaires relatives aux données de connexion[271] valent injonction de conservation rapide (ce que permet l'Union européenne). Elle valide donc l'utilisation des données de connexion, conservées dans un but de sécurité nationale, pour les cas de criminalité grave. Cette jurisprudence a été consacrée par la loi n° 2021-998 du 30 juillet 2021, et le nouvel article 34-1 III bis[272] du Code des postes et des communications électroniques, étendant ainsi, de manière floue[273], le champ d'application des injonctions de conservation rapide.

Le cadre juridique de l'accès aux données de connexion a lui aussi été précisé par les juridictions suprêmes, toujours sous l'influence de la jurisprudence de l'Union européenne. La Cour de cassation censure ainsi les dispositions du code de procédure pénale permettant aux enquêteurs et au Ministère public d'accéder directement à des données de connexion par voie de réquisitions judiciaires, sans autorisation d'une autorité indépendante[274]. En revanche, elle restreint les cas de nullités des réquisitions à l'action de la victime d'une atteinte à la vie privée et à l'exigence d'un grief prouvé[275].

Le Conseil constitutionnel, comme la Cour de cassation, valide les accès réalisés par le juge d'instruction, ce dernier étant une autorité indépendante au contraire du procureur

[269] Directive 2002/58/CE, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (12 juill. 2002, mod., Dir. 2009/136/CE, 25 nov. 2009), *JOUE* L337 du 18 décembre 2009.

[270] Cons. constit., 25 févr. 2022 , n° 2021-976 et 2021-977 QPC : JurisData n° 2022-002957 ; D. 2022, p. 398 ; *AJDA* 2022, p. 432; Cass. crim., 12 juill. 2022 , n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652 : JurisData n° 2022-011502, 2022-011500 et 2022-011499 ; *AJ pénal* 2022, obs. M. Bendavid, C. Quendolo.

[271] Art. 60-1 et s., 77-1-1 et s. et 99-3 et s. C. Proc. Pén.

[272] « Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données. »

[273] La notion de manquements graves n'étant pas définie, le champ de la criminalité grave apparaît indéterminé et donc extensible. V. R. Ollard, « Droit pénal numérique - Un an de droit pénal numérique (octobre 2021 - octobre 2022) » (2022), *Droit pénal*, chron. 12.

[274] Articles 60-1, 60-2, 77-1-1 et 77-1-2 du Code de procédure pénale.

[275] Cass. crim., 12 juill. 2022, op. cit.

de la République[276]. Il n'est cependant pas aussi radical que la Cour de cassation, puisqu'il valide également le dispositif d'accès aux données de connexion lorsqu'il est appliqué dans le cadre de l'enquête de flagrance. Or, dans ce cadre, l'accès n'est soumis à aucune autorisation[277].

La loi du 2 mars 2022, en ajoutant un article 60-1-2 au code de procédure pénale, circonscrit, de manière imprécise, le champ des réquisitions en matière de données de connexion, mais ne modifie pas le titulaire du contrôle de ces réquisitions dans le cadre des enquêtes policières.

La jurisprudence en la matière se fonde donc essentiellement sur le respect de la vie privée dans le cadre des procédures pénales. Il n'en est pas de même en matière de décryptage des données de téléphonie, la Cour de cassation s'étant récemment interrogée sur le respect des droits de la défense.

