



LA PROTECTION JURIDIQUE DES DONNÉES PERSONNELLES DANS L'ESPACE NUMÉRIQUE : ENTRE VULNÉRABILITÉ ACCRUE ET RÉPONSES NORMATIVES – ÉTUDE COMPARÉE DES APPROCHES ALGÉRIENNE ET EUROPÉENNE

Legal Protection of Personal Data in the Digital Space: Between Increased Vulnerability and Normative Responses – A Comparative Study of Algerian and European Approaches



Dr. Ould Mohamed Mohand Cherif^{1*}
University of Benyoucef Benkhedda, Algérie¹.

Date de soumission: 18/08/2025 Date d'acceptation: 06/10/2025 Date de publication: 30/12/2025



Résumé: Afin d'assurer la protection des données à caractère personnel, les instances normatives ont instauré un ensemble de règles encadrant la collecte, l'utilisation et la conservation des informations relatives à une personne. Cette protection revêt une importance croissante, car la numérisation accrue renforce l'exposition de ces données et multiplie les risques d'atteinte à la vie privée. Dans ce contexte, la présente étude propose une analyse comparée des cadres juridiques algérien et européen y afférents, qui, bien que convergents sur certains principes, diffèrent puisque le premier cadre repose sur une logique de formalité et le second sur le principe de responsabilisation continue.

Mots-clés: Données personnelles - RGPD - ANPDP ; *Accountability - Privacy by design*.

الحماية القانونية للبيانات الشخصية في الفضاء الرقمي: بين تصاعد المخاطر والاستجابات
القانونية – دراسة مقارنة بين النموذجين الجزائري والأوروبي

ملخص: من أجل ضمان حماية البيانات ذات الطابع الشخصي، أقرت الجهات المختصة مجموعة من القواعد التي تنظم حماية المعطيات ذات الطبع الشخصي ببيان شروط معالجتها واستخدامها والاحتفاظ بها. وتكتسي هذه الحماية أهمية متزايدة، إذ إن الرقمنة المتزايدة تعزز انكشاف هذه البيانات وتضاعف مخاطر المساس بالخصوصية. وفي هذا السياق، تقدم هذه الدراسة تحليلاً مقارناً للأطر القانونية الجزائرية



والأوروبي ذات الصلة، والتي، وإن تلاققت في بعض المبادئ، فإنها تختلف من حيث إن الأول يقوم على منطق الشكليات، بينما يقوم الثاني على مبدأ المساواة المستمرة.

الكلمات المفتاحية: المعطيات ذات الطابع الشخصي، اللائحة العامة لحماية البيانات الشخصية، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، مبدأ المسؤولية، الخصوصية بحكم التصميم.

Legal Protection of Personal Data in the Digital Space: Between Increased Vulnerability and Normative Responses – A Comparative Study of Algerian and European Approaches

Abstract: In order to ensure the protection of personal data, normative bodies have established a set of rules governing the collection, use, and retention of information relating to an individual. This protection is of growing importance, as increased digitization heightens the exposure of such data and multiplies the risks of infringements on privacy. In this context, the present study offers a comparative analysis of the Algerian and European legal frameworks in this regard, which, although converging on certain principles, differ in that the former is based on a formalistic approach while the latter is founded on the principle of continuous accountability.

Key words: Personal data – GDPR – ANPDP – Accountability - Privacy by design.



Introduction :

L'ère numérique dans laquelle nous évoluons voit se déployer, à une vitesse sans précédent, des moyens de collecte d'informations personnelles toujours plus puissants, diffus et souvent invisibles. Portée par la généralisation des objets connectés, l'intelligence artificielle et les applications mobiles, cette révolution technique transforme notre environnement quotidien en un vaste réseau de « capteurs ». Téléphones, montres, véhicules, enceintes vocales ou simples plateformes numériques : tous génèrent en continu des données relatives aux comportements, préférences, déplacements, voire à l'état de santé des individus. Ce maillage informationnel, souvent ignoré des utilisateurs eux-mêmes, rend la collecte de données à la fois massive et permanente, soulevant de profondes interrogations quant à la maîtrise que chacun conserve sur sa vie privée. La banalisation de ces technologies fait de ce fait émerger un enjeu central : celui de la protection des données personnelles dans un monde où leur captation est devenue quasiment inévitable¹.

Devenues omniprésentes, les données personnelles ne sont plus de simples traces numériques, mais de véritables leviers économiques d'une puissance considérable. Leur traitement, souvent sophistiqué, permet aux entreprises de construire une connaissance fine, voire intime des individus, ouvrant la voie à des stratégies commerciales d'une efficacité redoutable : ciblage comportemental, profilage algorithmique, tarification différenciée, etc. Ces pratiques reposent fréquemment sur l'analyse croisée de données parfois collectées à l'insu des personnes concernées. Ce capital informationnel, difficile à quantifier mais crucial pour la compétitivité des plateformes numériques, a donné naissance à de nouveaux marchés structurés autour de la circulation, du courtage et de la valorisation des données. Ainsi, les données personnelles deviennent un actif stratégique disputé, au cœur d'un écosystème numérique mondialisé dans lequel la logique économique tend à prévaloir sur les exigences éthiques et les garanties juridiques². Ce rôle central dans l'économie numérique leur a d'ailleurs valu d'être qualifiées de véritables « carburant du Net »³.

¹ LANNA Maximilien, « Objets connectés et protection des données à caractère personnel : vers un changement de paradigme des modalités de protection », *Droits*, n° 68, 2019, pp 223-235.

² CECERE Grazia, MANANT Mathieu, « Vie privée, valeur des données personnelles et régulation, *Annales des mines – Enjeux numérique*, » n° 2, 2018, pp 14-19. BONICHOT



Toutefois, leur importance ne se limite pas à la seule sphère économique. Les révélations d'Edward Snowden, ancien agent de la *National Security Agency* (NSA), ont mis en lumière l'existence de dispositifs massifs de surveillance et de collecte de données personnelles opérés par cet organisme étatique étasunien, en collaboration avec les géants technologiques américains — les GAFAM (Google, Apple, Facebook, Amazon, Microsoft). Ces révélations ont montré que les données personnelles revêtent également une dimension stratégique et politique, en raison de leur rôle dans les questions de sécurité, de contrôle social et de souveraineté numérique⁴.

