Intelligence artificielle générative et données à caractère personnel : la loi 09-08 à l'épreuve

Problèmes juridiques et imputation des responsabilités en droit marocain

Mustapha DEGDEG

Docteur en droit international, avocat agréé près la Cour de Cassation, enseignant en droit

Résumé

L'intelligence artificielle générative traite des données personnelles à trois moments : l'entraînement des modèles, la saisie des requêtes et la production des contenus. Confrontée à ces usages, la loi marocaine n° 09-08, adoptée en 2009, révèle moins un déficit de principes qu'une fragilité de son rattachement territorial et de ses sanctions face aux fournisseurs étrangers. Le présent article identifie les problèmes juridiques posés par ces traitements, puis propose une méthode d'imputation des responsabilités fondée sur une qualification des acteurs par phase, articulée avec le droit commun de la responsabilité civile. Il s'appuie sur la jurisprudence de la Cour de justice de l'Union européenne et sur les premières décisions rendues en Europe à l'égard des fournisseurs d'IA.

Mots-clés : intelligence artificielle générative, données personnelles, loi 09-08, CNDP, responsabilité, sous-traitant, transferts internationaux, Dahir des obligations et contrats.

Introduction

En quelques années, les systèmes d'intelligence artificielle générative se sont installés dans le quotidien des entreprises, des administrations et des particuliers marocains. Assistants conversationnels bancaires, outils de tri de candidatures, générateurs de textes et d'images : ces applications reposent toutes sur des modèles entraînés à partir de volumes considérables de données, dont une part importante est constituée de données à caractère personnel.

Le droit marocain dispose depuis 2009 d'un cadre général de protection de ces données, la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[1], dont l'application est contrôlée par la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP). Conçu avant l'essor de l'apprentissage automatique à grande échelle, ce texte n'en contient aucune disposition spécifique. Aucune décision juridictionnelle marocaine publiée ne s'est, à notre connaissance, encore prononcée sur l'application de la loi 09-08 à un système d'IA générative.

L'IA générative mobilise des données personnelles à trois moments distincts : lors de l'**entraînement** du modèle, à partir de corpus souvent constitués par collecte automatisée sur Internet (*scraping*) ; lors de la **saisie des requêtes** (*prompts*) par les utilisateurs, qui transitent généralement par une interface de programmation (API) vers des serveurs situés à l'étranger ; enfin,

[1] Loi n° 09-08 promulguée par le Dahir n° 1-09-15 du 18 février 2009, BO n° 5714 du 5 mars 2009.

lors de la **production des contenus**, qui peuvent comporter des informations inexactes sur des personnes réelles.

La question se pose dès lors de savoir si la loi 09-08 est en mesure d'appréhender ces traitements et, dans l'affirmative, à qui imputer la responsabilité d'une atteinte dans une chaîne qui associe développeurs, intégrateurs et utilisateurs. L'examen des problèmes juridiques révèle une loi éprouvée par l'IA générative (I), ce qui invite à construire une méthode d'imputation de la responsabilité adaptée à la pluralité des acteurs (II).

I. Une loi 09-08 éprouvée par l'IA générative

A. Un champ d'application territorial incertain

L'article 2 de la loi 09-08 rattache son application à l'établissement du responsable du traitement sur le territoire marocain ou, à défaut, au recours à des moyens de traitement situés au Maroc. Dans ce second cas, le responsable doit désigner un représentant installé au Maroc, qui se substitue à lui dans ses droits et obligations. Or la plupart des fournisseurs de modèles génératifs ne disposent au Maroc ni d'établissement ni de serveurs.

La question est alors de savoir si le terminal de l'utilisateur marocain constitue un « moyen de traitement » au sens de l'article 2 de la loi 09-08, débat qui s'était déjà posé sous l'empire de la directive européenne 95/46/CE, dont la loi marocaine s'est largement inspirée. La Cour de justice de l'Union européenne a, sous cette directive, retenu une conception extensive de l'établissement : dans l'arrêt *Google Spain*, elle a jugé qu'un traitement est effectué « dans le cadre des activités » d'un établissement dès lors que la filiale locale assure la promotion et la vente d'espaces publicitaires liés au service, même si le traitement lui-même est réalisé hors de l'Union[2]. Cette lecture fonctionnelle, transposable par voie doctrinale, offrirait un fondement pour soumettre à la loi 09-08 un fournisseur disposant au Maroc d'une activité commerciale, mais elle laisse hors d'atteinte ceux qui n'y ont aucune implantation.