1.3.2 Extraction et décryptage des données de téléphonie

Le 1er février 2022, la Cour de cassation a renvoyé au Conseil constitutionnel une question prioritaire de constitutionnalité (QPC), s'agissant de la possibilité discrétionnaire laissée au procureur de la République de recourir aux moyens de décryptage couverts par le secret de la défense nationale. Elle considère que cette décision « peut avoir pour conséquence que, par l'effet des règles concernant le secret-défense, de nombreuses informations utiles au contrôle de la régularité de l'opération ne puissent être soumises au débat contradictoire, ce qui est susceptible de constituer une atteinte excessive aux droits et libertés invoqués »[278]. Le Conseil constitutionnel considère au contraire qu' « en adoptant les dispositions contestées, le législateur a entendu permettre aux autorités en charge des investigations de bénéficier de moyens efficaces de captation et de mise au clair des données, sans pour autant fragiliser l'action des services de renseignement en divulguant les techniques qu'ils utilisent. ». Il précise également que la décision ne peut être prise que par le juge des libertés et de la détention ou le juge d'instruction et justifiée par les nécessités d'une enquête ou d'une information judiciaire relatives à certains crimes et délits d'une particulière gravité et complexité. Enfin, « si les dispositions contestées sont susceptibles de soustraire au contradictoire certaines informations techniques soumises au secret de la défense nationale » , certaines pièces demeurent obligatoirement versées au dossier de la procédure, comme l'ordonnance écrite et motivée du juge qui autorise la mise en œuvre d'un dispositif de captation, les différents procès-verbaux (de mise en place du dispositif, de transcription des données et de l'ensemble des éléments obtenus à l'issue des opérations de mise au

[276] Cons. const., 17 juin 2022 , n° 2022-1000 QPC : JurisData n° 2022-010483 ; D. 2022, p. 1154.
[277] A. Gogorza, « L'accès aux données de connexion : les affres du pluralisme normatif » (2022), *Droit pénal*, étude 20.
[278] Cass. crim., 1er févr. 2022, n° 21-85.148.

clair) et l'attestation visée par le responsable de l'organisme technique certifiant la sincérité des résultats transmis. Le Conseil constitutionnel valide donc les dispositions en cause[279].

La sincérité des résultats pourrait cependant être interrogée à court terme, certains dispositifs ayant récemment révélé des défaillances. C'est le cas du dispositif d'extraction et décryptage des données de téléphonie Cellibrite UFED, utilisé depuis 2019 par les services enquêteurs. L'un des principaux développeurs de la messagerie sécurisée Signal a mis en évidence une brèche dans le dispositif, dans laquelle il est possible de s'engouffrer pour exécuter du code informatique au moment de l'extraction des données d'un téléphone portable, permettant alors de falsifier les preuves récoltées par les enquêteurs[280]. Il n'est pas difficile d'imaginer le développement d'un contentieux sur la fiabilité de l'outil présenté comme révolutionnaire, d'autant que récemment la même société a été victime d'une fuite de données[281]…

2 Indices produits par les systèmes basés sur l'IA

2.1 La reconnaissance faciale

La reconnaissance faciale est une technologie biométrique, informatique et probabiliste de reconnaissance des visages[282], de type Machine Learning. Elle s'appuie sur des algorithmes qui recensent les caractéristiques particulières d'un visage pour déterminer un gabarit unique, comparé par le logiciel à d'autres gabarits déjà collectés ou calculés en direct. Le résultat de la comparaison est donné sous la forme d'un pourcentage de correspondance, d'une probabilité.

2.1.1 Utilisation de la reconnaissance faciale à des fins préventives et préconstitution de preuves

[279] Cons. constit., 8 Avril 2022, n° 2022-987 QPC.

[280] F. Reynaud, « Le pied de nez de Signal à Cellebrite, l'entreprise qui exploite les téléphones pour les forces de l'ordre » (22 avril 2021), *Le Monde*.

[281] G. Thierry, « La société Cellebrite victime d'une nouvelle fuite de données » (17 janvier 2023), *ZDNet*, https://www.zdnet.fr/actualites/la-societe-cellebrite-victime-d-une-nouvelle-fuite-de-donnees-39952706.htm .

[282] CNIL, Reconnaissance faciale pour un débat à la hauteur des enjeux (15 nov. 2019).

Bien que certaines expérimentations de reconnaissance faciale aient été tentées dans un objectif de prévention de la délinquance, avec l'accord des participants[283], il est impossible d'utiliser ces dispositifs en temps réel pour préconstituer des preuves.