Cette importance stratégique, conjuguée au basculement vers une économie de la donnée confère à la protection juridique des informations personnelles une portée nouvelle, qui dépasse le strict cadre de la vie privée. À mesure que les technologies numériques modèlent les comportements et les rapports sociaux, la capacité à maîtriser ses données devient une condition concrète de l'autonomie individuelle. Dès lors, la régulation de ces flux informationnels ne peut plus être pensée comme un simple impératif technique, mais bien comme un enjeu structurel de gouvernance démocratique et de protection des droits fondamentaux. C'est dans cette perspective que se justifie une analyse approfondie des cadres juridiques en présence.

Longtemps centrée sur les risques d'ingérence des autorités publiques⁵, l'attention dans la protection des données personnelles s'est progressivement déplacée vers les pratiques des acteurs privés, désormais premiers collecteurs et exploitants de l'information personnelle. L'évolution rapide des modes de traitement et de circulation des données impose aujourd'hui de repenser les mécanismes de régulation, dans une logique de transparence et de renforcement des droits fondamentaux.

Jean Claude, « Données personnelles : l'invention européenne d'un nouveau monde », Pouvoirs, n°185, 2023, pp 97-109.

³ GALUSTIAN Gohar, « La protection des données personnelles à l'épreuve du numérique », Revue de droit public n°05, 2018, p 1391.

⁴ PEYROU Sylvie, « La protection des données à caractère personnel au sein de l'UE : des enjeux économiques et sécuritaires encadré par le législateur sous le contrôle du juge », Revue de droit public, n°1, 2015, p 58.

⁵ DEBIÈS Élise, « Big data de santé et autodétermination informationnelle : quelles articulations possibles pour une innovation protectrice des données personnelles ? » Revue française d'administration publique, n° 167, 2018, pp 570-573.



Dans ce contexte, le principe de confidentialité des données personnelles a été élevé au rang de droit fondamental dans de nombreux systèmes juridiques. C'est notamment le cas de l'Algérie, dont l'article 47 alinéa 4 de la Constitution dispose que « *la protection des personnes dans le traitement des données à caractère personnel est un droit fondamental*⁶. » De manière convergente, la Cour de justice de l'Union européenne reconnaît le droit à l'autodétermination informationnelle comme un principe à valeur constitutionnelle. Ce concept consacre la faculté pour chaque individu de contrôler l'usage et le traitement de ses données personnelles, en tant qu'expression directe de sa liberté et de sa dignité⁷.

La loi n° 18-07 du 10 juin 2018⁸, modifiée et complétée par la loi n° 25-11 du 24 juillet 2025⁹ constitue une tentative par le législateur algérien de structurer juridiquement le traitement des données personnelles. Définies à l'article 3 comme « *toute information, quelle qu'en soit la forme, concernant une personne identifiée ou identifiable* », ces données sont placées sous la protection de principes tels que la licéité, la finalité et la proportionnalité.

L'essor fulgurant des technologies numériques, tel qu'observé, rend d'autant plus pressante la nécessité d'un cadre juridique adapté. En accentuant les risques d'atteinte à la vie privée, ces technologies révèlent les limites des dispositifs législatifs et réglementaires existants. Dans ce contexte, une mise en regard du droit algérien avec des cadres plus aboutis, en particulier celui de l'Union européenne où le Règlement général sur la protection des données (RGPD)¹⁰, fondé sur la responsabilisation et la transparence, fait figure de référence, s'impose pour évaluer la portée et les limites du dispositif.

⁶ Décret présidentiel n° 20-442 du 30/12/2020 relatif à la promulgation au journal officiel de la république algérienne démocratique et populaire de la révision constitutionnelle, adoptée par le référendum du 1^{er} novembre 2020, JORA n° 82, publié le 30/12/2020.

⁷ DEBIÈS Élise, *op. cit.*, pp 570-573.

⁸ Loi n° 18-07 du 10 juin 2018, Relative à la protection des personnes physiques dans le traitement des données à caractère personnel, JORA n° 34, publié le 10/06/2018.

⁹ Loi 25-11 du 24 juillet 2025 modifiant et complétant la loi 18-07, Relative à la protection des personnes physiques dans le traitement des données à caractère personnel, JORA n° 48, publié le 24 juillet 2025.

¹⁰ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).



Dans ce contexte, l'intérêt de cette étude n'est pas seulement de décrire les règles en vigueur, mais d'apprécier leur portée réelle. L'évolution récente du cadre algérien invite ainsi à interroger sa capacité à offrir une protection effective des données personnelles, tout en mettant en lumière ses rapprochements et ses écarts avec le modèle européen. C'est à cette double perspective que s'attache cette analyse, en examinant, d'une part, les mesures visant à prévenir en amont les atteintes aux données à caractère personnel (Chapitre I) et, d'autre part, l'effectivité des mécanismes de contrôle et de sanction (Chapitre II).

CHAPITRE I :

La protection préventive des données personnelles : centralisation administrative en Algérie et responsabilisation en Europe

Une protection véritablement efficace des données à caractère personnel suppose, en amont, l'édification d'un cadre normatif minutieusement calibré qui anticipe et encadre chaque opération de collecte, de conservation et d'exploitation des informations relatives aux individus. Dans cette optique, les législateurs et régulateurs ont mis en place des mécanismes préventifs combinant, d'une part, des règles de conformité substantielles et procédurales imposées aux responsables de traitement des données et, d'autre part, l'action vigilante d'autorités de contrôle dotées de pouvoirs d'enquête et de sanction.

Toutefois, la portée concrète et l'organisation institutionnelle de ces dispositifs diffèrent sensiblement selon les systèmes juridiques. Tandis que le modèle algérien, hérité d'une tradition de contrôle administratif préalable, privilégie une approche centralisée et formaliste, fondée sur des procédures déclaratives ou sur des autorisations préalables (Section 01), la réglementation européenne – incarnée par le RGPD – repose sur une logique de responsabilisation continue et de transparence active : tenue de registres internes, analyses d'impact, désignation d'un délégué à la protection des données et notification obligatoire des violations, autant d'obligations dont la preuve doit être démontrée en permanence sous le contrôle *ex post* des autorités compétentes (Section 02).

