

Les angles morts de la loi n° 09-08 : Lacunes normatives et déficit d'effectivité du droit marocain des données personnelles

The blind spots of law no. 09-08: regulatory gaps and the lack of effectiveness of moroccan personal data protection law

Soufiane MOUHSSINE

Docteur en droit privé

Faculté des sciences juridiques, économiques et sociales Aïn-Chock, Université Hassan II de Casablanca, Maroc

soufianemouhssine@outlook.com

DOI: <https://doi.org/10.65040/remeye.2026.11.v02n30.45>



This work is licensed under a Creative Commons Attribution 4.0 International License

<https://creativecommons.org/licenses/by/4.0/>

Résumé:

La loi n° 09-08 du 18 février 2009 a doté le Maroc d'un régime général de protection des données à caractère personnel largement inspiré de la directive 95/46/CE. Dix-sept ans plus tard, le texte demeure inchangé alors que les traitements qu'il entend encadrer ont changé de nature. Le présent article propose de lire ses insuffisances à travers la notion d'angle mort, entendue comme la zone qu'un dispositif ne peut percevoir depuis la position où il a été placé. Deux familles d'angles morts sont mises en évidence. Les premières sont normatives. Elles tiennent à un champ d'application que les exclusions régaliennes, les lois spéciales et un critère territorial fondé sur les moyens de traitement rendent poreux, ainsi qu'à un contenu de protection pensé pour le fichier plutôt que pour le profil. Les secondes sont institutionnelles. Elles tiennent à une autorité de contrôle privée de pouvoir de sanction administrative et contrainte de réguler par délibérations, et à un contentieux où la voie pénale l'emporte sur la réparation. L'analyse s'appuie sur les délibérations de la Commission nationale de contrôle de la protection des données à caractère personnel, sur la jurisprudence marocaine disponible et sur une comparaison avec le droit de l'Union européenne, le droit français et plusieurs droits africains. Elle conclut que la refonte annoncée ne corrigera ces angles morts qu'à la condition de traiter ensemble la règle et l'institution.

Mots-clés : Loi n° 09-08 ; données à caractère personnel ; angle mort ; effectivité ; profilage.

Abstract:

Moroccan Law No. 09-08 of 18 February 2009 established a general data protection regime modelled on Directive 95/46/EC. Seventeen years later the statute remains unchanged, while the processing it seeks to govern has been transformed. This article reads its shortcomings through the notion of the blind spot, understood as the area a system cannot perceive from the position in which it was placed. Two families of blind spots are identified.

Normative blind spots stem from a scope weakened by sovereign exclusions, special statutes and a territorial test based on the location of processing means, and from a body of rights designed for the file rather than the profile. Institutional blind spots stem from a supervisory authority without administrative fining powers, which is forced to regulate through deliberations, and from a litigation landscape in which criminal prosecution prevails over compensation. Drawing on the deliberations of the Moroccan data protection authority, available Moroccan case law and a comparison with EU, French and several African laws, the article argues that the announced reform will only address these blind spots if it treats the rule and the institution together.

Keywords: Law no. 09-08; personal data; blind spot; effectiveness; profiling.

Introduction

Le président de la Commission nationale de contrôle de la protection des données à caractère personnel présente volontiers la loi n° 09-08 comme un code de la route applicable à la « conduite » des traitements de données¹. La comparaison mérite d'être prise au sérieux, et peut-être plus loin que ne l'entendait son auteur. Tout conducteur sait qu'il existe, autour de son véhicule, des zones que ni le pare-brise ni les rétroviseurs ne laissent voir. Ces zones ne résultent pas d'une faute de conduite. Elles tiennent à la place qu'occupe le conducteur et à la manière dont l'habitacle a été dessiné. Un texte juridique connaît des phénomènes semblables. Il regarde le réel depuis le lieu et le moment de son écriture, et certaines situations lui échappent pour cette seule raison.

Promulguée par le dahir n° 1-09-15 du 18 février 2009, la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel a été complétée par le décret n° 2-09-165 du 21 mai 2009². Elle a institué la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) et fixé, pour la première fois en droit marocain, un régime général applicable aux traitements publics et privés. Ses sources d'inspiration sont connues. Le texte reprend l'architecture de la directive 95/46/CE et emprunte de nombreuses formules à la loi française du 6 janvier 1978 dans sa rédaction issue de la réforme de 2004³. Sa raison d'être ne l'est pas moins. La note de

¹ O. Seghrouchni, « Est-ce que la protection de la vie privée est un concept marginal ? », chronique, *Médias24*, en ligne. Dans un entretien ultérieur, le même auteur compare la notification préalable à la CNDP au permis de conduire. V. « Protection des données, la confiance, moteur de l'économie numérique », entretien, *Finances News Hebdo*, 4 août 2026.

² Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, *B.O.* n° 5714 du 5 mars 2009 ; décret n° 2-09-165 du 21 mai 2009 pris pour l'application de la loi n° 09-08.

³ Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation

présentation du projet insistait sur la nécessité d'offrir à l'Union européenne un niveau de protection jugé adéquat, et un ancien président de la CNDP rattachait ouvertement la loi au développement de l'offshoring¹. La protection de la personne et l'attractivité du territoire ont donc été pensées d'un même geste.

Depuis, le paysage normatif s'est profondément modifié. La Constitution de 2011 a consacré, en son article 24, le droit de toute personne à la protection de sa vie privée². Le Maroc a adhéré à la Convention 108 du Conseil de l'Europe et à son protocole additionnel, entrés en vigueur à son égard le 1er septembre 2019³. L'Union européenne a remplacé la directive de 1995 par le règlement général sur la protection des données, et le Conseil de l'Europe a modernisé sa convention par le protocole d'amendement dit « Convention 108+ »⁴. Le texte marocain, lui, n'a pas été retouché. Une refonte a bien été préparée avec le ministère de la Justice et transmise au Secrétariat général du gouvernement, mais elle n'avait pas été publiée au Bulletin officiel à la date de rédaction de ces lignes⁵.

Ce décalage invite à une lecture critique. Encore faut-il choisir l'instrument de cette lecture. La notion de lacune, familière à la théorie du droit, désigne l'absence d'une règle là où l'on en attendait une⁶. Elle appelle un remède simple, l'ajout de la règle manquante. La notion d'angle mort est plus exigeante. Elle désigne ce qu'un dispositif ne peut pas percevoir

de ces données ; loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

¹ Sur la note de présentation, v. « Le gouvernement s'intéresse finalement à la protection des données personnelles », *Yabiladi*, article n° 1422. Sur l'objectif lié à l'offshoring, v. les propos du président de la CNDP de l'époque rapportés par *Al3omk*, en langue arabe.

² Constitution du Royaume du Maroc, promulguée par le dahir n° 1-11-91 du 29 juillet 2011, art. 24, al. 1er.

³ Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) et protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181). Les instruments de ratification ont été déposés le 28 mai 2019. V. Conseil de l'Europe, « Bienvenue au Maroc, 55e État partie à la Convention 108 », communiqué du 28 mai 2019. Les lois d'approbation n° 46-13 et n° 132-13 avaient été publiées au *Bulletin officiel* en 2014.

⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD), applicable depuis le 25 mai 2018 ; protocole d'amendement à la Convention 108 (STCE n° 223), ouvert à la signature le 10 octobre 2018.

⁵ Entretien précité, *Finances News Hebdo*, 4 août 2026. Le président de la CNDP y indique que la proposition de refonte a été travaillée avec le ministère de la Justice, qui l'a transmise au Secrétariat général du gouvernement.

⁶ Ch. Perelman (dir.), *Le problème des lacunes en droit*, Bruxelles, Bruylant, 1968.

en raison même de sa construction. Un angle mort ne se comble pas par une disposition supplémentaire, car il procède du point de vue adopté par le législateur. Il présente en outre une particularité redoutable. Ceux qui appliquent le texte ne le voient pas davantage que ceux qui l'ont écrit, de sorte qu'il peut subsister longtemps sans susciter de contentieux.

L'image convient particulièrement à une loi qui raisonne en termes de « fichier », c'est-à-dire d'« ensemble structuré de données à caractère personnel accessibles selon des critères déterminés »¹. Un juriste familier de l'administration des bases de données mesure combien cette représentation, exacte en 2009, s'accorde mal avec les architectures actuelles. Celles-ci sont faites de lacs de données, de journaux techniques, de flux continus et de modèles entraînés dont les paramètres ne contiennent aucune fiche individuelle et peuvent pourtant restituer des informations sur des personnes. Le fichier supposait un contenant identifiable et un gestionnaire unique. Le traitement contemporain se présente plutôt comme une chaîne d'opérations réparties entre plusieurs acteurs, dont aucun ne détient seul la totalité des données ni la maîtrise de leur usage.

La méthode retenue combine trois sources. L'exégèse du texte et de son décret d'application constitue le premier niveau d'analyse. Les délibérations de la CNDP en forment le deuxième, car la Commission a dû, au fil des années, préciser et parfois prolonger une loi restée immobile. La jurisprudence, encore rare mais en voie de constitution, offre le troisième². Le droit comparé intervient à chaque étape. Le droit de l'Union européenne et le droit français fournissent un point de comparaison naturel, compte tenu de la filiation du texte marocain. Les droits tunisien, algérien et sénégalais permettent de vérifier que les solutions européennes ne sont pas les seules concevables sur le continent. Le RGPD sera donc traité comme un terme de comparaison et non comme un étalon. La greffe d'un modèle étranger sur un ordre juridique qui ne partage ni ses institutions ni sa culture contentieuse produit rarement les effets attendus³.