La CNIL et le Conseil constitutionnel veillent à la protection des données personnelles et de la vie privée. La CNIL considère ainsi que « le sentiment de surveillance renforcée, l'exploitation accrue et potentiellement a grande échelle de données personnelles, pour certaines sensibles (données biométriques), la restriction de la liberté d'aller et de venir anonymement, sont autant de problématiques essentielles pour le bon fonctionnement de notre société démocratique »[284]. Elle rappelle que toute autorisation de l'utilisation des techniques de reconnaissance faciale doit respecter le RGPD et/ou la directive police-justice[285].

La loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure permet l'installation de vidéosurveillance dans les locaux de garde à vue ou de rétention, mais elle interdit tout dispositif biométrique, de captation du son ou tout couplage avec un autre système de traitement automatisé de données a caractère personnel[286]. De même, si elle autorise l'utilisation de dispositifs de caméras aéroportées, notamment des drones équipés, ainsi que de caméras embarquées, pour des opérations de police administrative, ces dispositifs ne peuvent inclure ni être reliés à un logiciel de reconnaissance faciale[287], ainsi que l'a précisé le Conseil constitutionnel[288]. S'agissant d'opérations de police judiciaire visant une ou des personnes déterminées, l'utilisation

[283] Par exemple par la ville de Nice au moment du Carnaval, L. Mercier, « La bataille de la reconnaissance faciale » (21 févr. 2019), *Nice Matin* ; C. Rotily, L. Archambault, « Données biométriques issues d'expérimentations de reconnaissance faciale sur le territoire français : un défi à l'aune du droit 2.0 ? » (2020) *Dalloz IP/IT*, 54. V. ce rapport, première partie : police prédictive.

[284] La CNIL appelle a la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo, https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-videoCNIL , V. Aussi CNIL, Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position, 29 oct. 2019, (En ligne), https://www.cnil.fr/fr/experimentation-de-la-reconnaissance - faciale -dans-deux-lycees-la-cnil-precise-sa-position.

[285] Directive (UE) 2016/680 relative a la protection des personnes physiques a l'égard du traitement des données a caractère personnel par les autorités compétentes a des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et a la libre circulation de ces données (27 avril 2016).

[286] Art. L. 256-3 C. Sécurité intérieure, E. Clément, « Loi responsabilité pénale et sécurité intérieure : souriez, vous êtes filmés » (8 février 2022), *Dalloz actualités*.

[287] Art. L 242-4 et Art. 243-3 C. Sécurité intérieure

[288] Cons. Constit. N° 2021-834 DC du 20 janvier 2022, consid. 30. « En dernier lieu, en application du deuxième alinéa de l'article L. 242-4 du code de la sécurité intérieure, les dispositifs aéroportés ne peuvent procéder à la captation du son, ni comporter de traitements automatisés de reconnaissance faciale. Ces dispositifs aéroportés ne peuvent procéder à aucun rapprochement, interconnexion ou mise en relation automatisé avec d'autres traitements de données à caractère personnel. Toutefois, ces dispositions ne sauraient, sans méconnaître le droit au respect de la vie privée, être interprétées comme autorisant les services compétents à procéder à l'analyse des images au moyen d'autres systèmes automatisés de reconnaissance faciale qui ne seraient pas placés sur ces dispositifs aéroportés. »

de caméras aéroportées n'implique logiquement pas de traitement automatisé de reconnaissance faciale, si bien que la captation, la fixation, la transmission et l'enregistrement sans leur consentement de l'image d'une ou de plusieurs personnes se trouvant dans un lieu public[289] n'ont pas été censurés par le Conseil constitutionnel[290].

En revanche, l'utilisation des enregistrements de vidéoprotection en entrée d'un traitement de reconnaissance faciale, peut, quant à elle, être autorisée dans les conditions fixées par la loi Informatique et Libertés[291]. S'agissant de preuves préconstituées, leur utilisation doit en effet être strictement encadrée, car les données sont recueillies en dehors de toutes les garanties du procès pénal. Le procureur de la République peut autoriser l'exploitation de ces données, en cas de nécessité et uniquement pour des crimes et délits passibles d'emprisonnement, limitativement énumérés[292].