Le RGPD a comblé cette lacune par le critère du « ciblage » (article 3.2), qui soumet au droit européen tout responsable qui offre des biens ou services à des personnes situées dans l'Union. Ce critère n'a pas d'équivalent en droit marocain. Un fournisseur étranger peut donc soutenir qu'il échappe à la loi 09-08, alors que l'entreprise marocaine qui intègre son outil y demeure pleinement soumise.

L'expérience européenne montre d'ailleurs que la question du rattachement peut décider à elle seule de l'issue d'un contentieux. Par un jugement du 18 mars 2026, le Tribunal de Rome a annulé la sanction de 15 millions d'euros prononcée par le *Garante* italien contre OpenAI, au motif que l'autorité italienne n'était plus compétente depuis que l'autorité irlandaise était devenue autorité chef de file, à la suite de l'établissement de la filiale irlandaise d'OpenAI le 15 février 2024 ; le tribunal

[2]CJUE, gr. ch., 13 mai 2014, *Google Spain SL et Google Inc. c. AEPD et Mario Costeja González*, aff. C-131/12.

n'a pas examiné le fond des manquements reprochés[3]. Si le choix d'un établissement suffit, dans un système aussi intégré que le RGPD, à déplacer la compétence, l'enjeu est plus aigu encore pour un État tiers dépourvu de critère de ciblage.

Dans l'arrêt *Google c. CNIL*, la Cour de justice a par ailleurs précisé que l'exploitant d'un moteur de recherche n'est pas tenu, en l'état du droit de l'Union, d'opérer un déréférencement sur l'ensemble des versions de son moteur dans le monde[4]. Cette décision rappelle que l'effectivité des droits reconnus aux personnes s'arrête, sauf coopération internationale, aux frontières du droit qui les consacre.

B. Des exigences de licéité et de qualité difficilement conciliables

L'article 4 de la loi 09-08 subordonne le traitement au consentement indubitable de la personne concernée, sous réserve d'exceptions limitatives, dont la réalisation d'un intérêt légitime du responsable, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne. La collecte massive de données publiquement accessibles aux fins d'entraînement ne peut, en pratique, reposer que sur cette dernière exception, dont la CNDP n'a pas encore précisé la portée en matière d'IA.

Les autorités européennes se sont montrées réservées. La CNIL française a sanctionné en 2022 la société Clearview AI, qui constituait une base de données biométriques à partir d'images collectées sur Internet, en retenant notamment l'absence de base légale de ce traitement[5]. De même, le *Garante* italien reprochait à OpenAI d'avoir entraîné ses modèles sans base juridique adéquate et en méconnaissance de son obligation de transparence, même si ces griefs n'ont pas été examinés au fond par le juge romain.

L'article 3 de la loi 09-08 exige en outre des données collectées pour des finalités déterminées, explicites et légitimes, adéquates, pertinentes, non excessives et exactes. Un modèle « à usage général » s'accorde mal avec la détermination préalable de la finalité. Surtout, les « hallucinations », c'est-à-dire la génération d'informations fausses présentées comme vraies, heurtent directement le principe d'exactitude. L'association autrichienne noyb[6] a déposé plusieurs plaintes sur ce fondement : en avril 2024 devant l'autorité autrichienne, au sujet d'une date de naissance erronée attribuée à une personnalité publique, puis en mars 2025 devant l'autorité norvégienne, au nom d'un

---

[3]Tribunale ordinario di Roma, Sezione diritti della persona e immigrazione, 18 mars 2026, R.G. n. 4785/2025, annulant le *provvedimento* n. 755 du *Garante per la protezione dei dati personali* du 2 novembre 2024.

[4]CJUE, gr. ch., 24 septembre 2019, *Google LLC c. CNIL*, aff. C-507/17.

[5]CNIL, formation restreinte, délibération n° SAN-2022-019 du 17 octobre 2022, *Clearview AI* (amende de 20 millions d'euros).