Une question guide l'ensemble de l'étude. Dans quelle mesure la loi n° 09-08, conçue en 2009 sur le modèle de la directive 95/46/CE, parvient-elle encore à saisir les traitements contemporains de données et à garantir effectivement les droits qu'elle proclame ? La réponse suppose de distinguer deux familles d'angles morts. Les uns affectent la règle elle-même, qu'il s'agisse de son périmètre ou de son contenu. Ils correspondent à ce que la loi ne voit pas (I). Les autres affectent l'appareil chargé de la faire respecter, qu'il s'agisse de l'autorité de contrôle ou du juge. Ils correspondent à ce que la loi voit sans pouvoir l'atteindre (II).

¹ Loi n° 09-08, art. 1er, 4°.

² Selon le président délégué du Conseil supérieur du pouvoir judiciaire, les juridictions marocaines ont connu 153 affaires relatives à la protection des données personnelles en 2024, dont 83 devant les tribunaux de première instance et 70 devant les cours d'appel. V. « Protection des données personnelles, le débat est ouvert, quid des solutions », *Hespress FR*, 28 janvier 2025.

³ P. Legrand, « The Impossibility of "Legal Transplants" », *Maastricht Journal of European and Comparative Law*, vol. 4, 1997, p. 111.

Première partie: Les angles morts normatifs, une protection aux contours lacunaires

Toute loi de protection repose sur deux choix préalables. Elle désigne les situations qu'elle gouverne et fixe le contenu des garanties qu'elle accorde. Dans la loi n° 09-08, ces deux choix ont été faits à partir d'un même point de vue, celui d'un responsable identifiable, établi sur le territoire et détenteur d'un fichier. Ce point de vue explique la porosité du périmètre de la protection (A) autant que l'inadaptation de son contenu aux traitements contemporains (B).

A. Les angles morts du champ d'application

Le champ d'application d'une loi de protection des données se mesure selon deux axes. L'axe matériel détermine quels traitements sont concernés. L'axe territorial détermine quels responsables sont tenus. Sur chacun d'eux, la loi n° 09-08 laisse hors de sa vue des pans entiers de l'activité de traitement.

1° Un champ matériel amputé par les exclusions régaliennes et les lois spéciales

L'article 2 de la loi pose un principe large. Le texte s'applique à tout traitement automatisé en tout ou en partie, ainsi qu'aux traitements non automatisés de données contenues ou appelées à figurer dans des fichiers manuels¹. Le paragraphe 4 du même article apporte cependant quatre tempéraments dont la portée cumulée est considérable.

Le premier vise les traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. L'exclusion est classique et se retrouve dans tous les textes de la famille européenne. Elle soulève pourtant une difficulté que la loi ne tranche pas, celle des dispositifs privés qui débordent le cercle domestique. La caméra installée par un particulier à l'entrée de son domicile filme aussi le passage commun, la rue, la porte du voisin. La Cour de justice de l'Union européenne a jugé, dans l'arrêt *Ryneš*, qu'un tel dispositif ne relève pas de l'exception domestique dès lors qu'il couvre, même partiellement, l'espace public². Elle avait auparavant refusé le bénéfice de l'exception à la publication de données sur une page internet accessible à un nombre indéfini de personnes³. La Cour de cassation marocaine est parvenue, par une autre voie, à un résultat voisin. Dans un arrêt du 16 avril 2024, elle a approuvé les juges du fond d'avoir ordonné le retrait de caméras installées par les propriétaires d'une villa casablancaise, en relevant que ceux-ci ne prouvaient pas avoir informé les personnes filmées comme l'exige la loi n° 09-08⁴. La solution est

¹ Loi n° 09-08, art. 2, 1.

² CJUE, 11 décembre 2014, *František Ryneš c. Úřad pro ochranu osobních údajů*, aff. C-212/13.

³ CJCE, 6 novembre 2003, *Bodil Lindqvist*, aff. C-101/01.

⁴ Cour de cassation, arrêt n° 1870 du 16 avril 2024, dossier civil n° 2023/3/1/1870, rapporté par *Akhbarona*, 10 juin 2026, en langue arabe. La Cour rappelle que la loi reconnaît à toute personne le droit de s'opposer au traitement des données la concernant et que l'usage de la vidéosurveillance reste soumis à des conditions protectrices de la vie privée, puis rejette le pourvoi.

heureuse. Elle montre cependant que la frontière de l'exception domestique, que le législateur n'a pas tracée, se dessine au gré des litiges.

Le deuxième tempérament exclut purement et simplement les données « recueillies et traitées dans l'intérêt de la défense nationale et de la sécurité intérieure ou extérieure de l'État ». Le troisième soumet les traitements de prévention et de répression des crimes et délits aux seules conditions fixées par la loi ou le règlement qui crée le fichier, ce règlement étant soumis à l'avis préalable de la CNDP¹. Ces dispositions sont héritées de la directive de 1995, qui excluait elle aussi de son champ la sécurité publique, la défense et les activités de l'État relatives au droit pénal². L'héritage a toutefois été recueilli sans le correctif qui l'accompagnait en Europe. Les États membres disposaient de législations nationales couvrant ces fichiers, et le droit de l'Union a fini par les saisir au moyen d'un instrument spécifique, la directive 2016/680, qui soumet les traitements policiers et judiciaires à des principes, à des droits et à un contrôle indépendant³. En France, même les traitements intéressant la sûreté de l'État et la défense demeurent soumis à la loi de 1978 et ouvrent un droit d'accès indirect exercé par l'intermédiaire de la CNIL⁴. La loi marocaine, elle, ne prévoit pour la défense et la sécurité de l'État ni principe minimal, ni avis de la CNDP, ni voie d'accès indirect. Le contraste est d'autant plus net que la Convention 108, à laquelle le Maroc est partie, n'admet de dérogations pour la sûreté de l'État que si elles sont prévues par la loi et constituent une mesure nécessaire dans une société démocratique⁵. L'exclusion totale satisfait mal cette exigence, car elle dispense précisément l'autorité publique de toute justification au cas par cas.

Le quatrième tempérament est le plus original et, à notre sens, le plus lourd de conséquences. La loi ne s'applique pas « aux données à caractère personnel recueillies en application d'une législation particulière ». Les projets ou propositions de loi créant de tels fichiers sont seulement « communiqués » à la CNDP, avec l'indication de leur responsable, de leurs finalités et des mesures de sécurité envisagées⁶. Cette exclusion n'a pas d'équivalent dans la directive de 1995, qui laissait les traitements fondés sur une obligation légale dans son

¹ Loi n° 09-08, art. 2, 4, deuxième tiret, et art. 27, A, 2°.

² Directive 95/46/CE, art. 3, paragraphe 2.

³ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 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.

⁴ Loi n° 78-17 du 6 janvier 1978, titre IV relatif aux traitements intéressant la sûreté de l'État et la défense, dans sa rédaction issue de l'ordonnance n° 2018-1125 du 12 décembre 2018.

⁵ Convention 108, art. 9, paragraphe 2, a. Le protocole d'amendement de 2018 maintient cette exigence en la renforçant (Convention 108+, art. 11).

⁶ Loi n° 09-08, art. 2, 4, troisième tiret.

champ et autorisait seulement des limitations ciblées de certains droits¹. Elle aboutit à un résultat paradoxal. Plus un traitement est massif et structurant, plus il a de chances d'être institué par une loi spéciale, et plus il s'éloigne du droit commun de la protection. Le registre national de la population et le registre social unifié, institués par la loi n° 72-18, en offrent une illustration². Leur régime dépend d'abord de la loi qui les crée, et la protection qu'ils offrent tient moins au droit commun qu'aux garanties que le législateur spécial a bien voulu y inscrire. Le Médiateur du Royaume a d'ailleurs publiquement dénoncé, en janvier 2025, la collecte par certaines administrations de données d'utilisateurs sans base légale identifiable³. Le président de la CNDP a, de son côté, demandé que le gouvernement sollicite l'avis de la Commission avant l'adoption de toute loi impliquant des traitements de données⁴. Cette demande révèle l'angle mort. L'article 27 de la loi ne permet à la CNDP de rendre un avis que sur les projets « dont elle est saisie ». La Commission a ainsi pu se prononcer sur le projet de loi relatif aux bureaux d'information sur le crédit, sur le projet de loi n° 41-19 relatif à l'administration numérique ou sur le projet de décret relatif au registre public des bénéficiaires effectifs⁵. Rien n'oblige toutefois l'auteur d'un texte à la consulter.

L'addition de ces exclusions dessine une géographie singulière. La protection est forte là où le responsable est un acteur privé ordinaire, soumis à déclaration et exposé à des sanctions pénales. Elle s'affaiblit à mesure que l'on s'approche de l'État, alors que c'est précisément là que se constituent les fichiers les plus complets et les interconnexions les plus nombreuses.

2° Un champ territorial inadapté à l'économie des plateformes

La loi s'applique au traitement effectué par un responsable établi sur le territoire marocain. Elle s'applique aussi au responsable non établi au Maroc qui recourt à des moyens de traitement situés sur ce territoire, à l'exclusion du simple transit⁶. Dans ce second cas, le responsable étranger doit notifier à la CNDP l'identité d'un représentant installé au Maroc.

¹ Directive 95/46/CE, art. 7, c, et art. 13.