À l'heure actuelle, le débat relatif à l'utilisation de logiciels de reconnaissance faciale reste vif entre ses partisans et ses détracteurs[293], tandis que la CNIL adopte une position de prudence et souligne l'importance de la proportionnalité des traitements envisagés aux fins poursuivies[294]. De son côté, la CNCDH « recommande d'interdire l'identification biométrique à distance des personnes dans l'espace public et les lieux accessibles au public, en admettant par exception son utilisation, dès lors que celle-ci est strictement nécessaire, adaptée et proportionnée pour la prévention d'une menace grave et imminente pour la vie ou la sécurité des personnes et celle des ouvrages, installations et établissements d'importance vitale »[295]. Elle craint en effet que cette technologie ait un impact négatif sur la liberté de réunion, la liberté de circulation ou d'autres droits fondamentaux[296].

L'utilisation de la reconnaissance faciale, et plus généralement des algorithmes de reconnaissance appliqués aux images de vidéoprotection mise en œuvre dans le cadre d'opérations de police administrative ou de renseignement, peut en effet révéler en temps réel la commission d'une infraction. Se pose alors la question du déclenchement de la phase d'enquête : pourrait-elle s'ouvrir par le constat de l'infraction réalisé par la machine ?

---

[289] Art. 230-47 à 230-53 C. Proc. Pén.

[290] Cons. Constit. n° 2021-834 DC du 20 janvier 2022, consid. 47.

[291] CSI, art. L 252-1 al. 2.

[292] C. proc. pén. art. 77-1-1.

[293] C. Rotily, L. Archambault, « Données biométriques issues d'expérimentations de reconnaissance faciale sur le territoire français : un défi à l'aune du droit 2.0 ? » (2020), Dalloz IP/IT, 54.

[294] CNIL, avis du 17 octobre 2019, *op. cit*. (n 283).

[295] CNCDH, *Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux*, n° A-2022-6 (7 avril 2022), recommandation n°6.

[296] Risque de « *chilling effect* » associé à l'utilisation de drones équipés d'un logiciel de reconnaissance faciale : CNCDH, *Avis sur la proposition de loi relative à la sécurité globale*, Assemblée plénière du 26 novembre 2020, *JORF* n°0290 du 1er décembre 2020, texte n° 83.

La loi du 19 mai 2023[297] prend toutes les précautions possibles à ce sujet. Cette loi permet en effet, à titre expérimental, pour une durée déterminée et dans des conditions strictement précisées (notamment dans le cadre des Jeux Olympiques et Paralympiques de Paris), d'appliquer des traitements algorithmiques aux images collectées par les systèmes de vidéoprotection autorisés sur le fondement du code de la sécurité intérieure. Ces traitements ont pour unique objet de détecter, en temps réel, des événements prédéterminés susceptibles de présenter ou de révéler certains risques prédéterminés, et de les signaler en vue de la mise en œuvre des mesures nécessaires par les services compétents. La loi exclut tout système d'identification biométrique, dont la reconnaissance faciale. Les traitements algorithmiques autorisés ne peuvent traiter aucune donnée biométrique ni procéder à aucun rapprochement, à aucune interconnexion ni à aucune mise en relation automatisée avec d'autres traitements de données à caractère personnel.

Enfin, la loi prend soin de préciser que ces traitements algorithmiques « procèdent exclusivement à un signalement d'attention (…). Ils ne produisent aucun autre résultat et ne peuvent fonder, par eux-mêmes, aucune décision individuelle ni aucun acte de poursuite »[298].

2.1.2 Utilisation de la reconnaissance faciale dans le cadre de l'enquête judiciaire

L'usage de la reconnaissance faciale dans le cadre de l'enquête judiciaire est soumis au régime applicable aux traitements automatisés de données personnelles. Ce régime est fixé par la loi Informatique et Libertés[299], amendée[300] à la suite de l'adoption du Règlement général pour la protection des données[301] et la transposition de la directive dite « Police-Justice »[302]. Cette loi qualifie les données biométriques de données sensibles, et édicte une interdiction de principe de traiter des données biométriques aux fins d'identifier une personne physique de manière unique.