[6]*noyb (acronyme de « none of your business », « ça ne vous regarde pas ») est une ONG autrichienne à but non lucratif, officiellement dénommée European Center for Digital Rights. Fondée par Max Schrems et basée à Vienne, elle œuvre à faire appliquer le droit de la protection des données, en particulier le RGPD et la directive ePrivacy*. Créée en 2017 grâce à un financement participatif, l'association avait pour ambition d'exploiter les mécanismes du RGPD, applicable à partir de mai 2018, pour traiter des atteintes aux droits fondamentaux et soutenir les personnes concernées, notamment par des actions collectives ou représentatives. Elle se présente comme une « plateforme d'application du droit à la vie privée » qui porte des affaires de protection des données devant les tribunaux. Max Schrems en est aujourd'hui le président d'honneur et fondateur

particulier que ChatGPT présentait faussement comme le meurtrier de ses enfants[7]. Enfin, l'obligation d'information prévue par l'article 5 est pratiquement inexécutable pour des données collectées indirectement auprès de millions de personnes.

C. Des garanties difficilement effectives

1. Les droits des personnes et les décisions automatisées

Les droits d'accès, de rectification et d'opposition (articles 7 à 9) supposent de pouvoir localiser et corriger une donnée. Dans les paramètres d'un modèle entraîné, cette opération demeure techniquement incertaine, le « désapprentissage » (*machine unlearning*) n'étant pas maîtrisé à grande échelle.

L'article 11 est plus exigeant encore. Il interdit qu'une décision de justice impliquant une appréciation sur le comportement d'une personne ait pour fondement un traitement automatisé, et encadre les autres décisions produisant des effets juridiques fondées exclusivement sur un tel traitement. La Cour de justice a donné à la notion de décision automatisée une portée large : dans l'arrêt *SCHUFA*[8], elle a jugé que l'établissement automatisé d'une valeur de probabilité relative à la capacité d'une personne à honorer ses engagements constitue une telle décision dès lors que le tiers auquel elle est transmise s'y fonde de manière déterminante pour accorder ou refuser un crédit[9]. Transposée à l'IA générative, cette solution conduit à considérer qu'une réponse générée qui conditionne en fait une décision à l'égard d'une personne relève de l'article 11, même lorsqu'un agent humain intervient formellement en aval. Les usages en ressources humaines, en matière bancaire et, à terme, dans les juridictions sont directement concernés.

2. Les données sensibles et les formalités préalables

Les modèles peuvent mémoriser ou inférer des données relatives à la santé, aux opinions politiques ou aux convictions religieuses, qui relèvent du régime renforcé de l'article 21 et de

---

[7]Plaintes de noyb contre OpenAI devant la *Datenschutzbehörde* autrichienne (29 avril 2024) et le *Datatilsynet* norvégien (mars 2025), fondées notamment sur l'article 5.1.d du RGPD. À notre connaissance, aucune décision définitive n'avait été rendue sur ces plaintes à la date de rédaction.

[8]CJUE, 7 décembre 2023, OQ c. Land Hessen (SCHUFA Holding), C-634/21

Une particulière s'était vu refuser un crédit bancaire en raison d'un score négatif établi par SCHUFA, principale agence allemande d'évaluation de solvabilité. Elle avait demandé à l'agence des explications sur la méthode de calcul, que celle-ci avait refusé de fournir au nom du secret des affaires. Après le rejet de sa réclamation par l'autorité de contrôle de Hesse, le tribunal administratif de Wiesbaden a saisi la Cour.

La Cour juge que le calcul automatisé d'un score de solvabilité constitue une décision individuelle automatisée au sens de l'article 22 du RGPD lorsque le tiers qui le reçoit, ici la banque, s'y fonde de manière déterminante pour accorder ou refuser un contrat. Elle retient une conception large de la notion de décision, afin d'éviter une lacune de protection : sans cela, la banque, qui ignore la logique du calcul, et l'agence, qui la connaît mais ne décide pas formellement, échapperaient toutes deux aux obligations de l'article 22 et au droit d'accès renforcé de l'article 15.

Il en résulte que le scoring est en principe interdit, sauf s'il relève de l'une des exceptions de l'article 22, paragraphe 2 : nécessité contractuelle, autorisation légale assortie de garanties ou consentement explicite. La Cour émet des doutes sur la validité de la base légale allemande invoquée et laisse au juge national le soin de trancher.