² Loi n° 72-18 relative au dispositif de ciblage des bénéficiaires des programmes d'appui social et portant création de l'Agence nationale des registres, promulguée en 2020. Sur le lien entre la pérennité du registre social unifié et l'accès aux données des citoyens, v. l'intervention du président du Conseil de la concurrence rapportée par *Hespress FR*, 28 janvier 2025.

³ Intervention de M. Mohamed Benalilou, Médiateur du Royaume, lors de la conférence organisée par la CNDP le 27 janvier 2025, rapportée par *Hespress FR*, 28 janvier 2025.

⁴ Entretien précité, *Finances News Hebdo*, 4 août 2026.

⁵ CNDP, délibération n° D-170-2020 du 19 octobre 2020 portant avis sur le projet de loi relatif aux bureaux d'information sur le crédit ; délibération n° D-127-2020 portant avis sur le projet de loi n° 41-19 relatif à l'administration numérique ; délibération n° D-181-2021 portant avis sur le projet de décret relatif au registre public des bénéficiaires effectifs.

⁶ Loi n° 09-08, art. 2, 2 et 3.

Ces deux critères reproduisent ceux de l'article 4 de la directive de 1995. Ils supposaient un monde où le traitement exigeait une présence matérielle, qu'il s'agisse d'un siège, d'une agence, d'un serveur ou d'un terminal.

Le critère de l'établissement peut recevoir une interprétation extensive. La loi précise d'ailleurs qu'est considéré comme établi le responsable qui exerce une activité sur le territoire dans le cadre d'une « installation, quelle que soit sa forme juridique ». La Cour de justice a montré le parti qu'on pouvait tirer d'une formule voisine. Elle a jugé que le traitement réalisé par un moteur de recherche américain était effectué « dans le cadre des activités » de sa filiale publicitaire espagnole, et elle s'est contentée, dans l'affaire *Weltimmo*, d'une activité réelle et effective exercée au moyen d'une installation stable, fût-elle minime¹. Cette lecture suppose néanmoins une implantation locale. Une plateforme qui collecte depuis l'étranger les données d'utilisateurs marocains, sans filiale ni bureau au Maroc, n'est saisie par aucun des deux critères. Le critère des moyens pourrait être sollicité si l'on considérait, comme l'avait fait le groupe de l'article 29 en 2002, que le dépôt de témoins de connexion sur le terminal de l'utilisateur constitue l'usage d'un moyen situé sur le territoire². La construction est fragile, et aucune délibération de la CNDP ne l'a consacrée à notre connaissance.

Le législateur européen a tiré les conséquences de cette fragilité. L'article 3, paragraphe 2, du RGPD rattache désormais au règlement le responsable non établi dans l'Union qui offre des biens ou des services à des personnes qui s'y trouvent ou qui suit leur comportement³. Ce critère du ciblage a permis à la CNIL de sanctionner une société américaine de reconnaissance faciale dépourvue de tout établissement européen, et à l'autorité italienne d'imposer des mesures puis une amende au fournisseur d'un agent conversationnel⁴. Plusieurs législations africaines récentes ont emprunté la même voie. La loi nigériane de 2023 sur la protection des données s'applique ainsi au responsable étranger qui traite les données

¹ CJUE, gr. ch., 13 mai 2014, *Google Spain et Google*, aff. C-131/12 ; CJUE, 1er octobre 2015, *Weltimmo*, aff. C-230/14.

² Groupe de travail « Article 29 », document de travail WP 56 du 30 mai 2002 sur l'application internationale de la législation européenne relative à la protection des données au traitement des données à caractère personnel sur l'internet par des sites web établis en dehors de l'Union européenne.

³ RGPD, art. 3, paragraphe 2, et art. 27 ; Comité européen de la protection des données, lignes directrices 3/2018 relatives au champ d'application territorial du RGPD, version adoptée le 12 novembre 2019.

⁴ CNIL, formation restreinte, délibération n° SAN-2022-019 du 17 octobre 2022 concernant la société Clearview AI, amende de 20 millions d'euros ; Garante per la protezione dei dati personali, mesure de limitation provisoire du 30 mars 2023 visant OpenAI, puis sanction de 15 millions d'euros prononcée en décembre 2024.

d'une personne se trouvant au Nigeria¹. La CNDP, qui a conclu en 2026 un mémorandum d'entente avec son homologue nigérienne, dispose là d'un modèle de proximité².

Faute d'un tel critère, l'action de la CNDP envers les grandes plateformes emprunte les voies de la diplomatie plus que celles du droit. En août 2023, la Commission a cosigné avec onze autorités étrangères une lettre adressée à plusieurs groupes du numérique au sujet de l'extraction automatisée de données sur leurs services³. L'initiative est utile. Elle reste néanmoins une invitation, dépourvue de force contraignante à l'égard de destinataires que la loi marocaine ne saisit pas.

L'angle mort territorial se prolonge dans le régime des transferts. Les articles 43 et 44 subordonnent le transfert de données vers un État étranger à un niveau de protection suffisant, apprécié par la CNDP, ou à l'une des dérogations énumérées⁴. Ce régime raisonne en termes d'exportation. Il suppose que les données se trouvent d'abord au Maroc, entre les mains d'un responsable marocain, avant d'en sortir. Or une part croissante des données des résidents marocains n'est jamais « transférée » au sens de la loi. Elle est collectée directement à l'étranger par le service que l'utilisateur emploie. Le contrôle des transferts ne voit pas ces flux, puisqu'il n'y a pas de frontière à franchir. Les critères d'appréciation retenus par l'article 43 appellent une seconde observation. Ils portent sur la législation du pays de destination, les mesures de sécurité et les caractéristiques du traitement. Ils ignorent la question, devenue centrale depuis l'arrêt *Schrems II*, de l'accès des autorités publiques étrangères aux données transférées⁵. Au moment où le Royaume attire des projets de centres de données et d'informatique en nuage, cette lacune touche directement à la souveraineté numérique dont se réclament les pouvoirs publics⁶.

B. Les angles morts du contenu de la protection

Même lorsqu'un traitement entre dans le champ de la loi, la protection qu'elle accorde porte la marque de son époque. Les droits reconnus à la personne ont été pensés face à un

¹ Nigeria Data Protection Act, 2023, section 2.

² CNDP, « La CNDP et NDPC du Nigéria (Nigeria Data Protection Commission) signent un mémorandum d'entente », 22 mai 2026.

³ CNDP, communiqué du 24 août 2023 relatif à la lettre conjointe « Data scraping et protection de la vie privée », adressée notamment à Alphabet, ByteDance, Meta, Microsoft, Sina et X Corp., et cosignée par les autorités d'Australie, du Canada, du Royaume-Uni, de Hong Kong, de Suisse, de Norvège, de Nouvelle-Zélande, de Colombie, de Jersey, d'Argentine et du Mexique.

⁴ Loi n° 09-08, art. 43 et 44 ; adde art. 28, 10° et 11°.

⁵ CJUE, gr. ch., 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland et Maximilian Schrems*, aff. C-311/18.

⁶ Sur l'usage que le président de la CNDP fait de la notion de souveraineté à propos du nuage et des centres de données, v. l'entretien précité, *Finances News Hebdo*, 4 août 2026.

fichier que l'on consulte et que l'on corrige (1°). Les obligations imposées au responsable relèvent d'une logique de formalités préalables plus que d'une responsabilité continue (2°).

1° Des droits désarmés face au traitement algorithmique

Le chapitre II de la loi consacre un catalogue cohérent. La personne concernée est informée lors de la collecte, elle peut accéder aux données, en obtenir la rectification ou l'effacement, s'opposer au traitement pour des motifs légitimes et refuser la prospection¹. Ce catalogue convient parfaitement à un fichier. On y trouve une fiche, on la lit, on la corrige. Le traitement algorithmique ne se laisse pas saisir de la même manière. Le profil qu'il produit n'est pas une donnée stockée qu'il suffirait de consulter. C'est le résultat d'un calcul, souvent recommencé à chaque requête, qui combine des données fournies, observées et déduites. Quatre angles morts découlent de ce décalage.

Le premier concerne les données sensibles. L'article 1er vise les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ou qui sont relatives à la santé, y compris les données génétiques. La liste ignore deux catégories que le droit comparé protège désormais. La vie sexuelle n'y figure pas, alors que l'article 6 de la Convention 108 la range parmi les catégories particulières, ce que le Conseil de l'Europe avait relevé lors de l'examen de la législation marocaine². Les données biométriques n'y figurent pas davantage. La CNDP a dû combler ce silence par ses propres moyens, d'abord par une délibération sur le contrôle d'accès biométrique³, puis par un moratoire sur la reconnaissance faciale adopté en août 2019 et prolongé jusqu'au 31 décembre 2020⁴. Pendant ce moratoire, la Commission a autorisé au cas par cas certains usages, comme l'ouverture de comptes bancaires à distance ou la preuve de vie des allocataires des organismes de prévoyance sociale, en recommandant la mise en place d'un tiers de confiance national plutôt que la multiplication des bases biométriques⁵.

¹ Loi n° 09-08, art. 5 à 10.

² Convention 108, art. 6. Le Conseil de l'Europe avait relevé, dans son analyse de la loi n° 09-08 au regard de la Convention réalisée en vue de l'adhésion du Maroc, que les données relatives à la vie sexuelle n'étaient pas qualifiées de sensibles par la loi marocaine.