SECTION 1 : L'approche préventive algérienne : une régulation centralisée à portée limitée

Étant donné que la pratique en droit comparé a mis en évidence l'insuffisance des seules dispositions répressives pour encadrer efficacement le « marché des données personnelles » en particulier dans l'environnement numérique, le législateur algérien devait opter pour une approche combinant régulation et contrôle institutionnel. À cet



effet, il a créé une autorité administrative indépendante, placée auprès du Président de la République, dotée de la personnalité morale et de l'autonomie financière, chargée en particulier de veiller au respect des dispositions de la loi n° 18-07 et appelée dans le texte « L'Autorité nationale de protection des données à caractère personnel. (ANPDP). »

L'article 25 de ladite loi confère un large éventail de missions à cet organe, visant non seulement à contrôler, mais également à accompagner, conseiller et encadrer les différents acteurs impliqués dans le traitement des données. Cette autorité est ainsi habilitée à délivrer des autorisations, à recevoir les déclarations et les réclamations, à ordonner la modification ou la suppression de données, ainsi qu'à élaborer des règles de bonne conduite applicables aux traitements des données à caractère personnel¹¹.

La loi n° 25-11 du 24 juillet 2025 modifiant la loi n° 18-07 renforce l'architecture de cette autorité en instituant des pôles régionaux chargés du contrôle et de l'audit (article 27 bis). Ce maillage vise à rapprocher la supervision des lieux de traitement, à accélérer les vérifications sur pièces et sur place, et à améliorer la prise en charge des réclamations.

Dans le cadre de ses missions, l'Autorité nationale est également chargée de mettre en œuvre des mécanismes à portée préventive, fondés sur le contrôle préalable des traitements et sur la sécurité des données. À ce titre, les articles 12 à 18 de la loi instituent un régime de formalités qui impose au responsable de traitement de soumettre, selon la nature des opérations envisagées, soit une déclaration, soit une demande d'autorisation, avant toute mise en œuvre. Ce contrôle en amont vise à s'assurer que les traitements projetés respectent les exigences légales, renforçant ainsi le rôle central de l'Autorité dans la régulation du traitement des données personnelles¹².

À la suite de sa modification par la loi n° 25-11, la loi n° 18-07 impose également, en vertu de son article 41 bis 2, à chaque responsable du traitement – ainsi qu'à son sous-traitant, le cas échéant – l'obligation de tenir un registre des activités de traitement. Ce registre, qui doit être documenté, tenu à jour et accessible à l'Autorité, consigne a minima les finalités poursuivies, les catégories de données et de personnes concernées, les destinataires envisagés, ainsi que les mesures de sécurité appliquées.

¹¹قونان كهينة، حمليلى نواره، " السلطة الوطنية كهينة مكلفة برقابة احترام تطبيق قانون حماية المعطيات الشخصية رقم 18-07"، مجلة الدراسات القانونية، المجلد 07، العدد 02، 2021، ص ص 563-572.

¹² نفس المرجع، ص ص 569-572.



Il s'érige ainsi en outil structurant de gouvernance interne et de démonstration de conformité, en complément des formalités préalables exigées par la loi.

Ce dispositif est renforcé par la tenue d'un carnet automatisé des opérations, prévue à l'article 41 bis 3, retraçant les principales actions réalisées sur les données – telles que la consultation, la modification, la suppression ou la diffusion – assorties d'un horodatage et de l'identification de l'utilisateur ou du destinataire. Ce mécanisme de traçabilité continue joue un rôle décisif dans la détection des incidents, la reconstitution des chaînes techniques et la démonstration ex post du respect des obligations légales.

Sur le plan organisationnel, la réforme introduit de surcroît l'obligation de désigner un délégué à la protection des données (DPD) pour tout responsable du traitement ainsi que pour les autorités compétentes sauf exception légale. Ce délégué, dont les coordonnées sont communiquées à l'Autorité, exerce des missions d'information, de conseil et de contrôle quant au respect des dispositions légales et des politiques internes. Il participe, en outre, à la sensibilisation et à la formation du personnel concerné, et veille à la conduite des analyses d'impact prévues aux articles 41 bis et 41 bis 1.

Ces exigences de gouvernance documentaire et organisationnelle se complètent avec les mesures de sécurité prévues aux articles 38 et 39, qui encadrent la confidentialité, l'intégrité et la disponibilité des données : l'article 38 impose au responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles nécessaires pour garantir la sécurité, la confidentialité et l'intégrité des données, en particulier contre toute perte ou accès non autorisé¹³. L'article 39 ajoute que ces mesures doivent être adaptées à la nature des données et aux risques que leur traitement comporte¹⁴. En articulation avec les mesures de sécurité, ces

¹³ L'article 38 de la loi n° 18-07 dispose : « *Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.*

Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. »

¹⁴ L'article 39 de la loi n° 18-07 dispose : « *Lorsque le traitement est effectué pour le compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes inhérentes aux mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et doit veiller au respect de ces mesures.*



instruments de gouvernance structurent la preuve interne de conformité et facilitent la maîtrise des risques opérationnels.

La réforme de juillet 2025 précise le champ d'application de la loi en excluant les traitements relatifs à la défense et à la sécurité nationales (article 6 modifié). Il ne s'agit pas d'ériger une zone de non-droit : cette délimitation matérielle vise à la sauvegarde d'intérêts régaliens soumis à des règles spécifiques de confidentialité et de classification. Hors de ce périmètre réservé ou de toute autre exception légalement affirmée, les autorités et organismes publics demeurent pleinement tenus par les obligations de conformité prévues par la loi, sous le contrôle de l'Autorité.

