



LES INSTITUTIONS PUBLIQUES : DE L'ALGORITHME PROTECTEUR À L'ALGORITHME CRIMINEL

Rajae ZINE EL ABIDINE

Docteure-chercheuse en Droit privé

Spécialisée en droit pénal et sciences criminelles

Doctorante à l'Université Paris 2 Panthéon-Assas, France

Membre associée au Laboratoire d'Études et de Recherches en Droit privé, l'Ingénierie juridique et le Développement durable

Université Sidi Mohamed Ben Abdellah, Fès, Maroc

Résumé: Entré dans le domaine du grand public, Internet et les technologies de l'information revêtent désormais une importance majeure dans le quotidien des populations. Selon l'Union internationale des télécommunications, le nombre d'internautes dans le monde a atteint les 6 milliards en 2024, soit environ 227 millions de nouveaux utilisateurs de plus par rapport à l'année précédente. Parallèlement, une montée en puissance de la criminalité informatique fragilise les structures institutionnelles en causant des disparités dans la mise en œuvre de la protection des données à caractère personnel au sein des institutions publiques, qu'elles soient politiques, sociales ou juridiques. En France, malgré un cadre juridique avancé encadrant les algorithmes publics, l'expérimentation controversée d'outils prédictifs et de surveillance révèle des limites préoccupantes. Au Maroc, où la cybercriminalité est devenue une affaire d'état, la Direction Générale de la Sûreté Nationale du Maroc a lancé une nouvelle plate-forme nommée « E-Blagh » afin de lutter efficacement contre le phénomène grandissant de la cybercriminalité. Cet article se propose d'approfondir certains de ces aspects en se focalisant sur le glissement insidieux de l'algorithme protecteur vers l'algorithme criminel. En examinant les principaux risques et dérives liés à ces systèmes, il démontre la nécessité impérieuse d'un encadrement juridique rigoureux. Comme l'affirmait Stephen Hawking, une intelligence artificielle puissante sera « soit la meilleure chose, soit la pire chose jamais arrivée à l'humanité ».

Mots Clés: Gouvernance numérique, Données personnelles, Cybersécurité, Protection des données.

Digital Object Identifier (DOI): <https://doi.org/10.5281/zenodo.15773185>

1 Introduction

« Ce n'est pas à la personne humaine d'être l'esclave de la technique, c'est à elle de servir l'homme »¹

Alors que la criminalité « classique » paraît triompher, la cybercriminalité a littéralement explosé ces dernières années. Elle prolifère dans les sociétés contemporaines et remplace progressivement les formes traditionnelles de délinquance. Les systèmes d'information constituent un vecteur privilégié offrant de grandes possibilités aux personnes malveillantes, pour s'en prendre aux internautes les plus vulnérables. Les victimes potentielles ne se limitent pas aux enfants ou les personnes âgées mais aussi les administrations et les entreprises privées. Aujourd'hui on assiste à un véritable transfert des activités délictueuses du monde analogique vers un essor de la cybercriminalité.

À l'heure où le Maroc compte près de 35,3 millions d'internautes, soit 92,2% de sa population, l'enjeu de protection numérique devient une priorité absolue pour l'État et ses administrations². Toutes ces activités reposent sur le traitement et la transmission de données numériques et peuvent dès lors être fragilisées par des attaques informatiques.

La cyberattaque survenue en avril 2025 contre la Caisse Nationale de Sécurité Sociale en constitue une illustration significative. Des pirates ont réussi à infiltrer les systèmes informatiques de cet établissement stratégique, exfiltrant potentiellement des données personnelles sensibles de millions de citoyens. Suite à ce piratage, le Maroc a plongé dans un profond désarroi, tant par l'ampleur de l'intrusion que par la sensibilité des données compromises. « Bienvenue en enfer où tout le monde sait combien gagne son voisin ! »³, cette formule résume, à elle seule, l'état d'angoisse et de choc suscité par cette atteinte.

Cet incident révèle de manière saillante les failles structurelles du système de sécurité nationale, plus encore, les vulnérabilités du cadre juridique marocain en matière de cybercriminalité. Il soulève la question de l'effectivité des dispositifs existants de réponse et de protection.

Parallèlement à ces défis, les nouvelles technologies et l'intelligence artificielle sont progressivement déployées dans le cadre des missions de service public, tant qu'en France qu'au Maroc. Des outils algorithmiques, tels que la police prédictive, la vidéosurveillance automatisée ou encore l'aide à la décision judiciaire⁴, promettant sécurité⁵, anticipation et efficacité accrue. Cependant, cette confiance placée dans les algorithmes ne doit pas

¹ R. SAVATIER, Les métamorphoses économiques et sociales du droit privé d'aujourd'hui, 1959, Dalloz.

²<https://nerolinkmedia.com/blog/le-paysage-digital-au-maroc/#:~:text=Population%20connect%C3%A9e%3A%2035%2C3%20millions,%C3%A0%20143%25%20de%20la%20population> (consulté le 12 juin 2025 à 13h36).

³https://www.lemonde.fr/afrique/article/2025/04/14/le-maroc-sous-le-choc-apres-le-piratage-de-la-securite-sociale-bienvenue-en-enfer-ou-tout-le-monde-sait-combien-gagne-son-voisin_6595892_3212.html (consulté le 12 juin 2025 à 15h54).

⁴ S. LEBRETON-DERRIEN & R. RAHER (dir), Algorithmes, Justice Prédictive et Juges-Robots, Enrick-B-Éditions, Paris, 2023.

⁵ Rapport de la Commission informatique et libertés, dit Rapport Tricot, La documentation française, 1975, p. 15 : « L'ordinateur, dit-on, ne se trompe pas. C'est une réputation qui a de quoi inquiéter. »

masquer leur potentiel de dérives inquiétantes : profilage discriminatoire, surveillance généralisée, décisions arbitraires ou injustes,⁶ autant de menaces sérieuses pour les libertés individuelles et l'État de droit⁷.

À partir de là, se posent des questions fondamentales entre l'algorithme protecteur et l'algorithme criminel : quelles limites le droit pénal peut-il imposer à ces nouvelles technologies ? Comment les données personnelles des citoyens sont-elles protégées face à ces risques ? Qui répond juridiquement lorsque l'algorithme, conçu initialement pour protéger, devient un instrument de violation des droits fondamentaux ?

Au-delà du émoi médiatique et institutionnel, cet article se propose ainsi d'analyser ces problématiques dans une perspective comparée entre la France et le Maroc, en explorant à la fois les promesses et les risques liées à l'intégration des algorithmes au sein des institutions publiques, tout en identifiant les garanties nécessaires à un usage respectueux et satisfaisant des libertés individuelles et collectives.