³ CNDP, délibération n° 478-2013 relative au contrôle d'accès par biométrie, dont les conditions sont reprises dans la fiche pratique de la CNDP « Le contrôle d'accès par biométrie ».

⁴ CNDP, délibération n° D-194-2019 du 30 août 2019 relative à un moratoire sur la reconnaissance faciale ; délibération n° D-97-2020 du 26 mars 2020 relative à la prolongation de ce moratoire jusqu'au 31 décembre 2020.

⁵ CNDP, délibération n° D-108-EUS/2020 du 23 avril 2020 relative à l'usage des technologies de reconnaissance faciale dans le cadre du dispositif du compte à distance par les banques et établissements de paiement ; délibération n° D-126-EUS/2020 du 29 juillet 2020 relative à l'usage de ces technologies par les établissements de prévoyance sociale.

Des choix aussi structurants pour une technologie aussi intrusive ont donc été faits par un régulateur, en l'absence de toute base textuelle propre à la biométrie.

Le deuxième angle mort concerne les données inférées. Un système qui déduit la religion d'une personne de ses habitudes de consommation, ou son état de santé de ses déplacements, produit une donnée sensible qu'aucun formulaire n'a jamais recueillie. La Cour de justice a jugé que des données de nature à révéler indirectement une information sensible, par une opération intellectuelle de rapprochement ou de déduction, relèvent du régime des catégories particulières¹. Le texte marocain contient le germe d'une solution comparable. L'article 1er emploie le verbe « révéler », et l'article 57 réprime le traitement sans consentement exprès de données qui, « directement ou indirectement », font apparaître les caractéristiques protégées². Mais la définition et le régime d'autorisation des articles 12 et 21 ne tirent pas cette conséquence. La donnée sensible y apparaît comme une donnée donnée, que l'on collecte. La donnée sensible algorithmique est une donnée produite, que l'on calcule. La loi voit la première et ignore largement la seconde.

Le troisième angle mort tient au régime des décisions automatisées. Sur ce terrain, la loi marocaine n'est pas en retard sur la lettre de ses modèles. Son article 7 reconnaît à la personne le droit de connaître « la logique qui sous-tend tout traitement automatisé » des données la concernant, ce qui est plus large que l'article 15 du RGPD, limité aux décisions entièrement automatisées. Son article 11, intitulé « neutralité des effets », interdit qu'une décision de justice appréciant le comportement d'une personne soit fondée sur un traitement destiné à évaluer sa personnalité, et qu'une autre décision produisant des effets juridiques soit prise sur le seul fondement d'un traitement destiné à définir son profil. La doctrine marocaine y a vu le socle d'un encadrement de la justice algorithmique³. Ces dispositions restent pourtant en deçà des usages qu'elles devraient régir. Le profil n'est pas défini, alors que le RGPD donne du profilage une définition précise⁴. Seules les décisions produisant des effets juridiques sont visées, et non celles qui affectent la personne de manière significative sans modifier sa situation juridique, comme le refus d'un crédit, l'éviction d'une candidature ou la modulation d'un prix. L'exigence d'un « seul fondement » permet enfin d'échapper à l'interdiction par une validation humaine de pure forme. La Cour de justice a écarté ce dernier artifice en jugeant que l'établissement d'un score par une agence de crédit constitue lui-même une décision automatisée lorsque le prêteur s'y fie de manière déterminante⁵. Elle a ensuite

¹ CJUE, gr. ch., 1er août 2022, *OT c. Vyriausioji tarnybinės etikos komisija*, aff. C-184/20 ; CJUE, gr. ch., 4 juillet 2023, *Meta Platforms e.a. c. Bundeskartellamt*, aff. C-252/21.

² Loi n° 09-08, art. 1er, 3°, et art. 57.

³ F. Bensghir, « La justice algorithmique en droit marocain. Commentaire des articles 7 et 11 de la loi n° 09-08 relative à la protection des données personnelles », *Maroclaw*, en ligne, en langue arabe.

⁴ RGPD, art. 4, 4), et art. 22, paragraphe 1. Adde Groupe de travail « Article 29 », lignes directrices relatives à la prise de décision individuelle automatisée et au profilage, WP 251 rév. 01, 6 février 2018.

⁵ CJUE, 7 décembre 2023, *SCHUFA Holding (Scoring)*, aff. C-634/21.

précisé que l'explication due à la personne doit décrire, de façon intelligible, la procédure et les principes effectivement appliqués, le secret des affaires ne pouvant être opposé qu'au terme d'une pondération opérée par l'autorité ou le juge¹. Le règlement européen sur l'intelligence artificielle a ajouté un droit à l'explication des décisions fondées sur des systèmes à haut risque². En France, le Conseil constitutionnel a subordonné l'usage d'algorithmes par l'administration à la capacité du responsable d'en maîtriser les évolutions et d'en expliquer le fonctionnement³. Aucune de ces précisions ne se retrouve en droit marocain. Le droit de connaître la logique d'un traitement n'a, à notre connaissance, jamais été invoqué devant un juge. La CNDP a annoncé en mars 2025 une délibération sur les traitements d'intelligence artificielle, en insistant sur leur contestabilité et leur traçabilité⁴. Là encore, le régulateur tente de construire ce que le texte ne dit pas.

Le quatrième angle mort réside dans les droits que la loi ignore. Le droit à la portabilité, qui permet de récupérer ses données pour changer de prestataire, n'existe pas⁵. Le droit à l'effacement est limité aux données dont le traitement n'est pas conforme à la loi. La Cour de justice avait pourtant tiré des dispositions équivalentes de la directive de 1995 un droit au déréférencement opposable aux moteurs de recherche⁶. Les articles 8 et 9 de la loi marocaine, qui reproduisent ces dispositions, permettraient au juge de suivre le même raisonnement. Le débiteur de ce droit se trouverait toutefois, le plus souvent, hors du champ territorial de la loi. Deux angles morts se superposent alors et se renforcent. La loi ne dit rien non plus du consentement des mineurs, alors que le RGPD fixe un âge de référence que les États peuvent abaisser jusqu'à treize ans et que la France l'a fixé à quinze ans⁷. La CNDP mène des actions de sensibilisation auprès des jeunes, mais aucune règle ne fixe l'âge à partir duquel un mineur peut consentir seul à un service en ligne⁸. Le sort des données des personnes décédées n'est pas davantage réglé, contrairement au droit français qui permet

¹ CJUE, 27 février 2025, *CK c. Dun & Bradstreet Austria*, aff. C-203/22.

² Règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle, art. 86.

³ Cons. const., décision n° 2018-765 DC du 12 juin 2018, *Loi relative à la protection des données personnelles*.

⁴ « Encadrement de l'IA, la CNDP auditionne experts et institutions », *Médias24*, 19 mars 2025 ; « IA, pourquoi la question des données devient centrale », *TelQuel*, 10 avril 2026.

⁵ RGPD, art. 20.

⁶ Loi n° 09-08, art. 8, a ; CJUE, gr. ch., 13 mai 2014, *Google Spain et Google*, préc., fondé sur les articles 12, b, et 14, a, de la directive 95/46/CE.

⁷ RGPD, art. 8 ; loi n° 78-17 du 6 janvier 1978, art. 45.

⁸ CNDP, « Motatawi3, la CNDP sensibilise les jeunes aux enjeux de la protection des données à caractère personnel », 28 août 2026.

depuis 2016 de formuler des directives sur leur conservation et leur communication¹. L'anonymisation, enfin, n'est pas définie, alors qu'elle commande l'ouverture des données publiques et l'entraînement des modèles. Le président du Conseil de la concurrence a d'ailleurs appelé, en janvier 2025, à un cadre permettant l'exploitation de données anonymisées².

2° Des obligations formalistes sans responsabilisation

L'économie générale de la loi repose sur des formalités préalables. Tout traitement doit faire l'objet d'une autorisation lorsqu'il porte sur des données sensibles, sur un changement de finalité, sur des données génétiques, sur des infractions, sur le numéro de la carte nationale d'identité ou sur une interconnexion de fichiers. Les autres traitements relèvent d'une déclaration, dont la CNDP délivre récépissé dans les vingt-quatre heures, le responsable pouvant mettre en œuvre le traitement dès sa réception³. Ce dispositif reproduit celui de la directive de 1995. Le législateur européen l'a abandonné en 2016, en constatant que l'obligation générale de notification engendrait des charges administratives et financières sans toujours améliorer la protection, et en lui substituant des procédures ciblées sur les traitements présentant un risque élevé⁴.

La logique formaliste a deux visages. Vis-à-vis de l'autorité, elle prend la forme de la déclaration. Vis-à-vis de la personne, elle prend celle du consentement, que l'article 4 érige en principe et dont les autres fondements ne sont présentés que comme des exceptions. Dans les deux cas, une formalité accomplie à l'entrée tient lieu de garantie pour toute la durée du traitement. La doctrine a montré combien le consentement, réduit à un clic sur des conditions que personne ne lit, peine à remplir ce rôle⁵. La déclaration rencontre une limite symétrique. Le président de la CNDP compare la notification préalable au permis de conduire et rappelle qu'il ne faut pas conduire sans permis⁶. La comparaison est éclairante, mais pas dans le sens qu'il lui donne. Le permis atteste une aptitude à la date où il est délivré. Il ne dit rien de la manière dont le conducteur se comportera ensuite. Un récépissé délivré en vingt-quatre heures, sur la base d'une description générale des mesures de sécurité, ne dit rien de la manière dont le traitement sera conduit pendant dix ans.

