Le consentement dans le droit de la protection des données personnelles : crise du modèle RGPR et pistes de réforme par le droit comparé Un stage au barreau dans la matière du droit pénal spécial Une épreuve orale de simulation de plaidoirie en matière de droit international public

Auteur : Hendrickx, Malorie
Promoteur(s) : Fischer, Cyril
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit, à finalité spécialisée en droit privé
Année académique : 2025-2026
URI/URL : http://hdl.handle.net/2268.2/26462

LIÈGE université
Droit, Science Politique & Criminologie

Département de Droit

Le consentement dans le droit de la protection des données personnelle : crise du modèle RGPD et pistes de réforme par le droit comparé

Malorie HENDRICKX

Travail de fin d'études

Master en droit à finalité spécialisée en droit privé

Année académique 2025-2026

Recherche menée sous la direction de :

Monsieur Cyril FISCHER

Professeur

RESUME

Le consentement est au cœur du droit européen de la protection des données. Le Règlement général sur la protection des données l'entend comme une décision libre, précise, éclairée et sans ambiguïté et en fait l'une des principales bases légales pour autoriser un traitement. Mais cette approche repose sur une hypothèse de plus en plus contestée, celle d'une personne qui comprend vraiment ce à quoi elle consent, qui dispose d'un vrai choix et qui peut gérer ses préférences avec le temps.

Ce travail s'interroge sur les raisons pour lesquelles ce mécanisme peine à fonctionner dans l'environnement numérique actuel. La première partie expose le cadre juridique du consentement et détaille les quatre conditions qui fondent sa validité.

La deuxième partie explore les obstacles concrets qui empêchent ce consentement d'être libre, spécifique, éclairé et révocable : automatisation de la collecte, absence de véritable alternative, lassitude face aux demandes répétées, incompréhension des politiques de confidentialité. Ces difficultés ne relèvent pas de simples dysfonctionnements, elles révèlent un écart profond entre le mécanisme du consentement et la réalité dans laquelle il s'applique.

La troisième partie ouvre des pistes de réforme. Elle présente d'abord les mécanismes déjà existants dans le droit européen, puis s'appuie sur une comparaison avec les systèmes américain, canadien, indien, singapourien et australien pour dégager des solutions concrètes. Trois axes ressortent : recentrer le consentement sur les situations où il traduit un choix réel, renforcer les obligations des responsables de traitement pour que la protection ne dépende plus uniquement de la vigilance des personnes et encadrer le consentement par des limites matérielles, même en présence d'un accord formel.

REMERCIEMENTS

Je souhaite exprimer ma reconnaissance envers toutes celles et ceux qui, chacun à leur manière, ont contribué à l'aboutissement de ce travail.

Je remercie d'abord mon tuteur, Monsieur Fischer, pour le temps qu'il a consacré à m'accompagner dans ce mémoire. Ses remarques précises et ses conseils m'ont permis d'aller plus loin dans ma réflexion et d'améliorer la qualité de ce travail du début à la fin.

Je remercie aussi ma grand-mère pour sa relecture attentive et bienveillante. Sa disponibilité et son regard extérieur m'ont été d'une aide précieuse.

Je remercie enfin ma mère pour son soutien sans faille, tout au long de ce travail. Sa présence et ses encouragements constants m'ont permis d'avancer avec sérénité.

TABLE DES MATIERES

INTRODUCTION

Le consentement est l'une des notions fondamentales du droit. Il conditionne la formation des contrats, le transfert de droits et la validité de nombreux actes juridiques. Dans tous ces contextes, il remplit la même fonction : reconnaître à l'individu le pouvoir de décider pour lui-même. En matière de données personnelles, cette logique reste intacte. Le consentement fonctionne comme un mécanisme d'autorisation qui confère à la personne concernée un contrôle sur l'utilisation de ses données par autrui[1].

C'est pourquoi le consentement occupe une place centrale dans le droit européen de la protection des données. Il constitue une des bases légales les plus importantes pour légitimer un traitement[2] et le RGPD lui consacre des exigences strictes.

Mais la théorie du consentement repose sur l'hypothèse fragile d'un individu toujours capable de faire un choix volontaire et informé. Dans la réalité numérique actuelle, cette hypothèse est difficile à tenir. Télécharger une application, s'inscrire sur un réseau social, naviguer sur un site, chacun de ces gestes entraîne une demande de consentement acceptée presque automatiquement[3]. Loin de garantir un choix réel, le consentement devient une formalité expédiée en un clic.