2 L'algorithme au service de la protection et de la sécurité publique

Un algorithme est une suite finie et non ambiguë d'opérations ou d'instructions permettant de résoudre une classe de problèmes. Il existe plusieurs définitions⁸ plus au moins ésotériques de ce qu'est un algorithme. Issu historiquement du mathématicien persan Al-Khawarizmi, le terme « algorithme » est devenu courant dès la Renaissance⁹.

Dans l'administration publique, l'usage des algorithmes vise à optimiser et automatiser la prise de décision administrative. Ils se retrouvent dans des domaines très variés, allant du calcul automatisé des impôts ou de la répartition des aides sociales, à la gestion administrative de processus complexes comme l'admission universitaire ou la mobilité des agents publics. Ces algorithmes doivent impérativement respecter les grands principes du service public, notamment l'égalité, la continuité et la mutabilité. Néanmoins, leur complexité technique et leur manque potentiel de transparence peuvent constituer une source d'inquiétude, ce qui explique que le droit français impose des exigences précises en matière de transparence¹⁰ algorithmique, garantissant ainsi aux citoyens la possibilité de comprendre les processus décisionnels automatisés qui les affectent directement, et comme le rappelle la Commission nationale informatique et liberté (Cnil), « dans un État de droit, aucune considération ne saurait justifier une surveillance généralisée et indifférenciée de la population, pas plus que la « mécanisation » de cette surveillance par une aspiration automatique des données »¹¹.

⁶ T. MÉNISSIER, « Une intelligence artificielle pour la justice ? Institutions sociotechniques et autorité des machines », Dalloz IP/IT, n°1, 2022. 17.

⁷ N. CARR, Remplacer l'humain. Critique de l'automatisation sur les personnes de la société, p. 53 et s. L'échappée, coll. Pour en finir avec, 2017.

⁸ D. KNUTH, The Art of Computer Programming, Addison-Wesley, Boston, 1969, T. 4; G. BOOLOS, R. JEFFEREY, Computability and Logic, CUP, Cambridge, 1974.

⁹ Fr. RABELAIS, Les horribles et espoventables faictz et prouesses du très renommé Pantagruel(...), éd., 1533, Lyon, Chap. X, p. 73 : « Ces enfants deviendront grands en Algorisme ».

¹⁰ J.BODIN, Les six livres de la République, Jacques du Puys, Paris, 1576, 759 p ; Déclaration des Droits de l'Homme et du Citoyen de 1789 (Art. 14 & Art 15) ; Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF, 7 janvier 1978 ; Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ CE, JOUE, 4 mai 2016 ; Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, JORF, 13 décembre 2018 ; Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF, 30 mai 2019 ; Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, JORF, 18 juillet 1978 ; Loi n° 79-18 du 3 janvier 1979 sur les archives, JORF, 5 janvier 1979 ; Loi n° 79-587 du 11 juillet 1979 relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public, JORF, 12 juillet 1979 ; Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF, 8 octobre 2016.

¹¹ « Espionnage de la NSA, une ligne rouge a été franchie selon la Cnil », Le Monde, 24 octobre 2013.

2.1. Des outils algorithmiques pour anticiper et agir : Le cas de la France

Ces dynamiques s'observent avec acuité dans les domaines régaliens de la sécurité et de la justice¹². En matière de sécurité, la France utilise les nouvelles technologies au profit de la prévention des risques du quotidien, qu'il s'agisse de prévenir les incendies et les inondations ou de sauver la vie de victimes d'incidents cardiaques¹³.

Ainsi, les forces de l'ordre et les institutions judiciaires recourent depuis plusieurs années aux outils algorithmiques afin de renforcer l'efficacité tant de la prévention que de la répression des infractions. La police prédictive, par exemple, utilise des algorithmes analysant des données criminelles passées pour identifier les lieux et moments susceptibles de connaître une activité délictueuse. Plusieurs systèmes ont été expérimentés, tels que le *Risk Terrain Modelling* (RTM) par la préfecture de police de Paris, ou encore *PredVol* et *Paved*¹⁴, respectivement destinés à prédire vols de véhicules et cambriolages, même si ces derniers n'ont pas dépassé la phase expérimentale.

À l'échelle locale, la ville de Marseille a innové avec le dispositif M-Pulse pour optimiser l'action de sa police municipale. Parallèlement, la France a autorisé à titre expérimental, jusqu'en mars 2025, l'usage d'algorithmes de vidéosurveillance dits de « caméras augmentées » durant les Jeux Olympiques afin de détecter les menaces sécuritaires, avec un encadrement strict approuvé par le Conseil Constitutionnel¹⁵.

Dans le domaine judiciaire, les algorithmes se comportent comme de véritables sociologues de la justice. Ils apprennent à identifier les comportements des juges. Ils s'imprègnent de leurs pratiques et leurs routines et ils les répètent¹⁶. Les algorithmes ont trouvé leur place à travers le concept de « justice prédictive », exploitant de grandes masses de jurisprudence pour prévoir les issues probables de litiges futurs. Cette méthode qui se base principalement sur le traitement automatique du langage naturel (TAL)¹⁷, ou encore (NLP) pour *Natural Language Processing*, repose sur la capacité des machines à saisir des régularités statistiques et des corrélations entre certains observables, comme les mots ou les expressions utilisés dans une décision judiciaire, et l'issue probable du jugement¹⁸. Toutefois, les systèmes actuels d'intelligence artificielle ne parviennent pas encore à égaler les performances de l'intelligence humaine dans cette tâche prédictive. En effet, lors d'une expérience menée sur 100 décisions judiciaires, les prédictions humaines ont atteint un remarquable taux de précision allant jusqu'à 96%, alors que les modèles de TAL sont restés sensiblement en retrait, peinant à identifier correctement les indices pertinents au sein des textes¹⁹. Cette analyse approfondie des prescriptions erronées confirme qu'une part marginale des décisions de justice ne contient pas de motifs suffisamment clairs pour effectuer une prédiction fiable. L'intelligence naturelle raisonne alors de façon classique pour stabiliser cette ambiguïté. Elle est influencée par des biais individuels qui orientent l'esprit vers une solution plutôt qu'une autre. L'analyse nous apprend également qu'il n'est pas raisonnable d'attendre des outils d'intelligence artificielle un taux de prédiction de 100 %. Un taux d'erreur marginal semble irréductible et il dépend ici d'un problème de qualité des données. Certaines décisions ne peuvent être prédites car les situations sont complexes, ce qui conduit les juges à adopter des motivations ambivalentes ou contradictoires²⁰. Ainsi, même si les algorithmes progressent, l'expérience montre clairement que l'intelligence naturelle conserve actuellement un avantage décisif dans l'interprétation fine et nuancée nécessaire à la prédiction judiciaire.