Outre la création de l'autorité nationale de protection des données à caractère personnel, la loi n° 18-07 prévoit un ensemble de garanties visant à encadrer le traitement des données personnelles en amont et à limiter les risques d'atteinte à la vie privée. L'article 7 s'inscrit à cet égard comme une disposition importante, en érigeant le consentement de la personne concernée en condition préalable à toute opération de collecte ou de traitement. Ce même article interdit, sauf exception légale, toute communication des données à des tiers, traduisant ainsi une volonté de restreindre leur circulation non maîtrisée¹⁵. Par dérogation à cette règle pour les traitements pénaux visés au Titre V bis de la loi n° 18-07 modifiée et complétée, le consentement préalable de la personne concernée n'est pas requis, sous réserve des garanties propres à ces finalités.

Dans le prolongement de cette logique, l'article 9 subordonne la licéité du traitement au respect de conditions selon lesquelles : les données soient collectées pour des finalités déterminées, explicites, légitimes et qu'elles soient traitées de manière loyale et proportionnée. Il exige en outre que ces données soient exactes, tenues à jour, et conservées pour une durée limitée, strictement nécessaire à la

La réalisation de traitement en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sous la seule instruction du responsable du traitement et dans le respect des obligations prévues à l'article 38 ci-dessus.

Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures prévues au paragraphe 1er de l'article 38 ci-dessus sont consignés par écrit ou sous une autre forme équivalente. »

¹⁵ العيداني محمد، زروق يوسف، 'حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 07-18 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)'، مجلة معالم للدراسات القانونية والسياسية، العدد 05، 2018، ص 121 و122.



réalisation des objectifs poursuivis. Ces dispositions visent à établir des garanties relatives au traitement des données personnelles, applicables tout au long de leur cycle de vie.

Sans consacrer formellement le principe de *privacy by design* décrit ci-dessous, ces règles s'en rapprochent partiellement dans leur portée pratique.

Dans ce même cadre préventif, la loi n° 18-07, à l'instar du RGPD, consacre un ensemble de droits fondamentaux destinés à garantir aux personnes concernées un contrôle effectif sur leurs données personnelles. Il s'agit en particulier du droit à l'information (article 32), qui impose au responsable du traitement de fournir de manière claire toutes les informations pertinentes sur l'usage des données ; du droit d'accès (article 34), permettant à toute personne de savoir si ses données sont traitées et d'en obtenir communication ; du droit de rectification (article 35), qui autorise la correction des données inexacts ; du droit à l'effacement (article 35), permettant la suppression des données lorsque leur traitement n'est plus justifié ; et du droit d'opposition (article 36), permettant de s'opposer au traitement pour des motifs légitimes.¹⁶

En revanche, certains droits garantis par le RGPD ne sont pas repris dans la législation algérienne. C'est le cas du droit à la portabilité des données, qui permet de transférer ses données d'un responsable de traitement à un autre¹⁷, et du droit à la limitation du traitement, qui permet de suspendre temporairement leur utilisation dans certaines situations¹⁸. Cette absence traduit un écart persistant entre le droit algérien et les standards européens les plus récents en matière de protection des données.

Ainsi, bien que le dispositif algérien témoigne d'une volonté d'encadrement, il demeure marqué par une vision formelle de la conformité, centrée sur des obligations administratives statiques et un contrôle vertical, sans véritable ancrage dans une logique dynamique de responsabilisation des intervenants.

SECTION 2 : L'approche préventive européenne : la consécration d'une responsabilisation continue et d'une transparence renforcée

¹⁶ بوحليط يزي، عبد الرحمان فطناسي، "الحماية الإدارية والجزائية في مجال معالجة المعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07"، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 02، 2021، ص ص 62-64.

¹⁷ ZOLYNSKI Célia, LE ROY Marylou, « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », Légicom, n° 59, 2017, pp 105-113.

¹⁸ *ibid.*



Dans le système européen, la protection des données personnelles repose sur une logique dynamique fondée sur la responsabilisation des acteurs. Cette approche, consacrée par le Règlement général sur la protection des données (RGPD), marque une rupture avec les modèles exclusivement axés sur les formalités déclaratives.

Deux principes structurants traduisent cette évolution : *l'accountability*, d'une part, qui se manifeste en particulier par le biais de l'article 5, paragraphe 2, du RGPD, selon lequel « le responsable du traitement est responsable du respect des principes énoncés au paragraphe 1 et doit être en mesure de le démontrer » ; et d'autre part, le principe de *privacy by design*, énoncé à l'article 25¹⁹.

Le premier principe, celui de *l'accountability*, opère un véritable renversement de perspective en matière de conformité. Le responsable du traitement ne saurait plus se contenter de respecter la législation applicable ; il doit désormais pouvoir démontrer cette conformité à tout moment, tant devant les autorités de contrôle que vis-à-vis des personnes concernées. Cette exigence implique la mise en œuvre de mesures internes adaptées. Ce modèle substitue à l'ancien régime, fondé sur les formalités préalables, une logique de co-régulation, dans laquelle la conformité devient un processus permanent inscrit dans la gouvernance des données²⁰.

¹⁹ L'article 25 du règlement général européen sur la protection des données dispose : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.*

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article. »

²⁰ LANNA Maximilien, *op. cit.*, pp 227-230. GOLA Romain, « Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité », *Légicom*, n° 59, 2017, pp 30-32.



Le second principe, celui de la protection des données dès la conception *privacy by design*, impose quant à lui une intégration des garanties liées au respect de la vie privée dès la phase de conception des systèmes et des traitements. Inspirée d'expériences étrangères – en particulier canadiennes – cette approche vise à prévenir les atteintes aux données personnelles plutôt qu'à y remédier une fois survenues. Elle se traduit par plusieurs exigences concrètes : limitation des données collectées, sécurité renforcée, transparence des traitements et recentrage des traitements sur les droits de la personne concernée²¹.

Au-delà de ces exigences concrètes, l'approche consacrée par ce principe transforme selon certains auteurs²² la conformité en véritable impératif d'ingénierie. Elle repose d'abord sur une prévention proactive : en cartographiant les traitements et en conduisant des analyses d'impact en amont, l'organisation évite que l'atteinte ne se produise plutôt que d'en atténuer les conséquences a posteriori ; cette logique « *proactive not reactive* » constitue le cœur du modèle canadien qui a inspiré le régulateur européen. Elle impose ensuite que la protection soit activée par défaut : seuls les attributs strictement nécessaires sont collectés, la durée de conservation est limitée et la diffusion à des tiers fait l'objet d'un consentement explicite, garantissant de ce fait la minimisation sans intervention de l'utilisateur.