¹ Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, dont les dispositions figurent aujourd'hui à l'article 85 de la loi du 6 janvier 1978.

² RGPD, considérant 26 ; CJUE, 19 octobre 2016, *Patrick Breyer c. Bundesrepublik Deutschland*, aff. C-582/14. Sur la proposition du président du Conseil de la concurrence, v. *Hespress FR*, 28 janvier 2025, préc.

³ Loi n° 09-08, art. 12 à 20.

⁴ Directive 95/46/CE, art. 18 à 21 ; RGPD, considérant 89.

⁵ D. J. Solove, « Privacy Self-Management and the Consent Dilemma », *Harvard Law Review*, vol. 126, 2013, p. 1880.

⁶ Entretien précité, *Finances News Hebdo*, 4 août 2026.

Ce qui manque à la loi marocaine, c'est précisément l'outillage de la conduite. Elle ne connaît pas le principe de responsabilité, qui oblige le responsable à démontrer à tout moment sa conformité. Son article 3 lui impose seulement d'assurer le respect des principes « sous le contrôle de la Commission nationale »¹. Elle ne prévoit pas de registre des activités de traitement tenu par le responsable. Le registre national de l'article 45 en tient lieu, mais il est tenu par la CNDP et figé à la date des déclarations². Elle ignore l'analyse d'impact préalable aux traitements à risque, la protection des données dès la conception et par défaut, et le délégué à la protection des données³. Ces notions circulent pourtant dans le discours de la CNDP, qui les promeut à travers le programme « Data-Tika » lancé en juillet 2020 et lors de manifestations publiques⁴. Elles n'ont aucune force obligatoire. L'organisation qui adhère au programme s'engage volontairement, celle qui l'ignore ne s'expose à rien.

L'absence la plus lourde concerne la violation de données. La loi impose au responsable des mesures de sécurité appropriées et réprime pénalement leur défaut, ainsi que la négligence qui facilite l'usage abusif des données ou leur communication à des tiers non habilités⁵. Elle n'impose en revanche aucune notification de la violation, ni à la CNDP ni aux personnes concernées. La loi n° 05-20 relative à la cybersécurité oblige certes les administrations et les infrastructures d'importance vitale à déclarer immédiatement tout incident à l'autorité nationale de cybersécurité⁶. Cette obligation poursuit une autre finalité, la sécurité des systèmes d'information, et s'adresse à un autre destinataire. Elle ne bénéficie ni à la CNDP ni aux personnes dont les données ont fuité, et elle ne concerne pas les entreprises privées ordinaires. L'autorité de cybersécurité a d'ailleurs déploré, en janvier 2026, que de nombreuses entités ne déclarent pas leurs incidents dans les délais. La fuite de données subie par la Caisse nationale de sécurité sociale en avril 2025, qui aurait concerné près de deux millions de salariés, a révélé les effets de ce silence⁷. Les assurés ont découvert l'exposition de leurs données sur les réseaux sociaux. La CNDP a publié un communiqué mettant en garde

¹ Loi n° 09-08, art. 3, 3 ; comp. RGPD, art. 5, paragraphe 2, et art. 24.

² Loi n° 09-08, art. 45 et 46 ; comp. RGPD, art. 30.

³ RGPD, art. 25, 35 et 37 à 39.

⁴ Sur le programme Data-Tika, mis en place en juillet 2020, v. les conventions d'adhésion recensées sur le site de la CNDP. V. aussi la participation de la CNDP au panel « Privacy by Design » lors du GITEX Africa, avril 2026.

⁵ Loi n° 09-08, art. 23, 24, 58 et 61.

⁶ Loi n° 05-20 relative à la cybersécurité, art. 8 ; décret n° 2-21-406 du 15 juillet 2021 pris pour son application. Sur le rappel de cette obligation par la Direction générale de la sécurité des systèmes d'information, v. *TelQuel*, 21 janvier 2026.

⁷ Sur l'ampleur de la fuite, v. « La cyberattaque contre la CNSS décryptée en neuf points clés », *Médias24*, 12 avril 2025. Sur la réaction de la CNDP, v. son communiqué du 10 avril 2025, rapporté par *Hespress FR* le même jour.

contre l'usage des données fuitées et rappelant ses pouvoirs d'investigation, mais aucune règle n'imposait au responsable du traitement d'informer individuellement les personnes atteintes. Le RGPD impose une notification à l'autorité dans les soixante-douze heures et une communication aux personnes lorsque le risque est élevé. La Cour de justice a précisé qu'une violation ne suffit pas à établir l'insuffisance des mesures de sécurité, mais qu'il appartient au responsable de prouver leur caractère approprié¹. La loi marocaine laisse au contraire la personne supporter le risque sans même lui permettre de le connaître.

Un dernier angle mort tient à la manière dont la loi appréhende les acteurs du traitement. Le sous-traitant n'y est saisi qu'à travers le contrat qui le lie au responsable. Ce contrat doit prévoir qu'il n'agit que sur instruction et que les obligations de sécurité lui incombent également. La loi ne dit rien de la sous-traitance en cascade, qui est pourtant la règle dans l'informatique en nuage, où un prestataire étranger recourt lui-même à des sous-traitants répartis dans plusieurs pays². La responsabilité conjointe est mentionnée dans la définition du responsable du traitement, qui détermine les finalités et les moyens « seul ou conjointement avec d'autres », mais aucun régime n'en répartit les obligations. La Cour de justice a jugé que l'administrateur d'une page hébergée sur un réseau social et l'exploitant d'un site intégrant un module social sont responsables conjoints avec l'opérateur du réseau pour certaines opérations³. Transposée au Maroc, cette analyse conduirait à un résultat déséquilibré. L'administration ou l'entreprise marocaine qui anime une page sur un réseau social serait seule à répondre, devant la loi marocaine, d'un traitement dont les moyens essentiels sont fixés par un opérateur étranger que cette loi ne saisit pas. La loi atteint alors le maillon faible de la chaîne et laisse hors de vue le maillon fort.

Ces angles morts normatifs pourraient être en partie compensés par un régulateur doté de moyens d'action étendus et par un juge aisément accessible. L'appareil institutionnel chargé d'appliquer la loi connaît cependant ses propres angles morts.

Seconde partie: Les angles morts institutionnels, une protection à l'effectivité incertaine

Une règle ne vaut que par les mécanismes qui la font passer dans les faits. La sociologie du droit a montré depuis longtemps que l'ineffectivité n'est pas un accident de la règle, mais l'une de ses dimensions ordinaires, qu'il faut mesurer plutôt que déplorer⁴. La loi n° 09-08 confie sa mise en œuvre à deux gardiens. L'autorité de contrôle voit les

¹ RGPD, art. 33 et 34 ; CJUE, 14 décembre 2023, *VB c. Natsionalna agentsia za prihodite*, aff. C-340/21.

² Loi n° 09-08, art. 1er, 6°, art. 23, 2 et 3, et art. 25 ; comp. RGPD, art. 28, paragraphes 2 et 4.

³ Loi n° 09-08, art. 1er, 5° ; RGPD, art. 26 ; CJUE, gr. ch., 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, aff. C-210/16 ; CJUE, 29 juillet 2019, *Fashion ID*, aff. C-40/17.

⁴ J. Carbonnier, « Effectivité et ineffectivité de la règle de droit », *L'Année sociologique*, 1957-1958, repris dans *Flexible droit. Pour une sociologie du droit sans rigueur*, Paris, LGDJ.

manquements, mais ne peut guère les sanctionner elle-même (A). Le juge peut les sanctionner, mais il en connaît peu et répare mal (B).

A. Les angles morts de la régulation

La CNDP occupe une position paradoxale. Elle est l'institution qui connaît le mieux la réalité des traitements au Maroc, puisqu'elle reçoit les déclarations, instruit les autorisations et conduit les contrôles. Elle est aussi celle dont la loi a le plus étroitement borné les moyens. Ce paradoxe tient à son statut et à ses pouvoirs (1°), et il explique le recours massif aux délibérations comme instrument de régulation (2°).

1° Une autorité au statut et aux pouvoirs inachevés

L'article 27 de la loi institue la Commission « auprès du Premier ministre », aujourd'hui le Chef du gouvernement. Son président est nommé par le Roi, et ses six membres le sont également, sur proposition du Chef du gouvernement et des présidents des deux chambres du Parlement, pour un mandat de cinq ans renouvelable une fois¹. Des règles d'incompatibilité et de secret professionnel complètent ce dispositif. Plusieurs dispositions révèlent toutefois un rattachement administratif que le vocabulaire de l'indépendance ne suffit pas à masquer. L'article 38 prévoit que, lorsque la Commission délibère sur une question mettant en cause une administration, « les membres représentants du gouvernement » participent aux délibérations avec voix consultative, ce qui suppose une représentation gouvernementale au sein de l'organe. L'article 39 soumet son règlement intérieur à l'homologation du gouvernement. L'article 40 confie la nomination du secrétaire général au gouvernement, sur proposition du président, et fait de ce secrétaire général le sous-ordonnateur du budget de la Commission. L'article 41 compose enfin son personnel de fonctionnaires détachés des administrations et d'agents contractuels².