¹² En novembre 2024, le nombre d'algorithmes répertoriés s'élèvent à 72. <https://odap.fr/inventaire/synthese/>

¹³ X. LEONETTI, *Smartsécurité et cyberjustice*, PUF, 2021, p. 12.

¹⁴ L'outil PAVED a été créé par la gendarmerie : <https://www.franceinter.fr/emissions/grand-angle/grand-angle-02-octobre-2018>.

¹⁵ M. BARTOLUCCI, « L'expérimentation de la vidéosurveillance algorithmique », Dr. adm. 2023, étude 7 ; E. SERUGA-CAU, « L'utilisation de 'caméras augmentées' dans l'espace public ou comment innover sans (trop) surveiller », Comm. Com. Electr. 2023, étude 14 ; M.-A. GRANGER, « Surveiller et contrôler » : AJDA 2023, p. 2222. - C. CRICHTON, « Vidéosurveillance intelligente aux JO : validation sous réserve par le Conseil constitutionnel » : Dalloz actu, 12 juillet 2024

¹⁶ E. VERGÈS, C. BAZZOLI, « La modélisation des décisions de justice à partir des faits : Comment l'IA imite les raisonnements des juges à partir d'une grille de critères », La Semaine Juridique-Édition Générale-Supplément au n°6-10 février 2025, n°6004.

¹⁷ Le traitement automatique des langues naturelles comme outil de prédiction des jugements : JCP G 2025, doctr. 6001 ; O. VAUDAUX, C. BAZZOLI, M. COAVOUX, G. VIAL et E. VERGÈS, *Pretrained Language Models v. Court Ruling Predictions in Proceedings of the Natural Legal Language Processing Workshop 2023* : Association for Computational Linguistics, déc. 2023, Singapour, p. 38-43.

¹⁸ O. VAUDAUX, C. BAZZOLI, M. COAVOUX, G. VIAL et E. VERGÈS, « Intelligence artificielle contre intelligence humaine : comment l'esprit humain prédit les décisions des juges », La Semaine Juridique-Édition Générale-Supplément au n°6-10 février 2025, n°6002.

¹⁹ *Ibid.*,

²⁰ *Ibid.*,

En résumé, l'algorithme apparaît progressivement comme un véritable instrument protecteur au sein de l'action publique française, visant à garantir à la fois la sécurité collective par une prévention accrue des infractions et l'efficacité judiciaire par une meilleure harmonisation et célérité dans le traitement des dossiers, tout en posant de nouveaux défis de transparence et de respect des libertés fondamentales.

2.2 L'émergence de l'IA sécuritaire et judiciaire : Le cas du Maroc

Au Maroc, l'adoption des algorithmes par les institutions publiques s'inscrit dans un contexte de modernisation rapide et d'ouverture aux technologies. Si le phénomène est plus récent, on observe un essor considérable de l'intelligence artificielle dans les services de l'État ces dernières années. Une étude de Policy Center place cette technologie au cœur de l'encadrement réglementaire et stratégique du pays. En matière de sécurité publique, les pouvoirs publics marocains investissent dans des solutions de vidéosurveillance intelligente. Des grandes villes comme Casablanca, Marrakech, Rabat ou Fès sont désormais équipées de caméras urbaines connectées gérant la circulation et la surveillance des espaces publics. Ces dispositifs intègrent souvent des algorithmes de reconnaissance d'images : lecture automatique des plaques d'immatriculation par radar, détection de comportements suspects... Dans la perspective de la Coupe d'Afrique des Nations 2025 ou la co-organisation du Mondial 2030, le Maroc a franchi le pas de la reconnaissance faciale dans l'espace public. Ainsi, à l'instar de nombreux pays européens, Rabat et Agadir déploient actuellement des systèmes de caméras de nouvelle génération incluant la reconnaissance des visages et l'analyse comportementale en temps réel. Ces caméras dites intelligentes sont reliées à des centres de commandement, capables d'identifier des personnes dans la foule ou de signaler des attroupements inhabituels, le tout avant fin 2025²¹. De même un dispositif de reconnaissance faciale a été mis en place à l'aéroport international de Rabat-Salé pour renforcer les contrôles d'identité des voyageurs. L'Intelligence Artificielle est ainsi déployée comme un outil de surveillance avancée, visant à prévenir le terrorisme, la délinquance urbaine et à améliorer la réactivité des forces de l'ordre.

Le domaine policier et criminel au Maroc commence également à explorer des usages similaires à la police prédictive. Des responsables de la sécurité marocaine soulignent l'intérêt d'utiliser l'IA pour analyser d'importants volumes de données criminelles, repérer des schémas cachés et anticiper les zones à risque de crime. Cette approche de *predictive policing* émergente est encouragée par l'accès croissant à des données numériques sur la criminalité et par la volonté des autorités de disposer d'outils proactifs de lutte contre la délinquance²². Ainsi, selon M. Loubbardi commissaire divisionnaire et ex chef du service ADN du Laboratoire de police scientifique et de différents services de la police judiciaire de la DGSN²³, nous pouvons mettre à la disposition des services de police judiciaire marocains des outils d'intelligence artificielle pour identifier des séries de cambriolages ou de délits dans certains quartiers et adapter en conséquence leurs patrouilles. De plus, en matière criminelle, la recherche de suspects, ou les personnes disparues peut se faire avec des applications de l'IA en croisant les différentes bases de données ou en utilisant la reconnaissance vocale pour retranscrire automatiquement des interrogatoires et accélérer les procédures. La police scientifique peut bénéficier également d'avancées algorithmiques : analyse intelligente des vidéos de scène de crime, tri automatisé des indices numériques... Dans la même optique, l'IA permet en outre le développement d'outils de profilage criminel et de prédiction de la récidive, à l'image du logiciel COMPAS utilisé aux États-Unis, afin d'évaluer la dangerosité d'un individu et d'orienter les décisions de mise en liberté ou de suivi post-carcéral²⁴. Bien que de tels systèmes ne soient pas encore officiellement instaurés au Maroc, les experts prédisent leur arrivée prochaine dans le paysage judiciaire du pays.

Cette dynamique s'accompagne d'une volonté affichée de moderniser l'administration de la justice marocaine grâce au numérique pour transformer la gestion des litiges. Les autorités envisagent notamment d'intégrer l'intelligence artificielle dans différentes phases du contentieux à l'instar des systèmes ODR pour la résolution des petits litiges en ligne.