L'arrêt étend ainsi l'encadrement des décisions algorithmiques aux acteurs qui préparent la décision, et pas seulement à celui qui la prend formellement. Il a été complété par l'arrêt Dun & Bradstreet Austria (2025), qui précise le droit de la personne à obtenir une explication de la logique appliquée, y compris face au secret des affaires.

[9]CJUE, 7 décembre 2023, *OQ c. Land Hessen (SCHUFA Holding)*, aff. C-634/21.

l'autorisation préalable de la CNDP. Plus largement, tout traitement doit être déclaré ou autorisé avant sa mise en œuvre (article 12). La CNDP a rappelé ces exigences aux partis politiques à l'approche des élections législatives du 23 septembre 2026, en appelant en outre au signalement des contenus produits par l'IA sur le fondement de l'article 447-2 du Code pénal et de la loi organique n° 53-25 relative à la Chambre des représentants[10].

3. Les transferts internationaux

Chaque requête adressée à un service hébergé à l'étranger est susceptible de constituer un transfert de données. Les articles 43 et 44 ne l'autorisent que vers un État assurant un niveau de protection suffisant, sauf dérogations ou autorisation de la CNDP. L'arrêt *Schrems II* illustre l'exigence d'une protection effective, et non seulement formelle, dans l'État destinataire : la Cour de justice y a invalidé le « bouclier de protection des données » UE-États-Unis, en raison de l'accès des autorités américaines aux données transférées[11]. Pour les professions soumises au secret (avocats, établissements de crédit, professions médicales), la question se cumule avec les obligations de secret professionnel.

4. L'effectivité des sanctions

Les sanctions de la loi 09-08 sont principalement pénales et assorties d'amendes sans commune mesure avec celles du RGPD. Leur effet dissuasif sur un acteur mondial est faible, d'autant que l'incertitude sur le rattachement territorial rend leur application même discutable. Une refonte de la loi, visant à l'aligner sur le RGPD quant aux bases légales, à la responsabilisation des acteurs et au niveau des sanctions, est en discussion depuis plusieurs années ; à notre connaissance, aucun texte définitif n'a été adopté à ce jour.

---

[10] CNDP, communiqué relatif au traitement des données à caractère personnel dans le cadre des élections législatives de 2026, août 2026.

[11] CJUE, gr. ch., 16 juillet 2020, Data Protection Commissioner c. Facebook Ireland Ltd et Maximillian Schrems, aff. C-311/18. Au fait il y a un autre arrêt Schrems. Et les deux arrêts Shrems naissent de la plainte de Max Schrems contre Facebook Ireland, qui transférait ses données vers les États-Unis où elles étaient accessibles aux services de renseignement, comme l'avaient révélé les documents d'Edward Snowden.
Dans Schrems I (6 octobre 2015, C-362/14), la Cour juge qu'une décision d'adéquation de la Commission n'empêche pas une autorité nationale de contrôle d'examiner une plainte, seule la Cour pouvant toutefois invalider cette décision. Elle définit le niveau de protection adéquat comme un niveau « substantiellement équivalent » à celui de l'Union et invalide le Safe Harbor : ce régime ne liait pas les autorités publiques américaines, permettait un accès généralisé au contenu des communications et privait les personnes de tout recours, portant ainsi atteinte au contenu essentiel des articles 7 et 47 de la Charte.
Dans Schrems II (16 juillet 2020, C-311/18), Facebook s'appuyait désormais sur les clauses contractuelles types. La Cour valide ces clauses, mais impose à l'exportateur de vérifier au cas par cas le droit du pays destinataire, d'adopter si nécessaire des mesures supplémentaires et, à défaut, de suspendre le transfert. Elle invalide en revanche le Privacy Shield, au motif que la surveillance américaine n'est pas limitée au strict nécessaire et que le mécanisme de médiateur n'offre pas un recours effectif devant un organe indépendant.
Ces arrêts font de la Charte l'étalon du contrôle des transferts internationaux. Ils ont conduit les États-Unis à réformer leur encadrement du renseignement (Executive Order 14086) et à l'adoption du Data Privacy Framework en 2023, aujourd'hui contesté par noyb, ce qui ouvre la perspective d'un éventuel « Schrems III ».