Elle prévoit cependant une exception rendant licite la reconnaissance faciale « à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la

[297] Loi n° 2023-380 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, (19 mai 2023), *JORF* n° 116 du 20 mai 2023.
[298] *Ibid*. article 10.
[299] Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, *op. cit.* (n 187).
[300] Loi n° 2018-493 relative à la protection des données personnelles (20 juin 2018), *JORF* n° 141 du 21 juin 2018, et ses décrets d'application.
[301] Règlement (UE) 2016/679 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 (RGPD) (27 avril 2016), JOUE L 119/1.
[302] Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, dite Police-Justice (27 avril 2016), JOUE L 119/89.

matière » (art. 87). Elle doit alors être réalisée par une autorité compétente agissant dans un cadre législatif ou règlementaire, et « uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée » (art. 88). Le traitement des données biométriques doit être autorisé par décret en Conseil d'État pris après avis motivé et publié de la CNIL (art. 31 II).

Le code de procédure pénale, dans le respect de ce cadre strict, n'autorise la reconnaissance faciale qu'à partir des données du fichier des antécédents judiciaires (TAJ). L'article R. 40-26 permet en effet d'y enregistrer la « photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale (photographie du visage de face) » des personnes mises en cause ou des personnes décédées ou disparues faisant l'objet d'une enquête. Ce traitement biométrique a été validé par le Conseil d'État qui a relevé en outre que « le dispositif de reconnaissance faciale ne peut être utilisé par les services compétents qu'en cas de nécessité absolue, appréciée au regard des seules finalités du traitement, lorsque subsiste un doute sur l'identité d'une personne dont l'identification est requise »[303].

Le traitement de reconnaissance faciale ne peut être mis en œuvre à partir des informations contenues dans le TAJ, que par les agents individuellement désignés et spécialement habilités énumérés à l'article R. 40-28 C. proc. pén. S'agissant de recueillir un indice à l'aide de moyens techniques, ce traitement est soumis au régime des constatations[304]. Les constatations relèvent de la compétence de l'officier de police judiciaire (OPJ) qui peut recourir à toutes personnes qualifiées, avec ou sans l'autorisation du procureur de la République selon les cas, ou sur commission rogatoire du juge d'instruction[305]. Depuis la loi du 24 janvier 2023[306], l'article 55-1 du Code de procédure pénale permet à l'OPJ de procéder, ou faire procéder sous son contrôle, aux opérations permettant l'enregistrement, la comparaison et l'identification (notamment) des résultats des opérations de relevés signalétiques dans les fichiers de police selon les règles propres à chacun de ces fichiers[307]. L'autorisation du procureur de la République reste cependant requise pour l'accomplissement de ces opérations dans le cadre de l'enquête préliminaire[308]. En outre, l'habilitation nominative et spéciale prévue par l'article R. 40-28 du code de procédure pénale reste une condition de la légalité de cet acte d'investigation. La jurisprudence s'est d'ailleurs montrée très stricte dans

[303] Conseil d'État, 26 avril 2022, n° 442364.

[304] J. Buisson, « Preuve » (2020), *Répertoire de droit pénal et de procédure pénale, Dalloz*.

[305] C. proc. pén. art. 60, 77-1 et 81.

[306] Loi n° 2023-22 d'orientation et de programmation du ministère de l'intérieur (24 janvier 2023), JORF n° 21 du 25 janvier.

[307] Cette disposition est également applicable dans le cadre de l'enquête préliminaire et celui de l'instruction, C. proc. pén. art. 76-2 et 154-1.

[308] C. proc. pén. art. 76-2, alors que l'article 77-1 dispense d'autorisation les opérations de comparaison d'empreintes génétiques ou d'empreintes digitales.

l'appréciation de cette condition et exigeait que le nom de la personne habilitée figure dans le procès-verbal de consultation du TAJ sous peine de nullité[309].