Cette protection par défaut doit donc être intégrée à l'architecture même des systèmes (*privacy embedded into design*) : chiffrement, pseudonymisation, journalisation et mécanismes de purge automatique ne sont plus de simples ajouts, mais des spécifications fonctionnelles au même titre que la performance ou l'ergonomie. Loin d'entraver l'innovation, l'approche favorise une logique de somme positive : en mobilisant conjointement juristes et ingénieurs, l'entreprise conçoit des solutions où la compétitivité et le respect des droits progressent de concert, plutôt qu'au prix de compromis défensifs.

Dans ce même mouvement de responsabilisation, l'effectivité de ces obligations s'appuie sur l'action des autorités nationales de contrôle, prévues à l'article 51 du RGPD, telles que la CNIL en France. Ces organes qui doivent être indépendants accompagnent les responsables de traitement par des recommandations, veillent à la conformité des traitements, et assurent un rôle de conseil, d'information et de coopération internationale. Leur mission ne se limite donc pas à la sanction, mais

²¹ GOLLA Romain, *op. cit.*, pp 32-34.

²² *ibid.*



participe à instaurer un climat de transparence et de respect des droits, au cœur du modèle européen de gouvernance des données personnelles²³

À la lecture des dispositions de la loi n° 18-07 telle que modifiée en 2025, les principes *d'accountability* et de *privacy by design* ne sont pas consacrés en tant que tels ; cependant, l'introduction du registre, de la journalisation et du délégué à la protection des données traduit une évolution vers la responsabilisation, sans atteindre le niveau d'obligation de démonstration continue posé par le RGPD. Cette orientation témoigne d'une inspiration de la directive européenne 95/46/CE, aujourd'hui abrogée, dont le modèle reposait davantage sur une régulation par la procédure que sur l'instauration d'un devoir actif de conformité²⁴.

CHAPITRE II :

Les mécanismes répressifs de la protection des données personnelles : sanctions prévues et effectivité contrastée

Si la régulation préventive constitue un pilier fondamental de la protection des données personnelles, elle ne saurait, à elle seule, garantir l'effectivité de la protection des droits reconnus aux personnes. La perspective répressive, à travers la menace de sanctions, qu'elles soient administratives, pécuniaires ou pénales, confère une force contraignante aux obligations juridiques. Elle assure, d'une part, une réponse institutionnelle aux violations constatées et, d'autre part, renforce la fonction dissuasive du dispositif normatif. À ce titre, la dimension répressive apparaît comme le complément nécessaire aux mécanismes de responsabilisation et de contrôle.

L'analyse comparée révèle cependant des dynamiques contrastées. En Algérie, la loi n° 18-07 prévoit un ensemble structuré de sanctions applicables en cas d'atteinte aux données personnelles. Toutefois, sa mise en œuvre demeure à ce jour peu visible. Ce constat peut s'expliquer, notamment, par la relative nouveauté du cadre juridique, l'absence de jurisprudence consolidée, ainsi que par un écosystème numérique encore peu dominé par les grandes plateformes internationales. À l'inverse, le droit de l'Union européenne, en particulier à travers le RGPD et les instruments nationaux qui l'accompagnent, illustre une mobilisation partiellement effective de l'arsenal répressif, dans un contexte marqué par une forte exposition aux enjeux transfrontaliers des données personnelles.

²³ HUET Jérôme, LECLERCQ Pierre, « La CNIL a-t-elle accompli les missions dévolues par le législateur », *Légicom*, n° 42. 2009, pp 13-21.

²⁴ DEBET Anne, « La protection des données personnelles, point de vue du droit privé », *Revue de droit public*, n°1, 2016, pp 17-34.



Ainsi, une analyse comparative permettra de mieux apprécier, d'une part, les mécanismes instaurés en droit algérien pour sanctionner les atteintes aux données personnelles (Section 01), et, d'autre part, la portée et l'efficacité du modèle européen dans l'application de sanctions légales (Section 02).

SECTION 1 : Un encadrement répressif en construction dans le droit algérien

La loi n° 18-07 du 10 juin 2018 consacre une approche répressive articulée autour de deux axes : l'intervention d'une autorité administrative indépendante et l'établissement de sanctions pénales pour les atteintes graves aux données personnelles. En matière de répression, la réforme de 2025 n'a pas substantiellement modifié l'échelle des incriminations et peines prévue aux articles 54 et suivants de la loi n° 18-07 elle en renforce toutefois l'effectivité par l'introduction d'obligations nouvelles telles que la tenue d'un registre, la conservation d'un carnet des opérations, la désignation d'un délégué à la protection des données, la réalisation d'analyses d'impact relatives à la protection des données et la notification des violations

En premier lieu, l'article 25 investit l'Autorité de prérogatives coercitives étendues. Elle peut enjoindre toute modification nécessaire pour mettre un traitement en conformité, ordonner la fermeture des fichiers, exiger le retrait des données ou leur destruction pure et simple. À ces mesures correctives s'ajoute un éventail de sanctions administratives : avertissement, mise en demeure, retrait d'autorisation, tandis qu'une obligation, pour l'Autorité, d'alerter immédiatement le procureur général assure la jonction avec la répression judiciaire lorsque les faits sont pénalement qualifiables.

En second lieu, l'article 47 confère à la même Autorité le pouvoir de prononcer une amende forfaitaire de 500 000 DA à l'encontre de tout responsable de traitement qui, sans motif légitime, entrave l'exercice des droits d'information (article 32), d'accès (article 34), de rectification ou d'effacement (article 35) et d'opposition (article 36). La sanction frappe également le manquement à l'obligation de notification.