II. L'imputation de la responsabilité dans la chaîne de l'IA générative

A. Une qualification des acteurs par phase

Rechercher un responsable unique pour « le système » est une impasse. La loi 09-08 définit le responsable du traitement comme la personne qui, « seule ou conjointement avec d'autres », détermine les finalités et les moyens du traitement, et le sous-traitant comme celle qui traite des données pour le compte du responsable. Cette définition admet la co-responsabilité, même si la loi n'en organise pas le régime, à la différence de l'article 26 du RGPD.

La jurisprudence de la Cour de justice fournit une grille d'analyse transposable. L'arrêt *Wirtschaftsakademie*[12] a admis la qualité de co-responsable de l'administrateur d'une page Facebook, qui contribue par ses paramétrages à la détermination des finalités, alors même qu'il n'a pas accès aux données. L'arrêt *Jehovan todistajat* a précisé que la responsabilité conjointe n'implique pas une responsabilité égale et n'exige pas que chacun des acteurs dispose d'orientations écrites ou d'un accès aux données[13]. Enfin, l'arrêt *Fashion ID* a limité la responsabilité de chaque acteur aux seules opérations dont il détermine effectivement les finalités et les moyens, en l'espèce la collecte et la transmission de données par un module social intégré à un site marchand, à l'exclusion des traitements ultérieurs réalisés par le réseau social[14].

---

[12]CJUE, gr. ch., 5 juin 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16
L'affaire concerne une société allemande de formation qui administrait une page fan sur Facebook, par laquelle la plateforme collectait, au moyen de cookies, des données sur les visiteurs sans les en informer. L'autorité de protection des données du Schleswig-Holstein avait ordonné la fermeture de la page, et le Bundesverwaltungsgericht a saisi la Cour de justice sur l'interprétation de la directive 95/46/CE.
Sur le fond, la Cour retient que l'administrateur de la page est responsable du traitement conjointement avec Facebook. En créant la page et en paramétrant l'audience visée, il participe à la détermination des finalités et des moyens du traitement, peu important qu'il n'ait pas accès aux données personnelles et ne reçoive que des statistiques anonymisées. Cette responsabilité conjointe n'est cependant pas égale : chaque acteur répond selon son degré d'implication.
Sur la compétence, la Cour admet que l'autorité allemande peut agir contre la filiale allemande de Facebook, dont l'activité publicitaire est indissociablement liée au traitement, alors même que le responsable européen est établi en Irlande. Elle peut apprécier la légalité du traitement de façon autonome, sans passer par l'autorité irlandaise, et peut viser directement l'administrateur de la page.
L'arrêt ouvre une jurisprudence extensive sur la coresponsabilité, prolongée par Jehovan todistajat (2018) puis tempérée par Fashion ID (2019), qui limite la responsabilité conjointe aux seules opérations effectivement déterminées par chaque acteur. Le RGPD consacre cette notion à son article 26. En revanche, le volet relatif à la compétence est aujourd'hui encadré par le guichet unique, comme l'a précisé l'arrêt Facebook Belgium (2021). La doctrine critique enfin le risque de dilution de la notion de responsable du traitement.

[13]CJUE, gr. ch., 10 juillet 2018, *Tietosuojavaltuutettu (Jehovan todistajat)*, aff. C-25/17.

[14]CJUE, 29 juillet 2019, *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, aff. C-40/17.

Appliquée à l'IA générative, cette logique conduit à découper la chaîne en phases et à qualifier chaque acteur phase par phase :

Phase	Acteur	Qualification
Constitution du corpus et entraînement	Développeur du modèle (fournisseur)	Responsable du traitement : il choisit les sources, les méthodes de collecte et les données conservées.
Déploiement dans une activité	Entreprise intégratrice (déployeur)	Responsable pour ses propres finalités ; le fournisseur est en principe son sous-traitant (article 24).
Réutilisation des requêtes pour l'entraînement	Fournisseur	Sortie du rôle de sous-traitant : responsable, ou co-responsable, pour cette finalité propre.
Utilisation des contenus générés	Utilisateur final	Hors champ s'il agit dans un cadre exclusivement personnel (article 2) ; responsable en cas d'usage professionnel.