Néanmoins, au Maroc comme ailleurs, ces promesses technologiques vont de pair avec des défis. Les bénéfices potentiels ne doivent pas tout de même occulter que chaque algorithme déployé par l'État peut aussi engendrer des effets pervers.

3 Les dérives potentielles : de l'algorithme biaisé à l'atteinte aux droits fondamentaux

Les progrès réalisés par l'intelligence artificielle, mais aussi les craintes qu'elle a engendrées, ont fait naître une volonté politique de la réglementer dans la plupart des pays du monde. D'un côté, les gouvernements souhaitent

²¹ Ministère de l'intérieur – Direction Générale de la Sûreté Nationale, Mars 2025.

²² <https://www.intelligenceartificiellemaroc.com>

²³ <https://www.lopinion.ma/Intelligence-artificielle>

²⁴ Ibid.,

généralement encourager le développement des outils d'intelligence artificielle sur leur territoire. Mais d'un autre côté, elle soulève aussi des interrogations auxquelles les législateurs souhaitent aussi apporter des réponses.

3.1 Biais discriminatoires et profilage injuste

L'un des dangers majeurs des algorithmes publics est leur partialité potentielle, reflétant ou aggravant des biais déjà présents dans la société. Un algorithme n'est jamais neutre : il apprend à partir de données historiques, qui peuvent être entachées de discriminations structurelles, ou il applique des critères conçus par des humains avec leurs préjugés. Par conséquent, lorsque la police ou l'administration utilise ces outils, il existe un risque élevé de discrimination automatisée visant certains groupes de population.

Cette problématique est renforcée lorsque les traitements algorithmiques changent de finalité en cours d'exploitation. Pour reprendre l'exemple du Professeur Debet²⁵, des fichiers clients peuvent être utilisés par une banque pour faire du *scoring*. Or, dès lors que le fichier préexistant est utilisé pour un autre traitement constitué par un algorithme décisionnel, cette seconde finalité doit être évaluée à l'aune de la première. L'analyse d'une base de données par un algorithme, même si elle n'est pas initialement dans le but de prendre une décision, peut engendrer une nouvelle finalité. Dès lors c'est parfois le principe même de détermination a priori des finalités qui peut être questionné²⁶.

Les expériences de police prédictive en France en fournissent une illustration significative. Une enquête menée par La Quadrature du Net²⁷, affirme que plusieurs des logiciels prédictifs intègrent des variables sociodémographiques fortement corrélées à la criminalité, sans transparence ni justification causale. Prenons l'exemple de l'algorithme PAVED de la gendarmerie. Cet outil s'appuie sur une quinzaine de variables telles que le taux d'illettrisme local. De telles variables aboutissent presque mécaniquement à cibler les zones défavorisées et les minorités ethniques, déjà répertoriées dans les fichiers de police. Techniquement, le profilage est une technique d'analyse statistique en deux étapes : une étape de génération de profil et une étape d'application du profil. Ce profil est généré à partir d'informations issues de la personne elle-même, mais aussi d'autres personnes. Les données collectées proviennent d'une pluralité de sources : questionnaires remplis par la personne, données publiques, données confidentielles, *data brokers*²⁸. Ainsi, cette technique à double tranchant, en voulant identifier les lieux « à risque », assigne en réalité un score de dangerosité à des populations précarisées, renforçant le contrôle policier sur celles-ci plutôt que sur d'autres. Ces biais d'origine idéologique ou statistique se traduisent alors par une discrimination de fait : surcontrôle des mêmes communautés, suspicion généralisée à l'égard des plus pauvres... Face à ces risques, l'article 11 de la directive du 27 avril 2016 sur les décisions automatisées utilise un critère complémentaire à celui prévu par le RGPD exigeant explicitement que les effets juridiques du profilage soient défavorables à la personne concernée : « Toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative »²⁹. Cette disposition juridique souligne l'importance cruciale d'un cadre réglementaire clair et rigoureux pour prévenir les dérives discriminatoires liées aux algorithmes publics.

²⁵ A. DEBET, « Intelligence artificielle et données à caractère personnel », in A. Bensamoun et G. Loiseau (dir.), *Droit de l'intelligence artificielle*, p. 271, n° 461 ; C. CASTETS-RENARD, *Droit du marché unique numérique et intelligence artificielle*, p. 243, n° 301 : « la collecte massive des données de toute nature, y compris des données personnelles, consistant à agréger un maximum d'informations sans même nécessairement savoir à l'avance à quoi elles serviront peut porter atteinte aux principes de finalité, limitation, nécessité et minimisation du traitement des données personnelles » ; B. DELMAS-LINEL & G. DUMAS, « L'impact du RGPD sur les innovations en matière d'IA », in F. G'SELL (dir.), *Le Big Data et le droit*, op. cit., p. 213 : « L'évolution des technologies permet la création de nouvelles fonctionnalités ou de nouvelles idées qui n'avaient pas nécessairement été envisagées au départ. »

²⁶ Y. POULLET, *La vie privée à l'heure de la société du numérique*, Larcier, 2019, p. 117, n° 21 : « cette référence unique à l'examen d'une finalité prédéfinie se heurte, nous semble-t-il, à la spécificité de nombre de systèmes d'intelligence artificielle (...) ainsi, il peut s'avérer qu'à l'occasion de cette recherche de corrélations, il apparaisse que des éléments jusqu'ici jamais corrélés deviennent signifiants et engendrent dès lors une nouvelle finalité. (...) Le RGPD, dès lors, se trouve alors en porte-à-faux avec la réalité de certains traitements utilisant l'intelligence artificielle actuellement, et bien plus encore dans le futur ».

²⁷ <https://www.laquadrature.net>

²⁸ L. BYGRAVE, *Data Protection Law: Approaching its Rationale, Logic and Limits*, p. 301 : « *What is new – and which deserves the attention of this book – is the increasingly extensive, systematic use by organisations of relatively formalised and sophisticated profiling practices for a variety of control purposes.* »

²⁹ Dir. n° (UE) 2016/680 du Parlement européen et du Conseil, 27 avr. 2016, relative à la protection des personnes physiques à l'égard du traitement des 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, art. 11 (1).