Cependant, il convient de souligner que cette autorité, bien que prévue dès 2018, n'a été mise en place de manière réelle qu'en 2023²⁵, (ses membres ont été installés un an plus tôt)²⁶ soit cinq années après l'adoption du texte. Ce retard a

²⁵ CHIRIFI Imad, ZERGUINI Radia, "The protection of personal data in Algeria, between local challenges and international standards", Pakistan journal of Life and Social sciences, n° 22(2), 2024, p 18207.

²⁶ - Décret présidentiel n° 22-187 du 18 mai 2022 portant nomination du président et des membres de l'Autorité nationale de protection des données à caractère personne, JORA n° 35, publié le 24/05/2022.



considérablement freiné l'effectivité du volet répressif, en l'absence d'un organe opérationnel apte à exercer un contrôle autonome.

Au-delà des pouvoirs correctifs et de l'amende administrative confiés à l'Autorité nationale, la loi 18-07 déploie un volet pénal qui réprime les atteintes les plus graves au régime de protection des données. Relèvent de ce champ :

- la violation de la dignité ou de la vie privée (article 54) ;
- le traitement sans base légale ou malgré l'opposition de la personne concernée (article 55) ;
- la réalisation d'un traitement sans déclaration, sur fausse déclaration ou après retrait d'autorisation (article 56) ;
- le traitement illicite de données sensibles (article 57) ;
- le détournement de finalité et la collecte frauduleuse (articles 58 et 59) ;
- l'accès non autorisé ou laissé à des tiers, ainsi que l'entrave aux contrôles de l'Autorité (articles 60 et 61) ;
- l'accès illégal au registre national et le refus persistant d'honorer les droits d'information, d'accès, de rectification ou d'opposition (articles 63 et 64) ;
- les manquements aux obligations de sécurité, de conservation ou de notification de violation (articles 65 et 66) ;
- le transfert international prohibé de données et l'usage abusif des informations (articles 67 à 69).

Ces infractions sont punies d'une échelle de peines graduée : de six mois à trois ans d'emprisonnement et jusqu'à trois cents mille dinars pour les manquements intermédiaires (détournement de finalité, collecte frauduleuse, entrave aux contrôles) ; d'un à cinq ans et jusqu'à un million de dinars pour les atteintes les plus graves (traitements clandestins ou de données sensibles, transferts illicites, accès non autorisé massif) ; certaines violations purement techniques de sécurité peuvent être sanctionnées d'une amende de deux cents à cinq cents mille dinars²⁷.

La responsabilité pénale des personnes morales est expressément prévue, accompagnée de confiscations, d'effacement de données et de peines complémentaires (articles 70 à 74), tandis que la compétence extraterritoriale affirmée à l'article 53 est censée assurer la poursuite des atteintes commises en dehors du territoire national²⁸.

²⁷ جقريف الزهرة، "الحماية الجزائية للمعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون 18-07"، مجلة

العلوم القانونية والاجتماعية، المجلد 06، العدد 04، 2021، ص ص 490-495.

²⁸ L'article 53 de la loi n° 18-07 dispose : « *Les juridictions algériennes sont compétentes pour connaître des infractions prévues par la présente loi, commises hors du territoire de la République,*



Néanmoins, en dépit de ce cadre normatif, aucune décision publique significative n'a été portée à la connaissance du public depuis l'adoption de cette loi. L'absence de contentieux visibles, combinée à un environnement numérique local encore peu structuré et peu dominé par les géants du numérique, limite pour l'instant la portée du dispositif. La jeunesse du droit positif et le déficit de pratique jurisprudentielle contribuent ainsi à une forme de latence dans l'application des sanctions prévues.

Dans ce contexte, la répression en matière de protection des données personnelles en Algérie apparaît davantage comme un édifice juridique en construction, dont la solidité dépendra de l'effectivité des institutions, du renforcement de l'autorité de contrôle, ainsi que d'un éveil progressif à la culture du contentieux numérique.

SECTION 2 : Un encadrement répressif plus abouti : le modèle européen en contraste avec l'Algérie

Le modèle européen de protection des données personnelles repose sur un dispositif répressif structuré. Le RGPD, tout en consacrant une logique de responsabilisation, accorde une place importante à la sanction, conçue comme un levier dissuasif à destination des responsables de traitement.

Ainsi, sous la réglementation européenne, les autorités administratives indépendantes chargées de la protection des données telles que la CNIL en France, disposent de garanties d'indépendance et de pouvoirs de sanction plus étendus que ceux de l'autorité algérienne créée par la loi n° 18-07²⁹, ces garanties sont consacrées particulièrement par les articles 58 et 83 du RGPD. Ces prérogatives s'inscrivent dans une logique de régulation dissuasive. L'article 58 confère ainsi à ces autorités des pouvoirs correctifs importants : elles peuvent adresser des avertissements, ordonner la mise en conformité, imposer des limitations temporaires ou définitives de traitement, suspendre des flux transfrontaliers de données, ou encore retirer des certifications.

Elles disposent également du pouvoir d'ordonner la notification d'une violation aux personnes concernées, ou d'interdire un traitement lorsqu'il contrevient aux principes du règlement. Cet ensemble de mesures est complété par la faculté d'imposer des amendes administratives, conformément à l'article 83 du RGPD.

par un Algérien, une personne étrangère ayant son domicile en Algérie ou une personne morale de droit algérien.

Elles sont également compétentes pour connaître des infractions prévues par la présente loi, conformément aux règles de compétence prévues par l'article 588 du code de procédure pénale. »

²⁹سعودي عمر، "المركز القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: جمالية النص القانوني ومعوقات الواقع العملي"، معارف، المجلد 18، العدد 01، 2023، ص ص 172-180.



Celles-ci peuvent atteindre jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires annuel mondial, selon la gravité de l'infraction et sa nature³⁰.

L'effectivité de ces prérogatives correctives ne relève pas du seul principe théorique : elle se manifeste concrètement à travers des décisions rendues par plusieurs autorités de protection européennes à l'encontre d'acteurs d'envergure mondiale. Ainsi, en 2019, la CNIL a prononcé une amende de 50 millions d'euros à l'encontre de Google, reprochant à l'entreprise américaine un manque de transparence sur l'usage des données et l'absence de consentement valable pour la personnalisation publicitaire. Cette décision, confirmée par le Conseil d'État français par sa décision du 19/06/2020, a constitué l'un des premiers exemples significatifs d'application du RGPD à l'égard des géants du numérique. Puis en 2023, l'autorité irlandaise a infligé à Meta une amende record de 1,2 milliard d'euros pour des transferts de données vers les États-Unis opérés sans garanties suffisantes, en violation des règles encadrant les flux transfrontaliers.