Le droit comparé éclaire la portée de ces choix. Le RGPD exige que chaque autorité de contrôle agisse en toute indépendance, dispose de son propre personnel et d'un budget annuel public distinct³. La Cour de justice a donné à cette exigence une portée rigoureuse. Elle a jugé que l'indépendance « totale » exclut toute tutelle de l'État, même destinée à garantir la légalité de l'action de l'autorité, puis elle a condamné l'Autriche parce que le membre gérant de son autorité de contrôle était un fonctionnaire fédéral, que le bureau de l'autorité était intégré aux services de la chancellerie fédérale et que le chancelier disposait d'un droit d'information inconditionnel sur ses activités⁴. La ressemblance avec l'architecture marocaine est frappante. L'argument n'est pas seulement européen. Le protocole additionnel à la Convention 108, que le Maroc a ratifié en même temps que la Convention, impose que les

¹ Loi n° 09-08, art. 27 et 32.

² Loi n° 09-08, art. 35 à 41. Le règlement intérieur de la CNDP a été approuvé par décision du Premier ministre n° 3-33-11.

³ RGPD, art. 52.

⁴ CJUE, gr. ch., 9 mars 2010, *Commission c. Allemagne*, aff. C-518/07 ; CJUE, gr. ch., 16 octobre 2012, *Commission c. Autriche*, aff. C-614/10.

autorités de contrôle exercent leurs fonctions « en toute indépendance »¹. Le Royaume s'est donc engagé, sur le plan international, à un standard que sa loi interne ne garantit pas pleinement.

La question du statut constitutionnel prolonge cette observation. La Constitution de 2011 a consacré, dans son titre XII, plusieurs instances de protection des droits et libertés et de bonne gouvernance, parmi lesquelles le Conseil national des droits de l'Homme, le Médiateur, la Haute autorité de la communication audiovisuelle ou le Conseil de la concurrence². La CNDP n'y figure pas, alors qu'elle a pour mission de mettre en œuvre le droit à la vie privée consacré par l'article 24. Son indépendance repose donc sur la seule loi ordinaire et sur la pratique de ses dirigeants. Le contraste avec le Conseil de la concurrence est saisissant. Les deux autorités interviennent auprès des mêmes acteurs du numérique et sur les mêmes masses de données. La première est constitutionnalisée et peut infliger des amendes atteignant 10 % du chiffre d'affaires³. La seconde n'a ni rang constitutionnel ni pouvoir d'amende.

Les pouvoirs de la CNDP sont en effet essentiellement des pouvoirs d'instruction et d'injonction. Elle peut enquêter, accéder aux locaux et aux données, se faire communiquer des documents, ordonner la rectification, le verrouillage, l'effacement ou la destruction de données et interdire provisoirement ou définitivement un traitement⁴. L'exercice de certains de ces pouvoirs est subordonné à une procédure contradictoire. Le pouvoir d'interdiction contient lui-même un angle mort territorial, puisque le texte vise les traitements opérés « à partir de serveurs situés sur le territoire national ». Quant au retrait du récépissé ou de l'autorisation, prévu par l'article 51, il ne peut intervenir que si le traitement « porte atteinte à la sûreté ou à l'ordre public ou est contraire à la morale et aux bonnes mœurs ». Ces critères sont étrangers à la logique de la protection des données. Un traitement qui méconnaît gravement les droits des personnes sans menacer l'ordre public ne peut, sur ce fondement, être privé de son titre. Surtout, la loi ne reconnaît à la Commission aucun pouvoir d'amende administrative. Les plaintes qu'elle reçoit débouchent, aux termes de l'article 28, sur la publication de rectificatifs ou sur la saisine du procureur du Roi. Ses agents assermentés peuvent constater les infractions par procès-verbal, qu'ils transmettent au parquet dans les cinq jours⁵. La CNDP fonctionne ainsi comme une autorité d'instruction placée en amont de la chaîne pénale. La création, en 2019, d'une unité spécialisée au sein de la présidence du

¹ Protocole additionnel à la Convention 108 concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), art. 1er, paragraphe 3.

² Constitution du Royaume du Maroc, titre XII, art. 161 à 170.

³ Constitution, art. 166 ; loi n° 20-13 relative au Conseil de la concurrence ; loi n° 104-12 relative à la liberté des prix et de la concurrence.

⁴ Loi n° 09-08, art. 28, 30 et 31.

⁵ Loi n° 09-08, art. 28, avant-dernier alinéa, art. 51 et art. 66.

ministère public pour recevoir et traiter les dossiers transmis par la Commission confirme ce choix institutionnel¹.

Les droits comparés ont généralement emprunté une autre voie. La CNIL peut, depuis le RGPD, prononcer des amendes atteignant 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial². Le Conseil d'État a confirmé, en 2020, l'amende de 50 millions d'euros infligée à Google en 2019 pour manquement aux obligations de transparence et de consentement³. Sur le continent africain, la loi sénégalaise de 2008 et la loi algérienne de 2018 ont également confié à leurs autorités de protection un pouvoir de sanction administrative incluant des sanctions pécuniaires⁴. Le choix marocain d'une répression exclusivement pénale n'est donc pas une fatalité régionale. Il résulte d'une conception de 2009 qui faisait de la Commission un organe de déclaration et de conseil plutôt qu'un régulateur de plein exercice.

2° Une régulation compensatoire par délibérations

Face à une loi immobile et à des pouvoirs bornés, la CNDP a construit, délibération après délibération, un corpus qui précise le droit applicable et parfois le prolonge. Ce corpus présente une grande variété. Certaines délibérations fixent le cadre de traitements sectoriels. La délibération n° 350-2013 du 31 mai 2013 a ainsi posé les conditions de la vidéosurveillance dans les lieux de travail et les lieux privés communs, en affirmant que les images recueillies constituent des données à caractère personnel et en imposant une déclaration préalable et une signalétique visible⁵. D'autres encadrent une technologie, comme le contrôle d'accès biométrique ou la reconnaissance faciale, dont il a déjà été question. D'autres encore portent avis sur des projets de textes, qu'il s'agisse des bureaux d'information sur le crédit, de l'administration numérique, du registre des bénéficiaires effectifs ou des règles relatives aux transferts de données⁶. D'autres enfin simplifient des procédures, comme

¹ CNDP, communiqué du 21 janvier 2019 relatif à la réunion du 17 janvier 2019 entre le président du ministère public et le président de la CNDP, en langue arabe.

² RGPD, art. 83, paragraphe 5.

³ CNIL, formation restreinte, délibération n° SAN-2019-001 du 21 janvier 2019 concernant la société Google LLC ; CE, 19 juin 2020, *Google LLC*, n° 430810.

⁴ Loi sénégalaise n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel ; loi algérienne n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.

⁵ CNDP, délibération n° 350-2013 du 31 mai 2013 relative aux conditions de la vidéosurveillance dans les lieux de travail et les lieux privés communs. Sur son contenu, v. les déclarations du ministre de la Justice rapportées par *Al3omk*, en langue arabe.

⁶ CNDP, délibérations n° D-170-2020, n° D-127-2020 et n° D-181-2021, préc. ; délibération n° D-02-2023 du 27 février 2023 portant avis sur le projet d'annexe relative aux règles sur le transfert des

celle applicable aux études de bioéquivalence¹. Depuis mars 2025, la Commission a ouvert des auditions publiques en vue de délibérations sur les traitements d'intelligence artificielle et sur la vidéosurveillance, en citant expressément les risques liés à la reconnaissance faciale dans l'espace public². Elle justifie cette dernière démarche par la nécessité de veiller à ce que la loi n° 09-08 soit « communément interprétée » par les acteurs concernés.

Cette formule résume la nature de l'entreprise. La CNDP régle par l'interprétation. Elle donne à des dispositions générales, conçues en 2009, un contenu adapté à des techniques que le législateur ne pouvait pas connaître. La démarche a des mérites évidents. Elle est souple, technique, précédée de consultations, et elle permet d'éviter le vide. Elle se heurte cependant à trois limites.

La première limite est juridique. La loi habilite la Commission à fixer certaines listes de traitements, sous réserve d'homologation gouvernementale, à délivrer ou refuser des autorisations et à soumettre à autorisation un traitement déclaré³. Elle ne l'habilite pas à édicter des règles générales de conduite, encore moins à suspendre l'usage d'une technologie. Le moratoire sur la reconnaissance faciale repose ainsi sur une politique de refus d'autorisation annoncée par avance, dont la nature juridique reste incertaine. À notre connaissance, aucune délibération de la CNDP n'a été soumise au contrôle du juge administratif. Le droit français montre pourtant que ce contrôle est possible et qu'il peut être sévère. Le Conseil d'État a d'abord admis le recours contre les actes de droit souple des autorités de régulation lorsqu'ils sont de nature à produire des effets notables, avant d'étendre ce contrôle aux documents de portée générale émanant des autorités publiques⁴. Saisi des lignes directrices de la CNIL relatives aux témoins de connexion, il a annulé la disposition qui posait une interdiction générale et absolue des « murs de cookies », au motif qu'une telle interdiction excédait ce que l'autorité pouvait légalement prescrire par un acte de droit souple⁵. La leçon vaut pour le Maroc. Les initiatives les plus protectrices de la CNDP reposent sur les fondements textuels les plus étroits, et elles seraient les plus exposées à une censure si elles étaient contestées.

données ; délibération n° D-110-2021 du 30 avril 2021 portant avis sur un projet de directive fixant des règles minimales.

¹ CNDP, délibération n° D-03-2023 du 17 mars 2023 relative à la simplification de la procédure de notification des études de bioéquivalence.