Devant le risque accru de nullités de la procédure résultant de cette jurisprudence, la loi n° 2023-22 du 24 janvier 2023 a tempéré cette exigence[310]. Le nouvel article 15-5 du code de procédure pénale rappelle ainsi la nécessité de l'habilitation spéciale et individuelle pour l'accès au traitement de reconnaissance faciale, et la possibilité que cette habilitation soit contrôlée à tout moment, mais il exclut que l'absence du nom de la personne habilitée dans les actes de procédure puisse constituer en elle-même une cause de nullité de la procédure.

S'agissant des droits procéduraux, la nécessité et la proportionnalité de l'utilisation de la reconnaissance faciale peuvent être contrôlées par le juge, au regard du critère de subsidiarité posé par le Conseil d'État[311]. Le principe du contradictoire et les droits de la défense sont, quant à eux, garantis dans le cadre du régime des constatations, par la communication des résultats des examens techniques aux parties[312], qui peuvent ensuite solliciter une expertise[313]. Ces résultats peuvent être discutés à l'audience, voire contredits, conduisant alors le juge à écarter la contradiction par une décision motivée ou à diligenter un complément d'expertise ou une nouvelle expertise[314]. Même si cette procédure permet de contester la fiabilité des algorithmes utilisés, aucune disposition du code de procédure pénale ne prévoit la communication des informations relatives aux algorithmes utilisés.

2.2 Les autres systèmes de production d'indices basés sur l'IA

Les enquêteurs ont à leur disposition d'autres applications basées sur l'intelligence artificielle, à différents degrés, qui peuvent produire des indices.

La comparaison vocale ou l'identification vocale en fait partie. L'institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), par exemple, s'appuie sur plusieurs outils, dont un logiciel développé en interne, Gendvox. À côté de l'approche classique de certaines applications, visant à identifier des signes phonétiques discriminants (défaut de prononciation, vocabulaire employé, harmoniques de la voix, fréquence de la respiration, rythme de la parole …), Gendvox adopte une approche automatique permettant « l'extraction des descripteurs d'un locuteur, reflétant les caractéristiques

[309] Cass. crim. 25 octobre 2022, n° 21-81.466.
[310] V. Assemblée Nationale, Rapport sur le projet de loi d'orientation et de programmation du ministère de l'Intérieur (4 novembre 2022), n° 436, commentaire de l'article 12.
[311] Conseil d'État, 26 avril 2022, *op. cit*. (n 302).
[312] C. proc. pén. art. 60 in fine et 77-1.
[313] Par exemple une nouvelle analyse par reconnaissance faciale pour démontrer que l'identification est erronée, ou une analyse de la fiabilité des algorithmes utilisés, C. proc. pén. art. 156.
[314] C. proc. pén. art. 169-1.

physiques de son conduit vocal, et de leur modélisation statistique »[315]. Des méthodes d'évaluation de la force probante de ces analyses vocales sont mises en œuvre afin de rendre compte de leur fiabilité, en conformité avec l'état de l'art[316].

S'agissant de données biométriques, et donc sensibles, le cadre juridique est dans l'ensemble le même que celui de la reconnaissance faciale. S'appliquent la loi dite « Informatique et libertés » ainsi que le régime des constatations du Code de procédure pénale. Il n'existe pas de fichier des empreintes vocales, ce qui écarte la question des personnes habilitées à le consulter.

La Gendarmerie Nationale a également développé une autre application, Gendexif, permettant d'extraire et d'exploiter les métadonnées et notamment les données de géolocalisation des photographies ou vidéos prises au moyen de smartphones, tablettes ou appareils photo. Le logiciel permet de reconstituer la chronologie des données, de les situer précisément sur une carte, et donc de reconstituer le déplacement d'un individu en traitant une grande masse d'informations contenues dans les métadonnées. L'utilisation de ce logiciel dans le cadre d'une enquête est également régi par le droit commun de la procédure pénale et de la protection des données personnelles.