Ces exemples attestent de la capacité réelle des autorités de régulation à activer leurs leviers de sanction, même face à des entités puissantes, et à imposer ainsi une mise en conformité réelle avec les principes du RGPD³¹.

L'actualité récente vient renforcer cette tendance à une mobilisation se voulant effective des pouvoirs correctifs par les autorités de régulation européennes. Ainsi, en décembre 2024, l'Autorité italienne de protection des données a infligé une amende de 15 millions d'euros à *OpenAI* pour des violations multiples du RGPD dans le cadre du déploiement de *ChatGPT*. Il s'agit là de la première condamnation majeure d'un système d'intelligence artificielle générative sur ce fondement. La décision reproche à *OpenAI* l'absence de base légale claire pour le traitement des données, une politique de confidentialité déficiente, l'absence de vérification de l'âge des utilisateurs, ainsi que la non-notification d'une fuite de données. L'Autorité a également exigé une campagne de communication publique de six mois destinée à informer les citoyens sur leurs droits en matière de données personnelles. Cette affaire témoigne de la vigilance accrue des régulateurs face aux enjeux spécifiques que soulève l'intelligence artificielle, et de leur volonté d'appliquer le RGPD à des

³⁰ - BONICHOT Jean Claude, *op. cit.*, pp 98-100.

GRYNBAUM Luc, LE GOFFIC Caroline, PAILLER Ludovic, *Droit des activités numériques*, 2^{ème} édition, Dalloz, Paris, 2023, pp 990-994.

³¹ BONICHOT Jean Claude, *op. cit.*, pp 98-100.



technologies en évolution rapide, y compris lorsqu'il s'agit d'acteurs majeurs du numérique³².

Néanmoins, des auteurs attirent l'attention sur une application inégale du RGPD entre les États membres de l'Union européenne. Cette disparité est susceptible d'alimenter un phénomène de *forum shopping* réglementaire, les entreprises choisissant de s'implanter là où les autorités de contrôle sont perçues comme les moins contraignantes. Comme le relèvent Douwe Korff et Ian Brown, cette divergence institutionnelle fragilise la cohérence du dispositif européen de gouvernance des données. L'exemple de l'amende de 150 000 euros infligée à Facebook par la CNIL en 2017 illustre également les limites du pouvoir répressif : symbolique au regard de la taille et des ressources de la plateforme, cette sanction a eu un impact marginal sur ses pratiques opérationnelles³³.

L'importance des sanctions pécuniaires prévues par le RGPD se révèle, selon certains, souvent insuffisante pour exercer une pression véritablement dissuasive à l'égard des géants du numérique. La puissance économique de ces acteurs est telle que même des amendes de plusieurs dizaines de millions d'euros peuvent être perçues comme un simple coût d'exploitation, assimilable à une taxe occasionnelle plutôt qu'à une contrainte juridique réelle. L'amende maximale de 150 000 euros jadis infligée à Facebook par la CNIL, bien que symbolique, illustre les limites d'un tel dispositif lorsqu'il n'est pas adapté à l'échelle des opérateurs visés. En définitive, l'effectivité du régime sanctionnateur repose moins sur les plafonds théoriques que sur la capacité des autorités de contrôle à calibrer les sanctions en fonction du poids économique des entités concernées et à activer d'autres leviers réputationnels, structurels ou stratégiques susceptibles d'infléchir durablement leurs comportements³⁴.

³² JAULT-SESEKE Fabienne, IA générative et RGPD : L'autorité italienne sanctionne OpenAI d'une amende de 15 millions d'euros, Dalloz actualité, 16/01/2025.

³³ KORF Douwe, BROWN Ian, The inadequacy of UK data protection law, rapport indépendant, oct. 2020, p. 6, disponible en ligne : <https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf>, consulté le 1er août 2025.

³⁴ - GALUSTIAN Gohar, *op. cit.*, pp 1395-1396.



Conclusion :

L'étude comparée des approches algérienne et européenne en matière de protection des données personnelles met en évidence l'existence de deux modèles aux dynamiques contrastées, révélatrices de niveaux d'évolution juridique distincts face aux mutations de l'environnement numérique. Tandis que le cadre européen, structuré autour du RGPD, s'appuie sur une logique intégrée de responsabilisation, de transparence et de sanctions relativement effectives, le dispositif algérien, bien que fondé sur une volonté normative affirmée, demeure inscrit dans une logique de conformité administrative, marquée par un formalisme procédural et un contrôle centralisé.

Sur le plan préventif, le droit européen impose aux responsables de traitement une implication constante dans la gestion des risques, en intégrant la protection des données au cœur de la gouvernance des traitements, notamment à travers les principes d'*accountability* et de *privacy by design*, qui imposent à l'intervenant de démontrer en permanence sa conformité, à l'inverse, la loi algérienne n° 18-07, en s'inspirant d'un modèle désormais dépassé (la directive 95/46/CE), repose encore largement sur des mécanismes déclaratifs et d'autorisation, sans aller jusqu'à exiger une conformité démontrable et proactive. Toutefois, la réforme opérée en 2025 par la loi n° 25-11 marque une inflexion notable en introduisant de nouveaux outils de gouvernance (registre, journalisation, délégué à la protection des données) et en enrichissant le lexique juridique, elle amorce un mouvement vers une approche plus structurée et alignée sur les standards internationaux.

S'agissant du volet répressif, si les textes algériens prévoient une gradation cohérente de sanctions administratives et pénales, l'absence de jurisprudence, le retard institutionnel dans la mise en œuvre de l'organe de contrôle, ainsi qu'un écosystème numérique encore émergent, limitent fortement l'effectivité du dispositif. À l'inverse, le modèle européen se distingue par une culture du contentieux et une mobilisation plus active des autorités de contrôle.