Le champ de la justice prédictive n'est pas épargné non plus. Certes, en France, la loi du 23 mars 2019 de programmation et de réforme pour la justice interdit les services en ligne de conciliation et de médiation fondés exclusivement sur des décisions automatisées³⁰, mais les outils d'aide à la décision peuvent malgré tout influencer les juges de façon subtile. Or, si l'algorithme a des biais, ses recommandations seront biaisées et, donc, dans certains cas, illicites³¹. Cela emporte des effets conséquents, et possiblement préjudiciables sur le destinataire de la décision. Les exemples de telles dérives sont innombrables : Aux États-Unis, l'algorithme COMPAS, utilisé par certains juges pour évaluer le risque de récidive, a montré un biais ethnique manifeste³² : plusieurs études ont montré qu'il surestimait nettement le risque de récidive des prévenus noirs par rapport aux blancs. En effet, seulement 20% des personnes que COMPAS avait désignées comme futurs auteurs de crimes violents sont effectivement passées à l'acte dans les deux ans, et les personnes noires étaient près de deux fois plus souvent classées à tort comme futurs criminels que les personnes blanches. Ce biais racial incorporé dans l'algorithme a conduit à des décisions judiciaires inéquitable, les accusés se voyant refuser des libérations conditionnelles ou des aménagements de peine en raison de scores de risques faussés. Au-delà du champ strictement judiciaire, ces risques s'observent également dans d'autres contextes de décisions administratives automatisées. En France, le traitement automatisé Louvois chargé de gérer les soldes militaires, a connu de graves dysfonctionnements qui ont privé des familles militaires de toute subsistance³³. De même, l'algorithme mis en place par le Gouvernement anglais pour attribuer aux lycéens leur note de *A Level*, équivalent anglais du baccalauréat, déployé puis retiré en raison de ses résultats erronés...³⁴

Plus largement encore, au-delà des seuls critères ethniques, de multiples autres caractéristiques sensibles peuvent être involontairement ou intentionnellement prises en compte par des algorithmes publics à savoir l'âge, le genre, l'état de santé, la situation d'handicap, l'orientation sexuelle, les opinions politiques... L'affaire Amnesty International et la Caisse Nationale des Allocations Familiales met en évidence une problématique de discrimination algorithmique. La CNAF utilise un algorithme destiné à repérer les risques de fraude parmi les allocataires, en utilisant des critères tels que les très faibles revenus, l'habitation dans des quartiers défavorisés, la situation de chômage ou encore l'état de famille monoparentale. Amnesty International critique ce système pour son caractère discriminatoire ciblant les populations précaires comme suspectes de fraude³⁵. Là encore, l'intention initiale de détecter des fraudes pour protéger le budget public se transforme en un outil de fichage³⁶ discriminatoire de masse, aux dépens de certaines catégories de citoyens, et pose un grave problème de justice sociale.

A ce propos, le Maroc devra se montrer particulièrement vigilant face aux risques liés à l'utilisation croissante des algorithmes publics. Les projets récents tels que le déploiement annoncé de la reconnaissance faciale à grande échelle soulèvent des inquiétudes légitimes concernant les biais discriminatoires, notamment ethniques ou raciaux, documentés ailleurs avec des taux d'erreurs élevés pour certains groupes. De même, l'adoption éventuelle par les autorités marocaines de systèmes de police prédictive pourrait reproduire et amplifier des biais socio-spatiaux en ciblant principalement les quartiers populaires et certaines régions défavorisées. Enfin, les algorithmes de notation du risque, qu'ils soient destinés à la détection de la fraude ou à l'évaluation sécuritaire, pourraient se révéler intrusifs et injustes envers les populations vulnérables, en l'absence de garanties solides de transparence, de contrôle et de recours effectifs. L'affaire récente concernant la CNSS illustre d'ailleurs clairement que ces algorithmes peuvent également jouer en défaveur de l'administration publique elle-même, engendrant des dysfonctionnements majeurs dans les prestations, des erreurs de calcul massives, voire des pertes financières significatives pour l'État.

³⁰ L. n° 2019-222, 23 mars 2019, de programmation 2018-2022 et de réforme pour la justice, art. 4.

³¹ F. G'SELL, « Les décisions algorithmiques », in F. G'SELL (dir.), *Le Big Data et le droit*, op. cit., p. 97, distinguant entre la fiabilité de l'algorithme et les discriminations algorithmiques.

³² F. G'SELL, *Justice numérique*, op. cit., p. 93 s. ; S. DESMOULIN-CANSELIER & D. LE MÉTAYER, *Décider avec les algorithmes, Quelle place pour l'Homme, quelle place pour le droit ?*, p. 89 s.

³³ J. MONIN, « Louvois, le logiciel qui a mis l'armée à terre », *France inter*, 2018 ; T. FABRE, « Ces bugs informatiques qui coûtent très cher à l'État », *Challenges*, 2013 ; *Cour des comptes*, Référé n° 68579 à Monsieur Jean-Yves Le Drian ministre de la Défense, 27 déc. 2013, en ligne : https://www.ccomptes.fr/sites/default/files/EzPublish/systeme_paye_Louvois_refere_68579.pdf.

³⁴ S. COUGHLAN, « Why did the A-level algorithm say no? », *BBC*, 2020.

³⁵ *Journal Officiel* du 29 octobre 2017- Numéro254- Commission nationale consultative des droits de l'homme : Avis relatif au suivi des recommandations du Comité des Nations unies sur les droits économiques, sociaux et culturels adressées à la France.

³⁶ G. HERZLICH, « Recherche des situations de détresse en Moselle : 'Fichage de la pauvreté' ou 'prévention sociale' », *Le Monde*, 26 nov. 1984.

3.2. Atteintes aux libertés et surveillance excessive

Le deuxième grand risque des algorithmes publics concerne l'atteinte aux droits et libertés fondamentaux, au premier rang desquels la vie privée, la liberté individuelle et le droit à un procès équitable. En effet, sur les enjeux des algorithmes décisionnels, tout d'abord, la doctrine a pu montrer que les algorithmes décisionnels pouvaient s'avérer problématiques au regard des droits et libertés fondamentaux des personnes humaines³⁷. Les traitements massifs de données à caractère personnel, condition essentielle du fonctionnement des algorithmes décisionnels, portent par exemple atteinte au droit au respect de la vie privée³⁸. Sans une régulation stricte, on peut basculer dans une logique d'État surveillant et de justice déshumanisée.