2.3 La réception par le juge des preuves produites par l'IA

Des chercheurs se sont récemment intéressés à l'influence d'une preuve algorithmique sur la décision d'un juge, en menant une étude de terrain durant trois ans[317], aussi bien en matière civile qu'en matière pénale. Leurs conclusions font apparaître que la preuve algorithmique a une influence très marginale sur les décisions de culpabilité en matière pénale.

Cette étude peut être nuancée par des interrogations concernant plus particulièrement la reconnaissance faciale. Cette technologie, utilisée de manière subsidiaire pour lever un doute sur l'identité ou l'identification d'une personne, ne fournit en principe qu'une probabilité de correspondance. Cette probabilité n'est donc qu'un indice, la preuve de l'identité ou de l'identification du mis en cause devant découler de l'intime conviction du juge, fondée sur d'autres éléments complémentaires. La loi dite « informatique et libertés » n'interdit pas en effet de prendre une décision sur la culpabilité d'une personne sur le fondement d'un traitement algorithmique. Elle interdit seulement que ce

[315] Institut de Recherche Criminelle de la Gendarmerie Nationale, Les voix des saigneurs sont-elles impénétrables ?, https://www.gendarmerie.interieur.gouv.fr/pjgn/ircgn/l-expertise-decodee/analyse-numerique/les-voix-des-saigneurs-sont-elles-impenetrables

[316] L'article précité comporte une bibliographie.

[317] E. Vergès, G. Vial, « Dossier : L'impact des algorithmes sur la décision de justice » (2022), *Recueil Dalloz*, 1919.

traitement, comme la reconnaissance faciale, soit le seul fondement : le résultat probabiliste de la reconnaissance faciale doit donc bien être soutenu par d'autres éléments[318].

Cette disposition ne semble pourtant pas suffire à relativiser l'influence que peut avoir le traitement algorithmique sur l'intime conviction du juge et la force probante qui peut être accordée à la reconnaissance faciale[319]. L'utilisation de ces probabilités rend incertaine la frontière entre preuve et indice et peut entraîner un effet négatif sur la présomption d'innocence et la charge de la preuve, remettant en cause l'adage in dubio pro reo.

Dans une décision de justice, pour le moment isolée, et rendue en droit des étrangers, la charge de la preuve a été inversée par l'usage de la probabilité issue de la reconnaissance faciale de la personne mise en cause. La Cour d'appel énonce en effet : « Elle s'est dit mineure lors de son interpellation, les policiers ont procédé a une identification faciale de laquelle il est résulté qu'elle présente une similitude a 68% avec une jeune femme connue sous l'identité de Mme [O] [N], se disant née le [Date naissance 1] 2003 a [Localité 7], de nationalité serbe. L'intéressée soutient que ce n'est pas elle mais, si elle maintient être mineure, elle n'apporte aucun élément en faveur de sa minorité, ni d'élément probant susceptible de contrer ceux sur sa majorité établis lors de la procédure, elle refuse de se soumettre aux prises de photographies et d'empreintes qui pourraient permettre son identification, une évaluation de son âge ne peut être réalisée dans le temps de la garde a vue»[320]. L'arrêt précise par ailleurs que les éléments en faveur de la majorité de l'intéressée résultent seulement du fait qu'elle « a refusé que l'on prenne sa photographie et ses empreintes, ce qui peut laisser supposer qu'elle est connue comme majeure ».

Cette décision interroge quant à la force probante de la reconnaissance faciale. La présomption d'innocence est grandement fragilisée par un renversement de la charge de la preuve, la preuve algorithmique faisant foi jusqu'à preuve du contraire dans cette affaire, malgré un taux de correspondance peu élevé. Dans le même temps, le juge conserve sa liberté d'appréciation et forge son intime conviction en situation d'incertitude, alors que la probabilité aurait pu produire le doute profitable à la personne mise en cause. La preuve algorithmique joue ici un rôle contradictoire, qui nuit aux droits fondamentaux de la personne mise en cause.

---

[318] Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, *op. cit.* (n 187) art. 95. Elle interdit en revanche de prendre une décision de justice impliquant une appréciation sur le comportement d'une personne sur le fondement d'un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

[319] Gindre E., « Reconnaissance faciale : un mode de preuve 2.0 ? » (mars 2023), *AJ Pénal*, 123.