Ce décalage entre les ambitions du texte et la réalité de son application soulève une question de fond : le modèle du consentement tel qu'il a été conçu dans le RGPD est-il encore en mesure de remplir sa fonction protectrice ? Et si ce n'est pas le cas, quelles pistes permettraient de le réformer ?

Ce travail tente de répondre à ces questions. La première partie présente le cadre juridique du consentement dans le RGPD en identifiant les quatre conditions qui fondent sa validité. La deuxième partie examine les obstacles concrets qui empêchent à ce consentement d'être libre, spécifique, éclairé et révocable. La troisième partie explore les pistes de réforme, d'abord à travers les mécanismes déjà disponibles en droit européen, puis par le droit comparé en analysant les systèmes américain, canadien, indien, singapourien et australien, avant de proposer des pistes concrètes d'évolution.

---

[1] M. YIP, « Personal Data Protection Act 2012 : Understanding the Consent Obligation », in *Personal Data Protection Digest*, 2017, p. 267.

[2] B. CUSTERS, F. DECHESNE, W. PIETERS, B. W. SCHERMER et S. VAN DER HOF, « Consent and Privacy », in *The Routledge Handbook of the Ethics of Consent*, Londres, Routledge, 2019, p. 250.

[3] *Id*., p. 247.

PARTIE I : LE CONSENTEMENT, UN MÉCANISME EXIGEANT

Avant tout traitement de données, le responsable du traitement doit choisir le fondement juridique le plus adapté parmi les six prévus à l'article 6 du RGPD[4]. Le consentement[5], reconnu par la Charte des droits fondamentaux de l'Union européenne, demeure la principale source de licéité des traitements[6]. Il vise à garantir à la personne concernée un contrôle effectif sur l'utilisation de ses données[7].

Cependant, le consentement au sens du RGPD ne se réduit pas à un simple accord. L'article 4, paragraphe 11, le définit comme une manifestation de volonté libre, spécifique, éclairée et univoque, par laquelle la personne accepte, par déclaration ou acte positif clair, le traitement de ses données. Sa validité repose sur la réunion de ces quatre conditions.

La première condition est la liberté. Le consentement doit être donné sans contrainte[8], ce qui implique que la personne concernée puisse refuser ou retirer son accord sans conséquences. Cela implique également qu'il est interdit de conditionner l'accès à un service à l'acceptation d'un traitement qui n'est pas nécessaire à celui-ci[9]. Pour que cette liberté soit réelle, elle doit se traduire par la forme même du consentement, qui exige un acte positif et explicite de la personne concernée[10].

Cependant, cette liberté reste difficile à garantir lorsque des rapports de force peuvent influencer la décision de la personne, qui pourrait craindre les conséquences d'un refus. Le RGPD cite notamment les relations de travail et les rapports avec les autorités publiques comme exemples de tels contextes[11].

La deuxième condition est la spécificité. Si un traitement poursuit plusieurs finalités, chacune d'elles nécessite un consentement distinct. Il faut pouvoir accepter certains usages tout en en refusant d'autres[12], afin que l'accord corresponde précisément à l'utilisation des données[13].

---

[4] E.D.P.B., *Lignes directrices 05/2020 sur le consentement au sens du règlement (UE) 2016/679*, révisées et adoptées le 4 mai 2020, § 2 ; D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *B. U. L. Rev.*, vol. 104, 2024, p. 602-603.

[5] D. J. SOLOVE, *id.*, p. 603.

[6] Y. POULLET, « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.*, 2019/1-2, n° 122-123, p. 3.

[7] O. TAMBOU, *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020, p. 129 ; Y. POULLET, *id.*, p. 5.

[8] 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 (ci-après « RGPD »), J.O.U.E. L 119, 4 mai 2016, art. 7.

[9] RGPD précité, art. 7, §4 ; Y. POULLET, *op. cit.,* p. 6 et p. 7 ; O. TAMBOU, *op. cit.*, p. 130 - 131 ; GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, « Guidelines on consent under Regulation 2016/679 », adoptées le 10 avril 2018, p. 3.

[10] RGPD précité, consid. 32 ; O. TAMBOU, *id.*, p. 132 et 135 ; A. BENSOUSSAN, « C » in *La protection des données à caractère personnel de A à Z*, Bruxelles, Bruylant, 2017, p. 47.