L'exemple le plus emblématique est la vidéosurveillance algorithmique. En France, son expérimentation pour les JO 2024 a suscité de vifs débats parmi les défenseurs des libertés publiques. Certes, la loi française a explicitement exclu la reconnaissance faciale de ce dispositif et a prévu des finalités précises et temporaires. Néanmoins, des voix se sont élevées pour souligner que ce type de technologie porte atteinte au droit à la vie privée et au droit de circuler anonymement, protégés constitutionnellement. Le Conseil Constitutionnel, dans sa décision, a d'ailleurs insisté pour que l'atteinte soit proportionnée et a annulé la volonté du gouvernement de prolonger l'usage de ces caméras intelligentes au-delà de l'événement exceptionnel des JO. Ce débat sur la proportionnalité et les libertés fondamentales se retrouve également dans le secteur privé, où les algorithmes sont désormais utilisés à des fins de prévention des vols à l'étalage³⁹. Dans ce cadre, des entreprises ont développé des algorithmes de détection de gestes suspects. Les algorithmes analysent les gestes des clients enregistrés par les caméras de vidéosurveillance et envoient des alertes aux salariés des magasins. Ces traitements ne peuvent avoir pour base légale que l'intérêt légitime du responsable du traitement, soit l'article 5-6 de la loi « informatique et libertés », équivalent à l'article 6 (1) (f) du RGPD. L'intérêt légitime poursuivi est la réduction et la prévention des vols, lié au maintien du chiffre d'affaires de l'entreprise. Dans cette perspective, il convient d'examiner la proportionnalité à travers les critères du contrôle de nécessité. Un tel algorithme est-il nécessaire à ces fins ? On imagine que l'algorithme de détection des gestes suspects facilite et augmente l'interception des vols à l'étalage. Il pourrait donc être efficace.

Quid alors du second critère, celui des moyens moins attentatoires aux libertés pour atteindre cet objectif ? Existe-t-il dans cette situation des moyens moins attentatoires aux libertés pour prévenir les vols à l'étalage ? L'analyse des gestes d'une personne, même si elle n'est pas identifiée dans le but de prévenir une infraction, est particulièrement dangereuse au regard de ses droits et libertés⁴⁰.

Cette problématique ne concerne pas que la France. Au Maroc, l'enjeu est tout aussi crucial. Le déploiement en cours de milliers de caméras intelligentes à Rabat, Agadir, Fès ou Casablanca, avec identification biométrique en temps réel, soulève la question du respect de la vie privée et de la protection des données personnelles des citoyens. La Commission nationale de protection des données marocaine reconnaît que la reconnaissance faciale est une technologie à double tranchant et que des normes doivent être définies pour encadrer son usage dans le respect de la vie privée.

Enfin, ces réflexions ne se limitent pas à la vidéosurveillance. Elles s'étendent à la justice prédictive où l'utilisation des algorithmes pour aider le corps magistral suscite de vifs débats. L'idée qui réapparaît dans beaucoup de travaux sur la justice prédictive, est de ne pas déshumaniser la justice et ne faire qu'accompagner la prise de décision : « Les moteurs d'intelligence artificielle peuvent de toute évidence jouer un rôle dans l'équité de la justice, à condition de se rappeler constamment que la modélisation mathématique constitue pour le magistrat une simple aide à la décision, et jamais la prise de décision en elle-même »⁴¹. Ainsi, et comme pour les données à caractère personnel, l'existence de ces catégories permet d'articuler un régime protecteur dans le cas où, comme on a pu

³⁷ G. CORNU, « La personne humaine, sujet de droit », in *L'art du droit en quête de sagesse*, PUF, 1998, p. 13 ; C. LÉVY, *La personne humaine en droit*, C. LABRUSSE-RIOU (dir.), thèse dactyl., Univ. Paris 1, 2000 ; S. MAY-FERRIÉ, *Le droit à l'autodétermination de la personne humaine : essai en faveur du renouvellement des pouvoirs de la personne sur son corps*, préf. G. Loiseau, IRJS éditions, 2018, p. 26, n° 42 s.

³⁸ F. G'SELL (dir.), *Le big data et le droit*, Dalloz, coll. Thèmes & commentaires, 2020 ; D. CARDON, *A quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, Éditions du Seuil et la République des Idées, 2015 ; C. ZOLYNSKI, « Big data : pour une éthique des données », *I2D*, vol. 52, n° 2, 2015, p. 25. On peut, en suivant le Professeur VITALIS, penser que la protection contre les algorithmes par l'intermédiaire de la vie privée vise moins « à valoriser les petits secrets de la personne qu'à protéger une sphère d'autonomie citoyenne, base et condition de tout régime démocratique » : A. VITALIS, *Le profilage des populations*, op. cit., p. 148.

³⁹ L. HUTTNER, *La décision de l'algorithme, Étude de droit privé sur les relations entre l'humain et la machine*, thèse, Paris 1 Panthéon Sorbonne, 2022, p. 338

⁴⁰ *Ibid.*,

⁴¹ A. GAYTÉ-PAPON DE LAMEIGNÉ, P. LEGRAND & J. LÉVY-VÉHEL « La modélisation de l'indemnisation du préjudice corporel. Un exemple de "justice quantitative" au service de l'équité » in F. G'SELL (dir.), *Le Big data et le droit*, op. cit., p. 51. V. aussi dans le même ouvrage la contribution de F. G'SELL, « Les décisions algorithmiques », op. cit., p. 87 s.

l'expliquer, « l'algorithme pourrait ne pas être cantonné à un simple outil d'aide à la décision et se voir investi d'un pouvoir décisionnel direct »⁴².

Face à ces dangers, il est impératif d'examiner comment le droit encadre et limite l'action des algorithmes publics.

4. Le cadre juridique et institutionnel applicable en France et au Maroc

Dans l'ordre juridique français, l'encadrement des traitements algorithmiques par les pouvoirs publics s'est progressivement structuré autour de plusieurs principes essentiels, à savoir la protection des données personnelles⁴³, la transparence et information de l'utilisateur⁴⁴, le rôle du juge et la jurisprudence et le règlement sur l'intelligence artificielle⁴⁵.

Le Maroc, de son côté, dispose d'une base juridique pour la protection des données personnes depuis plus d'une décennie, mais cette base montre ses limites à l'ère de l'intelligence artificielle. La pierre angulaire est la loi n°09-08 du février 2009 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Inspirée de la Directive 95/46/CE de l'UE, cette loi a mis en place des principes équivalents à ceux de la loi française de 1978 à savoir l'obligation de finalité, de proportionnalité, de sécurité des données, consentement éclairé des personnes, droits d'accès et de rectification... Elle a créé également la Commission Nationale de contrôle de la Protection des Données à caractère personnel (CNDP), autorité administrative indépendante chargée de veiller au respect de la loi, d'instruire les plaintes et de sanctionner les manquements. Cet organisme a le pouvoir d'édicter des autorisations ou interdictions de traitements, y compris pour les administrations, et de prononcer des sanctions pécuniaires, des peines pénales...

Cependant, de l'aveu même des praticiens et observateurs, cette loi n'avait pas anticipé les avancées foudroyantes de l'intelligence artificielle. En effet, la transparence exigée par la loi 09-08 se heurte à l'opacité technique des algorithmes d'apprentissage profond, rendant illusoire l'information complète des individus sur le traitement de leurs données.