[320] Cour d'appel, Rouen, Chambre des étrangers, 18 octobre 2022, n° 22/03388.

3 Preuves évaluées par les systèmes basés sur l'IA

Les autorités de police judiciaire, et notamment la Gendarmerie, acteur de l'innovation en la matière[321], considèrent l'IA comme une chance d'améliorer l'efficacité et la rapidité des enquêtes. L'IA permet de plus en plus l'automatisation de la recherche d'indices, la mise en évidence de liens ou d'incohérences ou encore la détection des faux dans le cadre de la cybercriminalité. Face à une criminalité utilisant des outils basés sur l'IA, et « au regard des milliards de données constituant un dossier pénal ce jour, il n'apparaîtrait pas responsable de se passer de l'IA dans la recherche de la vérité judiciaire. »[322].

Pour autant, plusieurs questions restent posées, on l'a vu, quant à la fiabilité des outils utilisés, au respect des droits procéduraux dans l'utilisation de ces outils, à la force probante attachée à leurs résultats et son influence sur l'intime conviction du juge.

Là encore, il semble que la science, et plus particulièrement les mathématiques, peut-être d'ailleurs avec l'aide de l'intelligence artificielle, permettrait de chiffrer la force probante des indices et ainsi de déplacer le respect du principe du contradictoire en amont, dès la phase des expertises criminalistiques. C'est en tout cas l'idée développée par la Gendarmerie Nationale qui s'appuie sur une approche bayésienne qui « consiste à évaluer la force probante des résultats observés, à travers au moins deux hypothèses de travail alternatives explicites : celle à charge, et celle de la défense »[323]. Cette méthode permet de calculer le rapport entre la probabilité d'observer ces résultats, lorsque l'hypothèse à charge est supposée vraie et la probabilité d'observer ces résultats lorsque l'hypothèse à décharge est supposée vraie. Elle s'applique aussi bien aux traces partielles (traces d'ADN par exemple), aux traces latentes (traces présentes chez le suspect mais non retrouvées sur la trace relevée sur la scène de crime), mais aussi aux faisceaux d'indices grâce aux réseaux bayésiens.

Cette méthode est décrite comme un outil d'aide à la décision judiciaire, limitant les risques d'erreurs judiciaires, et permettant d'adapter les mesures coercitives à la force probante des indices. Elle reste cependant limitée à l'interprétation des indices par les experts et n'a pas pour objet de se substituer aux enquêteurs et aux juges dans l'évaluation des hypothèses et l'appréciation des éléments de preuve.

---

321 V. Le site du Pôle judiciaire de la Gendarmerie Nationale et notamment ses pages consacrées à l'innovation, https://www.gendarmerie.interieur.gouv.fr/pjgn/innovation

322 Pôle judiciaire de la Gendarmerie Nationale, L'impact de l'intelligence artificielle dans la conduite de l'enquête judiciaire, https://www.gendarmerie.interieur.gouv.fr/pjgn/innovation/les-publications-scientifiques/intelligence-artificielle/l-impact-de-l-intelligence-artificielle-dans-la-conduite-de-l-enquete-judiciaire#:~:text=L%27intelligence%20artificielle%20arrive%20pour,v%C3%A9rit%C3%A9%20expos%C3%A9e%20au%20proc%C3%A8s%20p%C3%A9nal

323 IRCGN, Élémentaire mon cher…Bayes !, https://www.gendarmerie.interieur.gouv.fr/pjgn/ircgn/l-expertise-decodee/de-la-trace-a-l-indice/elementaire-mon-cher-bayes .

En dehors de cet exemple, il ne semble pas exister en France d'outil basé sur l'IA assistant le juge pénal dans l'évaluation des preuves qui lui sont soumises. Les oppositions sont d'ailleurs les mêmes qu'en matière de justice prédictive[324].

[324] V. Ce rapport, deuxième partie : la justice prédictive.