[11] RGPD précité, consid. 43 ; O. TAMBOU, *id.*, p. 131-132.

[12] O. TAMBOU, *ibid.* ; A. BENSOUSSAN, *op. cit.*, p. 47 ; RGPD précité, consid. 32.

[13] O. TAMBOU, *id.*, p. 132.

La troisième condition est l'information. Le consentement n'est éclairé que si la personne a reçu au préalable des informations claires sur l'identité du responsable du traitement, le type de données collectées, les destinataires et la finalité du traitement[14].

La quatrième condition est la révocabilité. La personne doit pouvoir retirer son consentement à tout moment, aussi facilement qu'elle l'a donné[15]. Ce retrait ne vaut que pour l'avenir et ne remet pas en cause les traitements déjà réalisés[16].

Ces quatre conditions forment un cadre exigeant. Le législateur européen souhaitait faire du consentement un véritable outil de protection et non une simple formalité expédiée en un clic. Ce décalage avec la réalité numérique, que nous allons examiner, soulève ainsi une difficulté majeure.

[14] RGPD précité, art. 13 et consid. 42 ; Y. POULLET, *op. cit.*, p. 7 ; O. TAMBOU, *op. cit.*, p. 134.
[15] O. TAMBOU, *id.*, p. 132 et 142 ; RGPD précité, art. 7, §3 et consid. 42 ; A. BENSOUSSAN, *op. cit.*, p. 48.
[16] Y. POULLET, *op. cit.*, p. 11.

PARTIE II : LE CONSENTEMENT, UN MÉCANISME FRAGILISÉ

Titre I : Les obstacles au consentement volontaire

Le droit exige un consentement libre. Cependant, la réalité numérique s'y prête mal. L'automatisation de la collecte, l'absence d'alternative, la manipulation par les interfaces et la lassitude générée par la surcharge de demandes rendent le consentement volontaire de plus en plus difficile à obtenir.

Chapitre 1 : L'automatisation de la collecte et l'internet des objets

Un premier obstacle au caractère volontaire du consentement tient à l'automatisation croissante de la collecte des données. Le modèle prévu par le RGPD suppose qu'il existe un moment précis où un choix peut être exercé. Quand la collecte se fait de façon passive et continue, sans que la personne en ait vraiment conscience, ce moment n'existe tout simplement pas[17].

Ce phénomène est particulièrement visible avec l'Internet des objets[18]. Les appareils connectés collectent des données en continu, souvent en arrière-plan, et les utilisateurs en ont généralement moins conscience que lors d'un usage plus classique d'internet[19]. De plus, la plupart de ces appareils ne disposent pas d'interfaces permettant de recueillir un accord explicite[20].

La difficulté ne touche pas seulement les acheteurs de ces appareils. Les invités, proches ou passants n'ont signé aucun contrat mais leurs données sont tout de même collectées, sans possibilité de s'y opposer [21].

Même pour l'utilisateur ayant initialement consenti, cet accord n'est souvent donné qu'une seule fois, lors de la configuration. Les conditions peuvent ensuite évoluer et refuser les nouvelles conditions peut rendre l'appareil inutilisable. Dans ce contexte, le choix n'est pas réellement libre, car refuser revient à perdre l'usage de l'appareil[22]. Le consentement ainsi obtenu perd alors une grande partie de sa valeur[23].

---

[17] C. F. KERRY, « Why protecting privacy is a losing game today - and how to change the game », disponible sur www.brookings.edu, 12 juillet 2018 ; D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 621.

[18] S.-A. ELVY, *A Commercial Law of Privacy and Security for the Internet of Things*, Cambridge, Cambridge University Press, 2021, p. 36.

[19] C. F. KERRY, *op. cit.* ; L.M. TANCZER, M. CARR, I. BRASS, I. STEENMANS et J. BLACKSTOCK, *IoT and Its Implications for Informed Consent*, PETRAS IoT Hub, STEaPP, Londres, 25 juillet 2017, disponible sur www.ssrn.com, p. 6.

[20] L.M. TANCZER, M. CARR, I. BRASS, I. STEENMANS et J. BLACKSTOCK, *id.*, p. 2 et 18 ; S.-A. ELVY, *op. cit.*, p. 120 ; D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 608.