Un point particulièrement délicat est celui de la responsabilité juridique en cas de dommage causé par un algorithme. Aujourd'hui, bien que l'intelligence artificielle ne soit pas dotée de personnalité juridique, son utilisation dans des contextes variés, notamment les assistants virtuels, les systèmes de recommandation... peut entraîner des conséquences juridiques complexes⁴⁶. Ainsi, un système algorithmique de vidéosurveillance identifie à tort une personne comme dangereuse et provoque son arrestation injustifiée, ou si un algorithme judiciaire commet une erreur de profilage ayant des conséquences graves, la question se pose : qui est le responsable ? Le droit pénal marocain actuel ne prévoit pas la responsabilité d'une intelligence artificielle elle-même, pas plus qu'en France d'ailleurs, où l'IA n'a pas de personnalité juridique. Dans ce contexte, la reconnaissance d'une personnalité

⁴² S. CHASSAGNARD-PINET, « Les usages des algorithmes en droit : prédire ou dire le droit ? », *Dalloz IP/IT*, n° 10, 2017, p. 495.

⁴³ Toute utilisation d'algorithmes manipulant des données individuelles est soumise au cadre général de la Loi Informatique et Libertés de 1978 et du Règlement général sur la protection des données (RGPD). En matière de sécurité et de justice, une directive européenne de 2016 (transposée en France) s'applique également pour les traitements de données à des fins de police et de justice.

⁴⁴ La France a innové en 2016 avec l'introduction dans le Code des relations entre le public et l'administration (CRPA) de l'obligation d'informer toute personne concernée par une décision individuelle prise sur le fondement d'un algorithme.

⁴⁵ Il convient de signaler qu'au niveau européen, un projet de Règlement sur l'Intelligence Artificielle (AI Act) est en cours d'adoption (en 2025) et devrait s'imposer à la France. Ce texte prévoit une classification des systèmes d'IA par niveaux de risque et pourrait interdire purement et simplement certaines utilisations jugées trop dangereuses pour les droits fondamentaux.

⁴⁶ C'est le cas révélateur du tragique accident mortel survenu en mars 2018 en Arizona, impliquant une voiture autonome Uber en phase de test. Le véhicule, opérant en mode autonome, n'a pas détecté une piétonne traversant la chaussée et l'a mortellement percutée. Un opérateur de sécurité se trouvait derrière le volant, sans toutefois intervenir avant la collision. Cet événement est tragiquement devenu le premier cas documenté de décès d'un piéton causé par une voiture autonome. L'enquête a révélé que le logiciel avait identifié la passante mais a choisi de l'ignorer, et que le freinage d'urgence automatique était désactivé. Le parquet local, confronté à ce cas inédit, a estimé « qu'il n'y avait pas lieu d'engager la responsabilité pénale de la société Uber », écartant ainsi la poursuite de la personne morale. En revanche, l'opératrice humaine de sécurité présente derrière le volant, qui n'avait pas repris le contrôle à temps, distraite par son téléphone, s'est retrouvée poursuivie pour homicide par négligence. Ce cas américain illustre une tendance : en l'état actuel du droit, lorsqu'un accident impliquant une IA, les autorités cherchent le maillon humain fautif. Aux États-Unis, le backup driver d'Uber a finalement été inculpée de homicide involontaire, marquant la première poursuite pénale liée à une voiture autonome, là où l'algorithme en cause n'avait, par définition, ni conscience ni personnalité juridique.

juridique spécifique aux robots, communément appelée « personnalité robot » ou « électronique »⁴⁷, apparaît comme une nécessité. Certains juristes y voient une avancée nécessaire à l'émergence d'une « robohumanité » facilitant l'identification pénale et civile, tandis que d'autres considèrent cela comme une « incongruité »⁴⁸ ou « une monstruosité juridique »⁴⁹. Cette personnalité permettrait notamment d'identifier précisément la machine pénalement responsable, grâce à un système similaire au registre d'immatriculation⁵⁰.

En somme, le cadre juridique marocain relatif aux algorithmes publics est encore en construction. La loi 09-08 fournit une base de protection des données, mais doit être modernisée pour faire face aux enjeux spécifiques de l'IA. D'ici là, elle peut servir de socle juridique utile sur lequel s'appuyer pour éviter que l'algorithme criminel ne se matérialise davantage dans la pratique.

4. Conclusion

De l'algorithme protecteur à l'algorithme criminel, il n'y a qu'un pas et la création d'une intelligence artificielle puissante sera soit la meilleure chose, soit la pire chose jamais arrivée à l'humanité⁵¹. Entre l'usage éclairé encadré et proportionné d'un outil technologique, et l'usage opaque biaisé ou détourné à des fins répressives, la frontière demeure extrêmement fine. Certes les bénéfices attendus sont nombreux voire réels, tels que l'optimisation de l'action policière, la lutte préventive contre la criminalité, le désengorgement des tribunaux, la réduction de la subjectivité dans les décisions grâce à la data... Cependant, le risque de dérives est tout aussi tangible : biais discriminatoire ethnique et racial, renforcement d'inégalités sociales, surveillance généralisée, opacité décisionnelle et affaiblissement du rôle humain sont autant de dérives potentielles qui peuvent faire basculer l'algorithme du côté obscur.

Cette tension est d'autant plus forte que les lois pénales traduisent moins une réponse directe à une insécurité réelle qu'une réaction à des représentations sociales et médiatiques de la délinquance. Influencées par l'évolution des contextes socio-économiques et politiques, ces lois privilégient désormais une approche sécuritaire et préventive centrée sur la surveillance accrue des comportements jugés déviants, entraînant une extension du contrôle social bien au-delà de la seule répression judiciaire.

Ainsi, la puissance publique ne doit jamais perdre de vue que l'outil algorithmique n'est qu'un moyen, et non une fin en soi. S'il peut être un formidable allié protecteur dans les mains de l'État, il peut tout aussi bien devenir un adversaire des libertés s'il échappe à tout contrôle. Cette frontière fragile exige un équilibre constant entre innovation et éthique, efficacité et droits humains. La France et le Maroc, chacun à leur rythme, sont engagés dans cette quête d'équilibre. Le défi est de taille : il s'agit de réussir l'intégration des algorithmes dans la sphère publique sans trahir les valeurs fondamentales de nos systèmes juridiques. C'est le prix à payer pour que jamais « l'algorithme criminel » ne prenne le pas sur « l'algorithme protecteur ».