Face à ces constats, il apparaît urgent pour l'Algérie d'accélérer la modernisation de son cadre juridique et institutionnel, afin de répondre aux défis posés par la généralisation des technologies de surveillance, le recours massif à l'intelligence artificielle et l'internationalisation des flux de données. Cette modernisation passe non seulement par une révision législative s'inspirant du RGPD tel que la responsabilisation, la protection dès la conception, ou encore la portabilité des données mais également par un renforcement opérationnel des autorités de contrôle. Elle suppose également une politique soutenue de sensibilisation du public, la



méconnaissance des droits numériques demeurant préoccupante, tant en Algérie qu'à l'échelle internationale.

Dans un contexte mondial marqué par l'intensification des risques d'atteinte à la vie privée et par la captation algorithmique de l'identité numérique des individus, la protection des données personnelles ne saurait rester un domaine marginal ou purement technique. Elle s'impose, au contraire, comme une composante essentielle de la souveraineté informationnelle, de la confiance numérique, et plus largement de l'effectivité des droits fondamentaux dans l'espace numérique. Le droit comparé, à ce titre, constitue un levier précieux non seulement pour évaluer les écarts, mais aussi pour tracer des voies et des moyens d'adaptation aux exigences d'une gouvernance des données plus éthique et plus rigoureuse.

Bibliographie :

A- Ouvrages :

1. GRYNBAUM Luc, LE GOFFIC Caroline, PAILLER Ludovic, Droit des activités numériques, 2^{ème} édition, Dalloz, Paris, 2023.

B- Articles de revue :

1. BONICHOT Jean Claude, «Données personnelles :l'invention européenne d'un monde nouveau», Pouvoirs, N°185, 2023, pp 97-109.
2. CECERE Grazia, MANANT Mathieu, «Vie privée, valeur des données personnelles et régulation», Annales des mines – Enjeux numériques, n° 2, 2018, pp 14-19.
3. CHIRIFI Imad, ZERGUINI Radia, "The protection of personal data in Algeria, between local challenges and international standards", Pakistan journal of Life and Social sciences, n° 22(2), 2024, pp 18200-18215.
4. DEBET Anne, «La protection des données personnelles», point de vue du droit privé, Revue de droit public, n°1, 2016, pp 17-34.
5. DEBIÈS Élise, «Big data de santé et autodétermination informationnelle : quelles articulations possibles pour une innovation protectrice des données personnelles ?» Revue française d'administration publique, n° 167, 2018, pp 565-574.
6. GALUSTIAN Gohar, «La protection des données personnelles à l'épreuve du numérique», Revue de droit public, n°05, 2021, pp 1390-1415.
7. GOLA Romain, «Le règlement européen sur les données personnelles, une opportunité pour les entreprises au-delà de la contrainte de conformité», Légicom, n° 59, 2017, pp 29-38.
8. HUET Jérôme, LECLERCQ Pierre, « La CNIL a-t-elle accompli les missions dévolues par le législateur », Légicom, n° 42. 2009, pp 13-21.



9. JAULT-SESEKE Fabienne, «IA générative et RGPD : L'autorité italienne sanctionne OpenAI d'une amende de 15 millions d'euros», Dalloz actualité, 16/01/2025.
10. LANNA Maximilien, «Objets connectés et protection des données à caractère personnel : vers un changement de paradigme des modalités de protection», Droits, n° 68, 2019, pp 223-235.
11. PEYROU Sylvie, «La protection des données à caractère personnel au sein de l'UE : des enjeux économiques et sécuritaires encadré par le législateur sous le contrôle du juge», Revue de droit public, n° 1, 2015, pp 55-69.
12. ZOLYNSKI Célia, LE ROY Marylou, «La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée», Légicom, n° 59, 2017, pp 105-113.

C- Documentation électronique :

KORF Douwe et BROWN Ian, The inadequacy of UK data protection law, rapport indépendant, oct. 2020, p. 6, disponible en ligne : <https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf>, consulté le 1er août 2025.

D- Textes de loi :

1. Décret présidentiel n° 20-442 du 30/12/2020 relatif à la promulgation au journal officiel de la république algérienne démocratique et populaire de la révision constitutionnelle, adoptée par le référendum du 1^{er} novembre 2020, JORA n° 82, publié le 30/12/2020.
2. Loi n° 18-07 du 10 juin 2018, Relative à la protection des personnes physiques dans le traitement des données à caractère personnel, JORA n° 34, publié le 10/06/2018.
3. Loi n° 25-11 du 24 juillet 2025 modifiant et complétant la loi 18-07, Relative à la protection des personnes physiques dans le traitement des données à caractère personnel, JORA n° 48, publié le 24 juillet 2025.
4. Décret présidentiel n° 22-187 du 18 mai 2022 portant nomination du président et des membres de l'Autorité nationale de protection des données à caractère personnel, JORA n° 35, publié le 24/05/2022.

المراجع باللغة العربية:

المقالات:



1. العيداني محمد، زروق يوسف، حماية المعطيات الشخصية في الجزائر على ضوء القانون رقم 07-18 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية، العدد 05، 2018، ص ص 115-130.
2. بوحليط يزيد، فطناسي عبد الرحمان، الحماية الإدارية والجزائية في مجال معالجة المعطيات ذات الطابع الشخصي على ضوء القانون رقم 07-18، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 02، 2021، ص ص 55-76.
3. جقريف الزهرة، الحماية الجزائية للمعطيات ذات الطابع الشخص في التشريع الجزائري وفقا لأحكام القانون 07-18، مجلة العلوم القانونية والاجتماعية، المجلد 06، العدد 04، 2021، ص ص 484-499.
4. سعودي عمر، المركز القانوني للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: جمالية النص القانوني ومعوقات الواقع العملي، معارف، المجلد 18، العدد 01، 2023، ص ص 163-183.
5. قونان كهينة، حميل نواره، السلطة الوطنية كهينة مكلفة برقابة احترام تطبيق قانون حماية المعطيات الشخصية رقم 07-18، مجلة الدراسات القانونية، المجلد 07، العدد 02، 2021، ص ص 562-578.