Quatre questions guident cette qualification dans un dossier : qui a décidé de collecter la donnée litigieuse ? qui a fixé la finalité du déploiement ? le fournisseur réutilise-t-il les données saisies ? qui contrôle les filtres et paramètres de sortie ? La documentation (contrats, conditions générales d'utilisation, analyses de risques, journaux techniques) devient alors la preuve décisive : en pratique, la responsabilité suit ce qui est documenté.

B. Les ressources du droit commun de la responsabilité

1. La voie contractuelle

L'article 24 de la loi 09-08 impose un contrat entre le responsable et son sous-traitant. Ce contrat peut interdire la réutilisation des requêtes, fixer la localisation des données, prévoir un droit d'audit et une garantie d'indemnisation. Sa portée se heurte toutefois au rapport de force : les grands fournisseurs imposent des conditions générales d'adhésion, rarement négociables. À l'égard des consommateurs, la loi n° 31-08 édictant des mesures de protection du consommateur permet d'écarter les clauses abusives.

2. La responsabilité du fait des choses

L'article 88 du Dahir des obligations et contrats, inspiré de l'article 1384, alinéa 1er, de l'ancien Code civil français, fonde une responsabilité du gardien de la chose. La distinction entre garde de la structure et garde du comportement, consacrée par la Cour de cassation française dans l'affaire dite de l'*Oxygène liquide*[15], s'avère particulièrement féconde. Le développeur du modèle conserverait la garde de la structure (conception, données d'entraînement, défauts internes), tandis que le déployeur aurait la garde du comportement (usage, paramétrage, contexte de mise en œuvre). Cette piste, encore peu explorée par la doctrine marocaine, permettrait de répartir la responsabilité selon l'origine du dommage.

[15]Cass. 2e civ., 5 janvier 1956, affaire dite de l'*Oxygène liquide*. La distinction avait été proposée par B. Goldman dans sa thèse, *De la détermination du gardien responsable du fait des choses inanimées*, Lyon, 1946.

3. La responsabilité du fait des produits défectueux

Les articles 106-1 et suivants du DOC, issus de la loi n° 24-09 relative à la sécurité des produits et des services, instituent une responsabilité du producteur pour les dommages causés par le défaut de son produit. La difficulté est de savoir si un logiciel ou un modèle d'IA constitue un « produit ». Le législateur européen a tranché par l'affirmative : la directive (UE) 2024/2853 inclut expressément les logiciels, y compris les systèmes d'IA, dans la notion de produit[16]. Cette évolution constitue un argument de droit comparé solide en faveur d'une interprétation extensive du droit marocain.

4. La preuve et l'ancrage territorial

L'opacité des modèles rend la preuve de la faute presque impossible pour la victime. La proposition de directive européenne sur la responsabilité en matière d'IA, qui prévoyait des présomptions de causalité et un accès forcé aux éléments de preuve, a été abandonnée par la Commission en 2025, mais ses mécanismes demeurent une source d'inspiration. Le manquement aux obligations de documentation et de journalisation imposées par le règlement européen sur l'IA pourrait, pour sa part, être qualifié de faute au sens des articles 77 et 78 du DOC. Enfin, l'exigence d'un représentant au Maroc, prévue par l'article 2 de la loi 09-08, offre un point d'ancrage permettant de disposer d'un débiteur identifiable face à un fournisseur étranger.

C. Illustration : l'assistant conversationnel bancaire

Soit une banque marocaine qui propose à ses clients un assistant conversationnel reposant sur le modèle d'un fournisseur étranger, interrogé par API. Un client lui écrit : « J'ai été hospitalisé deux mois, je ne peux plus payer mes échéances de crédit. Mon numéro de compte est… ». En une phrase, il transmet des données d'identification, des données bancaires et des données de santé, lesquelles sont transférées instantanément vers les serveurs du fournisseur.

La banque, qui définit la finalité et choisit l'outil, est responsable du traitement ; le fournisseur est son sous-traitant. Il lui appartenait, avant la mise en service, d'accomplir les formalités auprès de la CNDP, notamment pour les données de santé et le transfert (articles 12, 21, 43 et 44), de conclure le contrat de l'article 24, d'informer les clients (article 5), de sécuriser le dispositif (article 23), par exemple en masquant les numéros de compte avant leur envoi, et de s'assurer du respect du secret bancaire.