[21] L.M. TANCZER, M. CARR, I. BRASS, I. STEENMANS et J. BLACKSTOCK, *id.*, p. 23 ; S.-A. ELVY, *id.*, p. 36.

[22] L.M. TANCZER, M. CARR, I. BRASS, I. STEENMANS et J. BLACKSTOCK, *id.*, p. 6 ; S.-A. ELVY, *id.*, p. 149.

[23] C. F. KERRY, *op. cit.*

Le problème dépasse un simple défaut d'application des règles. Le consentement, tel qu'il est conçu, suppose un échange clair à un moment précis entre des parties informées. L'Internet des objets ne permet pas ce type d'échange[24].

Chapitre 2 : L'absence d'alternative réelle

En théorie, chacun peut refuser le traitement de ses données. Mais dans de nombreux cas, ce refus entraîne l'impossibilité d'accéder au service[25]. Le choix se limite alors à accepter ou à renoncer[26], ce qui remet en cause la liberté du consentement.

Ce sentiment est largement partagé : 58 % des Européens estiment ne pas avoir réellement le choix de consentir pour accéder à un produit ou à un service[27]. Le consentement devient alors une formalité imposée, accordée faute d'alternative[28] et perd ainsi une grande partie de sa fonction protectrice.

Chapitre 3 : La fatigue du consentement

En imposant un consentement distinct pour chaque finalité, le RGPD a multiplié les sollicitations adressées aux utilisateurs[29]. Dans un environnement où les données sont générées en continu, il devient impossible d'examiner chaque demande avec attention[30]. Le nombre d'acteurs collectant des données dépasse ce qu'une personne peut raisonnablement gérer[31].

Le consentement devient alors un automatisme. L'objectif n'est plus de comprendre, mais de faire disparaître les fenêtres intrusives. Les bannières de cookies en sont l'exemple le plus visible. Censées informer, elles agissent comme des interruptions permanentes et la plupart des utilisateurs cliquent sur « accepter » sans vraiment savoir à quoi ils s'engagent[32]. Le Comité européen de la protection des données reconnaît d'ailleurs que la majorité des informations fournies ne sont plus lues[33].

---

[24] S.-A. ELVY, *op. cit.*, p. 120 ; C. F. KERRY, *op. cit.*

[25] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 608 ; F. ZUIDERVEEN BORGESIUS, S. KRUIKEMEIER, S. C. BOERMAN, et N. HELBERGER,« Tracking Walls, Take-It-Or-Leave-It Choices, The GDPR, and The ePrivacy Regulation », *E.D.P.L.*, vol. 3, n° 3, p. 6.

[26] T. SIGMUND, « Attention Paid to Privacy Policy Statements », *Information*, vol. 12, n° 4, 2021, p. 3 ; C.A. TSCHIDER, « Meaningful Choice : A History of Consent and Alternatives to the Consent Myth », *N.C. J.L. & Tech.*, vol. 22, n° 4, 2021, p. 636.

[27] F. ZUIDERVEEN BORGESIUS, S. KRUIKEMEIER, S. C. BOERMAN, et N. HELBERGER, *op. cit.*, p. 12-13.

[28] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 608 et 612.

[29] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 626.

[30] *Ibid.* ; C. UTZ, M. DEGELING, S. FAHL, F. SCHAUB et T. HOLZ, « (Un)informed Consent : Studying GDPR Consent Notices in the Field », *C.C.S.'19*, 2019, p. 973.

[31] D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *Harv. L. Rev.*, vol. 126, 2013, p. 1888.

[32] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 624-625 ; B. W. SCHERMER, B. CUSTERS et S. VAN DER HOF, « The crisis of consent : how stronger legal protection may lead to weaker consent in data protection », *Ethics Inf. Technol.*, n° 16, 2014, p. 177.

[33] E.D.P.B., « Lignes directrices 05/2020 sur le consentement au sens du règlement (UE) 2016/679 », *op. cit.*, §§ 87-88.

Il en résulte une désensibilisation progressive. Par souci de rapidité, les utilisateurs acceptent les options par défaut ou la solution la plus rapide, souvent sans y réfléchir[34]. Le droit suppose que chacun lit et comprend ce qu'il accepte, ce qui n'est pas le cas en pratique[35].