² Sur l'intelligence artificielle, v. *Médias24*, 19 mars 2025, préc. Sur la vidéosurveillance, v. « Vidéosurveillance, la CNDP ouvre des auditions pour mieux encadrer la protection de la vie privée », *Le Matin*, 22 mars 2025.

³ Loi n° 09-08, art. 16 à 18, 20 et 28.

⁴ CE, ass., 21 mars 2016, *Société Fairvesta International GmbH e.a.*, n° 368082 ; CE, sect., 12 juin 2020, *GISTI*, n° 418142.

⁵ CE, 19 juin 2020, *Association des agences-conseils en communication e.a.*, n° 434684.

La deuxième limite tient aux destinataires de cette régulation. La délibération, la convention « Data-Tika », la réunion sectorielle avec une profession atteignent ceux qui acceptent de dialoguer avec la Commission. Elles n'atteignent guère ceux qui l'ignorent. Elles ne touchent pas davantage l'État agissant dans les domaines exclus du champ de la loi, comme en témoignent les interrogations suscitées par le déploiement de caméras dans les grandes villes¹. Elles ne touchent pas non plus les plateformes étrangères, que seule la lettre conjointe de 2023 a tenté d'interpeller. La régulation par délibérations éclaire donc surtout la partie de la route déjà visible.

La troisième limite tient à la sécurité juridique. Les délibérations sont dispersées, rarement consolidées, parfois difficiles d'accès. Leur portée dépend en partie des orientations de la direction de la Commission, dont le président se décrit lui-même comme une « conscience morale » chargée d'alerter contre les mauvais usages des données². L'expression est révélatrice. Elle décrit une magistrature d'influence, utile et respectée, mais qui ne remplace pas une autorité dotée de pouvoirs juridiques précis et soumise à un contrôle juridictionnel clair. La CNDP voit les manquements. Son regard ne se convertit en sanction que par l'intermédiaire d'autres institutions, au premier rang desquelles le juge.

B. Les angles morts du contentieux

Le législateur de 2009 a ouvert deux voies contentieuses. La voie pénale occupe l'essentiel du chapitre VII de la loi, qui énumère de nombreuses incriminations. La voie civile n'est mentionnée qu'en passant, l'article 52 réservant la responsabilité civile à l'égard des personnes ayant subi un dommage du fait de l'infraction. La première se révèle peu dissuasive (1°). La seconde laisse la personne concernée sans réparation effective (2°).

1° Un arsenal répressif peu dissuasif

L'arsenal pénal de la loi est fourni. La mise en œuvre d'un traitement sans déclaration ou sans autorisation est punie d'une amende de 10 000 à 100 000 dirhams. Le refus des droits d'accès, de rectification ou d'opposition est puni d'une amende de 20 000 à 200 000 dirhams par infraction. La collecte déloyale, le détournement de finalité, la conservation excessive, le traitement sans base légale, le défaut de sécurité, le traitement malgré une opposition légitime, le transfert irrégulier et la négligence ayant facilité un usage abusif sont punis d'un emprisonnement de trois mois à un an et d'une amende de 20 000 à 200 000 dirhams, ou de l'une de ces peines. Le traitement de données sensibles sans consentement exprès est puni d'une amende portée à 300 000 dirhams. L'entrave à l'action de la CNDP et le refus d'appliquer ses décisions sont également réprimés. Les amendes sont doublées lorsque l'auteur est une personne morale, qui encourt en outre la confiscation ou la fermeture d'établissement, et elles le sont encore en cas de récidive³.

¹ « Vidéosurveillance et reconnaissance faciale, que peut réellement la CNDP face aux impératifs sécuritaires ? », *Le Desk*, 24 mars 2025.

² Entretien précité, *Finances News Hebdo*, 4 août 2026.

³ Loi n° 09-08, art. 52 à 65.

L'énumération impressionne davantage que le dispositif ne dissuade. Pour une personne morale, l'amende maximale encourue pour l'infraction la plus grave s'élève, hors récidive, à 600 000 dirhams. Fixé en 2009 et jamais réévalué, ce montant est sans rapport avec le chiffre d'affaires d'un opérateur de télécommunications, d'une banque ou d'une plateforme. Le doublement forfaitaire prévu pour les personnes morales ne corrige pas cette disproportion, puisqu'il ne tient aucun compte de la taille de l'entreprise. Le barème produit ainsi une proportionnalité inversée. Il pèse sur la petite structure et reste indolore pour le grand groupe, alors que c'est ce dernier qui traite le plus de données et qui en tire le plus de profit.

La nature pénale de la répression ajoute ses propres contraintes. Le principe de légalité impose une interprétation stricte des incriminations¹. Or ces incriminations ont été rédigées pour des opérations sur des fichiers, et des pratiques comme l'extraction massive de données publiquement accessibles, l'inférence d'informations sensibles ou le profilage s'y laissent difficilement ramener. Le parquet apprécie par ailleurs l'opportunité des poursuites, de sorte que le sort d'un procès-verbal de la CNDP dépend de priorités de politique pénale qui ne sont pas les siennes. La lecture des incriminations révèle enfin une asymétrie instructive. Le refus de faire connaître la logique d'un traitement automatisé, qui relève du droit d'accès de l'article 7, est pénalement sanctionné par l'article 53. La violation de l'article 11, qui interdit les décisions fondées sur le seul profilage, ne fait l'objet d'aucune incrimination spécifique. La loi punit donc le silence sur l'algorithme, mais pas la décision prise par l'algorithme. Ce droit à l'explication pénalement protégé, remarquable sur le papier, n'a d'ailleurs, à notre connaissance, jamais donné lieu à poursuites.

La pratique confirme ces observations. Selon le président délégué du Conseil supérieur du pouvoir judiciaire, les 153 affaires jugées en 2024 portaient principalement sur des traitements sans déclaration ou sans autorisation, sur le refus de respecter les droits des personnes et sur la conservation des données au-delà de la durée autorisée². La répression reflète fidèlement le formalisme de la loi. Elle saisit d'abord l'absence de formalité, le manquement le plus facile à établir, et beaucoup moins les atteintes de fond.

La loi n° 09-08 subit en outre la concurrence d'autres textes répressifs. Les articles 447-1 à 447-3 du Code pénal, issus de la loi n° 103-13 relative à la lutte contre les violences faites aux femmes, répriment la captation et la diffusion de paroles ou d'images sans le consentement des intéressés³. Les articles 607-3 et suivants du même code, issus de la loi n° 07-03, répriment les atteintes aux systèmes de traitement automatisé des données⁴. Une

¹ Code pénal, art. 3.

² *Hespress FR*, 28 janvier 2025, préc.

³ Code pénal, art. 447-1 à 447-3, issus de la loi n° 103-13 relative à la lutte contre les violences faites aux femmes, promulguée en 2018.

⁴ Code pénal, art. 607-3 à 607-11, issus de la loi n° 07-03 complétant le Code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données.

étude consacrée à la jurisprudence marocaine en la matière observe que les juridictions recourent plus volontiers au Code pénal et au Dahir des obligations et des contrats qu'à la loi n° 09-08 elle-même¹. La loi spéciale se trouve ainsi marginalisée dans son propre domaine. L'affaire de la Caisse nationale de sécurité sociale en offre une illustration. La réaction institutionnelle s'est tournée vers les auteurs de l'intrusion et vers ceux qui consulteraient ou diffuseraient les données fuitées, bien plus que vers l'appréciation des mesures de sécurité du responsable du traitement². La répression regarde vers l'aval de la fuite, rarement vers son amont.

Le droit français enseigne à cet égard une leçon utile. La loi de 1978 a toujours été assortie de sanctions pénales, aujourd'hui inscrites aux articles 226-16 et suivants du Code pénal³. Ces dispositions sont restées d'application rare. C'est le pouvoir de sanction administrative de la CNIL, renforcé par le RGPD, qui a donné à la protection des données son effectivité. La voie pénale convient à la répression des comportements frauduleux. Elle se prête mal à la régulation continue de la conformité des organisations.

2° Une personne concernée sans réparation effective

La réparation du dommage causé par un traitement illicite relève du droit commun de la responsabilité civile. Les articles 77 et 78 du Dahir des obligations et des contrats engagent la responsabilité de celui qui cause à autrui un dommage matériel ou moral par son fait ou par sa faute. L'article 79 retient la responsabilité de l'État et des collectivités pour les dommages causés directement par le fonctionnement de leurs administrations et par les fautes de service de leurs agents⁴. La personne concernée doit donc établir une faute, un dommage et un lien de causalité.

La jurisprudence montre que cette voie n'est pas fermée. Dans l'affaire déjà évoquée, le tribunal de première instance avait ordonné le retrait des caméras et alloué une indemnité au locataire. La cour d'appel avait confirmé le jugement en se fondant sur la loi n° 09-08, notamment sur l'obligation d'informer les personnes par une signalétique apparente, et la Cour de cassation a rejeté le pourvoi⁵. La décision est importante au-delà de ses faits. Elle montre que la loi spéciale peut servir d'étalon de la faute civile et qu'un manquement à ses prescriptions caractérise le fait illicite au sens du droit commun. Le président délégué du Conseil supérieur du pouvoir judiciaire a cité, dans le même sens, des décisions relatives à

¹ A. Gaagouch, « The protection of personal data according to the civil and criminal Moroccan laws in light of jurisprudence », *Journal of Data Protection & Privacy*, Henry Stewart Publications. L'auteur, magistrat au tribunal de commerce, s'appuie sur plus de vingt-huit décisions.