Trois incidents permettent d'éprouver la méthode proposée. Si le fournisseur réutilise les conversations pour entraîner son modèle, il sort de son rôle de sous-traitant et devient responsable de ce traitement, conformément à la logique de l'arrêt *Fashion ID* ; la banque reste exposée si elle a accepté des conditions le permettant. Si une fuite survient chez le fournisseur, la banque répond envers son client en sa qualité de responsable, puis dispose d'une action récursoire dont l'efficacité dépend du contrat. Si l'assistant refuse à tort un rééchelonnement, et que ce refus conditionne en fait la décision, la solution de l'arrêt *SCHUFA* conduit à y voir une décision automatisée au sens de

[16]Directive (UE) 2024/2853 du Parlement européen et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux, à transposer au plus tard le 9 décembre 2026.

l'article 11 ; la banque engage alors sa responsabilité au titre de la garde du comportement, sauf recours contre le fournisseur si le dommage procède d'un défaut de structure du modèle.

L'exemple montre que, pour la victime, l'interlocuteur juridique reste presque toujours le déployeur. La répartition effective de la responsabilité se joue ensuite entre le déployeur et le fournisseur, et dépend largement de ce que le premier a négocié, ou omis de négocier, dans le contrat.

Conclusion

La loi 09-08 dispose de principes adaptables à l'intelligence artificielle générative. Ses insuffisances tiennent au rattachement territorial des fournisseurs étrangers, à l'absence de régime organisé de co-responsabilité et à la faiblesse des sanctions. Dans l'attente de la refonte annoncée, la sécurité juridique repose sur une qualification rigoureuse des acteurs par phase, sur la négociation contractuelle et sur la mobilisation du droit commun de la responsabilité civile, en particulier de l'article 88 du DOC.

La réforme à venir gagnerait à consacrer un critère de ciblage des personnes situées au Maroc, à organiser la co-responsabilité et la répartition des obligations entre fournisseurs et déployeurs, à porter les sanctions administratives à un niveau dissuasif, et à prévoir des mécanismes d'allègement de la preuve au profit des victimes. Plusieurs pistes de *lege ferenda* peuvent enfin être envisagées : une responsabilité solidaire des acteurs de la chaîne envers la victime, assortie de recours entre eux ; une imputation de la charge du risque à celui qui peut prévenir le dommage au moindre coût, selon l'analyse de Guido Calabresi ; et une obligation d'assurance pour les déploiements à haut risque.

Références

Textes

- Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, BO n° 5714 du 5 mars 2009.
- Dahir des obligations et contrats, notamment articles 77, 78, 88 et 106-1 et suivants (loi n° 24-09).
- Code pénal marocain, articles 447-2 et 607-3 et suivants.
- Loi n° 31-08 édictant des mesures de protection du consommateur.
- Règlement (UE) 2016/679 (RGPD) ; Règlement (UE) 2024/1689 sur l'intelligence artificielle ; Directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux.

Jurisprudence et décisions

- CJUE, gr. ch., 13 mai 2014, *Google Spain*, aff. C-131/12.
- CJUE, gr. ch., 5 juin 2018, *Wirtschaftsakademie Schleswig-Holstein*, aff. C-210/16.
- CJUE, gr. ch., 10 juillet 2018, *Jehovan todistajat*, aff. C-25/17.
- CJUE, 29 juillet 2019, *Fashion ID*, aff. C-40/17.

- CJUE, gr. ch., 24 septembre 2019, *Google c. CNIL*, aff. C-507/17.
- CJUE, gr. ch., 16 juillet 2020, *Schrems II*, aff. C-311/18.
- CJUE, 7 décembre 2023, *SCHUFA Holding*, aff. C-634/21.
- Cass. 2e civ., 5 janvier 1956, *Oxygène liquide*.
- CNIL, délibération n° SAN-2022-019 du 17 octobre 2022, *Clearview AI*.
- Tribunale di Roma, 18 mars 2026, R.G. n. 4785/2025, *OpenAI c. Garante*.