REFERENCES

- [1] R. SAVATIER, *Les métamorphoses économiques et sociales du droit privé d'aujourd'hui*, Dalloz, Paris, 1959.
- [2] Nerolinkmedia, « Le paysage digital au Maroc », disponible sur : <https://nerolinkmedia.com/blog/le-paysage-digital-au-maroc> (consulté le 12 juin 2025 à 13h36).
- [3] Le Monde, « Le Maroc sous le choc après le piratage de la sécurité sociale », disponible sur : https://www.lemonde.fr/afrique/article/2025/04/14/le-maroc-sous-le-choc-apres-le-piratage-de-la-securite-sociale-bienvenue-en-enfer-ou-tout-le-monde-sait-combien-gagne-son-voisin_6595892_3212.html (consulté le 12 juin 2025 à 15h54).
- [4] S. LEBRETON-DERRIEN et R. RAHER (dir.), *Algorithmes, Justice Prédictive et Juges-Robots*, Enrick-B-Éditions, Paris, 2023.
- [5] Rapport de la Commission informatique et libertés, dit Rapport Tricot, La documentation française, 1975, p. 15.
- [6] T. MÉNISSIER, « Une intelligence artificielle pour la justice ? Institutions sociotechniques et autorité des machines », *Dalloz IP/IT*, n°1, 2022, p. 17.

⁴⁷ J.-Cl. PLANQUE, « *Robotum Delinquere Potest ?* » *L'intelligence artificielle et la responsabilité pénale* », *Droit pénal*, n°6, Juin 2022, Études n°14.

⁴⁸ N. NEVEJANS, *Règles de droit civil en robotique*, Étude pour le Parlement européen, commission des affaires juridiques, 2016, p. 16 et s.

⁴⁹ G. LOISEAU, « *La personnalité juridique des robots : une monstruosité juridique* », *JCP G* 2018, 597.

⁵⁰ J.-Cl. PLANQUE, op. cit.,

⁵¹ S. HAWKING, Allocution lors de l'inauguration du *Leverhulme Centre for the Future of Intelligence* à Cambridge en octobre 2016.

- [7] N. CARR, *Remplacer l'humain. Critique de l'automatisation sur les personnes de la société*, L'échappée, coll. « Pour en finir avec », 2017, p. 53 et s.
- [8] D. KNUTH, *The Art of Computer Programming*, Addison-Wesley, Boston, 1969, T. 4 ; G. BOOLOS, R. JEFFEREY, *Computability and Logic*, CUP, Cambridge, 1974.
- [9] Fr. RABELAIS, *Les horribles et espouvantables faictz et prouesses du très renommé Pantagruel*, éd., Lyon, 1533, Chap. X, p. 73.
- [10] J. BODIN, *Les six livres de la République*, Jacques du Puys, Paris, 1576, 759 p.
- [11] Déclaration des Droits de l'Homme et du Citoyen de 1789 (Art. 14 & Art 15).
- [12] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF, 7 janvier 1978.
- [13] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, JOUE, 4 mai 2016.
- [14] Ordonnance n° 2018-1125 du 12 décembre 2018, JORF, 13 décembre 2018.
- [15] Décret n° 2019-536 du 29 mai 2019, JORF, 30 mai 2019.
- [16] Loi n° 78-753 du 17 juillet 1978, JORF, 18 juillet 1978.
- [17] Loi n° 79-18 du 3 janvier 1979 sur les archives, JORF, 5 janvier 1979.
- [18] Loi n° 79-587 du 11 juillet 1979 relative à la motivation des actes administratifs, JORF, 12 juillet 1979.
- [19] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF, 8 octobre 2016.
- [20] Le Monde, « Espionnage de la NSA, une ligne rouge a été franchie selon la Cnil », 24 octobre 2013.
- [21] Observatoire des algorithmes publics, disponible sur : <https://odap.fr/inventaire/synthese> (consulté en novembre 2024).
- [22] X. LEONETTI, *Smartsécurité et cyberjustice*, PUF, 2021, p. 12.
- [23] France Inter, « L'outil PAVED créé par la gendarmerie », disponible sur : <https://www.franceinter.fr/emissions/grand-angle/grand-angle-02-octobre-2018>.
- [24] M. BARTOLUCCI, « L'expérimentation de la vidéosurveillance algorithmique », Dr. adm. 2023, étude 7.
- [25] E. SERUGA-CAU, « L'utilisation de 'caméras augmentées' dans l'espace public », Comm. Com. Electr. 2023, étude 14.
- [26] M.-A. GRANGER, « Surveiller et contrôler », AJDA 2023, p. 2222.
- [27] C. CRICHTON, « Vidéosurveillance intelligente aux JO », Dalloz actu, 12 juillet 2024.
- [28] E. VERGÈS, C. BAZZOLI, « La modélisation des décisions de justice », La Semaine Juridique, Supplément n°6, 10 février 2025, n°6004.
- [29] O. VAUDAUX, C. BAZZOLI et al., Proceedings of the Natural Legal Language Processing Workshop 2023, Association for Computational Linguistics, décembre 2023, Singapour, p. 38-43.
- [30] O. VAUDAUX, C. BAZZOLI et al., « Intelligence artificielle contre intelligence humaine », La Semaine Juridique, Supplément n°6, 10 février 2025, n°6002.
- [31] Ministère de l'intérieur – Direction Générale de la Sûreté Nationale, mars 2025.
- [32] Intelligence artificielle au Maroc, disponible sur : <https://www.intelligenceartificiellemaroc.com>.
- [33] L'Opinion, « Intelligence artificielle », disponible sur : <https://www.lopinion.ma/Intelligence-artificielle>.
- [34] A. DEBET, « Intelligence artificielle et données à caractère personnel », in A. Bensamoun et G. Loiseau (dir.), *Droit de l'intelligence artificielle*, p. 271, n°461.
- [35] Y. POULLET, *La vie privée à l'heure de la société du numérique*, Larcier, 2019, p. 117, n°21.
- [36] La Quadrature du Net, disponible sur : <https://www.laquadrature.net>.
- [37] L. BYGRAVE, *Data Protection Law*, 2017, p. 301.
- [38] Directive (UE) 2016/680 du 27 avril 2016.
- [39] Loi n° 2019-222, 23 mars 2019, art. 4.
- [40] F. G'SELL, « Les décisions algorithmiques », in F. G'SELL (dir.), *Le Big Data et le droit*, Dalloz, 2020, p. 97.
- [41] J.-Cl. PLANQUE, « Robotum Delinquere Potest ? », Droit pénal, n°6, juin 2022, étude n°14.
- [42] S. HAWKING, Allocution inaugurale, Leverhulme Centre, Cambridge, octobre 2016.