² V. le communiqué de la CNDP du 10 avril 2025, préc., qui rappelle que la consultation, la détention ou la diffusion des données issues de la fuite sont illicites.

³ Code pénal français, art. 226-16 à 226-24.

⁴ Dahir du 9 ramadan 1331 (12 août 1913) formant Code des obligations et des contrats, art. 77 à 79.

⁵ Cour de cassation, arrêt n° 1870 du 16 avril 2024, préc.

l'utilisation de l'image d'une personne sans son consentement ou au traitement erroné des données d'un client par une banque¹.

Cette voie reste pourtant inadaptée aux atteintes typiques du monde numérique, pour trois raisons. La première tient à la structure du dommage. L'atteinte aux données est souvent immatérielle, modeste à l'échelle de chaque individu et massive à l'échelle du groupe. Lorsque deux millions de personnes voient leurs données exposées, aucune d'elles n'a intérêt à engager seule un procès dont le coût excède l'indemnité espérée. Cette apathie rationnelle assure l'impunité civile des atteintes de masse. La deuxième tient à la causalité. Après une fuite, les victimes subissent des tentatives d'hameçonnage dont l'origine reste incertaine, faute de pouvoir rattacher avec certitude l'escroquerie à telle ou telle base compromise. La presse a ainsi rapporté, en avril 2025, des vagues de fraude visant des clients bancaires sans que l'on sache si elles procédaient de la fuite de la CNSS ou d'une autre source². La troisième tient à la preuve de la faute. La victime n'a aucun accès au système d'information du responsable et ne peut démontrer l'insuffisance de ses mesures de sécurité. Le droit de l'Union a résolu ces difficultés par des règles précises. La Cour de justice a jugé que la seule violation du règlement ne suffit pas à ouvrir droit à réparation, mais qu'aucun seuil de gravité ne peut être exigé pour le dommage moral³. Elle a ajouté que la crainte d'un usage abusif des données après une cyberattaque peut constituer un tel dommage, et que la charge de prouver le caractère approprié des mesures de sécurité pèse sur le responsable⁴. Le droit marocain reconnaît le dommage moral, mais il ne contient aucune règle comparable sur la preuve. La personne supporte l'essentiel des difficultés probatoires.

La dimension collective du contentieux fait également défaut. Le droit marocain ne connaît pas d'action de groupe en matière de données personnelles, et le contentieux reste dominé par les plaintes pénales individuelles⁵. La loi n° 31-08 relative à la protection du consommateur permet certes aux associations de consommateurs reconnues d'utilité publique d'agir pour la défense de l'intérêt collectif des consommateurs⁶. Son champ est toutefois limité aux relations de consommation. Il laisse hors de portée les traitements opérés par les employeurs, par les organismes de sécurité sociale ou par les administrations. L'Union européenne a choisi une autre voie. Le RGPD permet aux personnes de mandater un organisme à but non lucratif pour agir en leur nom, et la Cour de justice a admis qu'une

¹ *Hespress FR*, 28 janvier 2025, préc.

² « Après la CNSS, les banques ciblées, les Marocains piégés par des arnaques en série ? », *Hespress FR*, 17 avril 2025.

³ CJUE, 4 mai 2023, *UI c. Österreichische Post*, aff. C-300/21.

⁴ CJUE, 14 décembre 2023, *VB c. Natsionalna agentsia za prihodite*, aff. C-340/21, préc.

⁵ V. en ce sens *Chambers Global Practice Guides*, « Data Protection & Privacy 2025, Morocco ».

⁶ Loi n° 31-08 édictant des mesures de protection du consommateur.

association de consommateurs puisse agir même sans mandat¹. En France, l'action de groupe en matière de données personnelles existe depuis 2016 et peut tendre à la réparation des préjudices depuis 2018². La procédure de plainte devant la CNDP ne comble pas ce vide. La Commission s'est déclarée prête à recevoir les plaintes des victimes de la fuite de la CNSS, mais elle ne peut allouer aucune indemnité.

Lorsque le responsable du traitement est une personne publique, la réparation relève des juridictions administratives, compétentes pour connaître des actions en réparation des dommages causés par les actes et les activités des personnes publiques³. Le régime de responsabilité fondé sur le fonctionnement des services, que consacre l'article 79 du Dahir des obligations et des contrats, pourrait offrir aux victimes de fuites de données publiques un fondement plus favorable que la faute prouvée. Cette piste n'a, à notre connaissance, pas encore été explorée devant le juge administratif.

Au terme de ce parcours, la personne concernée apparaît comme la grande absente du dispositif contentieux. Elle n'est pas informée des violations qui l'atteignent, elle ne peut agir collectivement et elle ne peut obtenir réparation auprès de l'autorité de contrôle. La loi la protège comme un objet de protection plus qu'elle ne l'arme comme un acteur de sa propre protection. C'est peut-être là le plus profond de ses angles morts. Elle voit les données, elle voit moins les personnes qui se trouvent derrière.

Conclusion

Les angles morts de la loi n° 09-08 ne sont pas des défauts isolés qu'il suffirait de corriger un à un. Ils forment un système, et c'est sans doute le principal enseignement de cette étude. Le formalisme des obligations nourrit une répression elle-même formelle, qui saisit l'absence de déclaration plus volontiers que l'atteinte aux droits. Les exclusions qui éloignent l'État du droit commun de la protection font écho au statut d'une autorité de contrôle instituée auprès du Chef du gouvernement et privée de pouvoir d'amende. Les droits que la loi reconnaît face aux traitements automatisés demeurent virtuels, faute d'un régulateur capable de sanctionner et d'un juge régulièrement saisi. L'insuffisance du champ territorial, enfin, réduit l'action de la CNDP envers les grandes plateformes à des démarches diplomatiques. Chaque angle mort renforce les autres. Corriger l'un sans les autres reviendrait à déplacer la zone d'ombre plutôt qu'à la réduire.

¹ RGPD, art. 80 ; CJUE, 28 avril 2022, *Meta Platforms Ireland c. Bundesverband der Verbraucherzentralen*, aff. C-319/20. Adde directive (UE) 2020/1828 du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs.

² Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXI^e siècle ; loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

³ Loi n° 41-90 instituant des tribunaux administratifs, art. 8.

Bibliographie

Textes

Constitution du Royaume du Maroc, dahir n° 1-11-91 du 29 juillet 2011.

Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, dahir n° 1-09-15 du 18 février 2009, B.O. n° 5714 du 5 mars 2009.

Décret n° 2-09-165 du 21 mai 2009 pris pour l'application de la loi n° 09-08.

Loi n° 05-20 relative à la cybersécurité et décret n° 2-21-406 du 15 juillet 2021.

Loi n° 72-18 relative au dispositif de ciblage des bénéficiaires des programmes d'appui social et portant création de l'Agence nationale des registres.

Loi n° 31-08 édictant des mesures de protection du consommateur.

Loi n° 104-12 relative à la liberté des prix et de la concurrence ; loi n° 20-13 relative au Conseil de la concurrence.

Code pénal, art. 3, 447-1 à 447-3 et 607-3 à 607-11 ; Dahir formant Code des obligations et des contrats, art. 77 à 79.

Directive 95/46/CE du 24 octobre 1995 ; règlement (UE) 2016/679 du 27 avril 2016 ; directive (UE) 2016/680 du 27 avril 2016 ; directive (UE) 2020/1828 du 25 novembre 2020 ; règlement (UE) 2024/1689 du 13 juin 2024.

Loi française n° 78-17 du 6 janvier 1978 modifiée ; loi n° 2016-1321 du 7 octobre 2016 ; loi n° 2016-1547 du 18 novembre 2016 ; loi n° 2018-493 du 20 juin 2018.

Délibérations et documents de la CNDP

Délibération n° 350-2013 du 31 mai 2013 (vidéosurveillance dans les lieux de travail et les lieux privés communs).

Délibération n° 478-2013 (contrôle d'accès par biométrie).

Délibération n° D-194-2019 du 30 août 2019 et délibération n° D-97-2020 du 26 mars 2020 (moratoire sur la reconnaissance faciale).

Délibérations n° D-108-EUS/2020 du 23 avril 2020 et n° D-126-EUS/2020 du 29 juillet 2020 (usages encadrés de la reconnaissance faciale).

Délibérations n° D-127-2020, n° D-170-2020 du 19 octobre 2020, n° D-110-2021 du 30 avril 2021, n° D-181-2021, n° D-02-2023 du 27 février 2023 et n° D-03-2023 du 17 mars 2023.

Communiqués du 21 janvier 2019, du 24 août 2023, du 18 mars 2025 et du 10 avril 2025.

Doctrine

F. Bensghir, « La justice algorithmique en droit marocain. Commentaire des articles 7 et 11 de la loi n° 09-08 », Maroclaw, en langue arabe.

J. Carbonnier, « Effectivité et ineffectivité de la règle de droit », L'Année sociologique, 1957-1958.

A. Gaagouch, « The protection of personal data according to the civil and criminal Moroccan laws in light of jurisprudence », Journal of Data Protection & Privacy.

P. Legrand, « The Impossibility of "Legal Transplants" », Maastricht Journal of European and Comparative Law, vol. 4, 1997, p. 111.

Ch. Perelman (dir.), Le problème des lacunes en droit, Bruxelles, Bruylant, 1968.

D. J. Solove, « Privacy Self-Management and the Consent Dilemma », Harvard Law Review, vol. 126, 2013, p. 1880.