Titre II : Les obstacles au consentement spécifique

Le RGPD impose un consentement spécifique. Chaque finalité doit être identifiable et distincte et un bouton d'acceptation global n'est conforme que si l'utilisateur peut aussi consentir séparément à chaque finalité[36]. Cette exigence se heurte à deux difficultés en pratique.

La première difficulté est que les choix proposés restent souvent trop généraux. Dans de nombreux cas, l'utilisateur ne peut pas refuser certaines pratiques tout en acceptant d'autres. C'est tout ou rien. L'utilisateur accepte alors un ensemble de conditions qu'il n'a pas réellement examinées[37].

La seconde difficulté est opposée. Lorsque les choix sont trop nombreux ou trop détaillés, ils deviennent impossibles à traiter. Demander un consentement distinct pour chaque finalité, responsable du traitement et type de données submerge l'utilisateur[38]. Des études montrent que l'excès d'informations finit par nuire à la décision plutôt que de l'éclairer[39]. En pratique, la plupart des interactions avec les fenêtres de consentement se limitent à la première page. Ce qui n'est pas immédiatement visible est tout simplement ignoré[40]. Placer des options sur les pages suivantes revient à les rendre inexistantes[41].

Le consentement spécifique suppose que l'utilisateur puisse distinguer et évaluer chaque finalité. Or, ce n'est ni ce que les interfaces permettent, ni ce que les utilisateurs font.

---

[34] H. CHOI, J. PARK et Y. JUNG, « The role of privacy fatigue in online privacy behavior », *Computers in Human Behavior*, vol. 81, 2018, p. 44 ; E. CORREN, « The Consent Burden in Consumer and Digital Markets », *Harv. J.L. & Tech.*, vol. 36, 2023, p. 593.

[35] B. W. SCHERMER, B. CUSTERS et S. VAN DER HOF, *op. cit.*, p. 2.

[36] RGPD précité, art. 6, §1, a) ; M. NOUWENS, I. LICCARDI, M. VEALE, D. KARGER et L. KAGAL, « Dark Patterns after the GDPR : Scraping Consent Pop-ups and Demonstrating their Influence », CHI'20, 2020, p. 2.

[37] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 622.

[38] D. J. SOLOVE, *id.*, p. 622-623.

[39] N. S. KIM, *Consentability: Consent and Its Limits*, Cambridge, Cambridge University Press, 2019, p. 13.

[40] M. NOUWENS, I. LICCARDI, M. VEALE, D. KARGER et L. KAGAL, *op. cit.*, p. 8.

[41] *Id.*, p. 10.

Titre III : Les obstacles au consentement éclairé

Donner un consentement éclairé suppose de comprendre ce à quoi on consent. Or, les politiques de confidentialité sont rarement lues ou comprises et les utilisateurs manquent souvent de connaissances nécessaires pour en mesurer les enjeux.

Chapitre 1 : L'absence de lecture

Les politiques de confidentialité ne sont pas lues. Ce constat est confirmé par les enquêtes qui montrent que la grande majorité des utilisateurs ne les consulte jamais ou très rarement[42]. Le consentement repose donc souvent sur un réflexe, plutôt que sur une compréhension réelle de ce qui est accepté[43].

Plusieurs raisons expliquent cela. D'abord, le consentement est souvent demandé alors que l'utilisateur souhaite accéder rapidement à un contenu précis et n'a ni le temps ni l'envie de lire un texte juridique[44]. Sur smartphone, c'est encore moins réaliste[45].

Le mécanisme lui-même n'encourage pas la lecture. Un clic ou une case cochée suffit à exprimer un accord valable, sans avoir ouvert le moindre document[46]. Et même lorsque la politique est affichée, rien n'oblige à la lire. On peut très bien la faire défiler sans y prêter attention[47]. Le temps que les gens consacrent à accepter est d'ailleurs bien inférieur à celui qu'il faudrait pour lire ce à quoi ils consentent[48].

S'ajoute à cela la longueur des documents. Lire toutes les politiques de confidentialité auxquelles un utilisateur est exposé prendrait plusieurs centaines d'heures par an[49]. Le consentement éclairé demeure donc largement théorique.

Chapitre 2 : L'incompréhension des politiques de confidentialité

Une politique de confidentialité est avant tout un document juridique technique[50]. Elle doit expliquer quelles données sont collectées, à quelles fins et avec qui elles sont partagées[51]. Ces

---

[42] European Commission, Directorate-General for Justice and Consumers et Kantar, *The General Data Protection Regulation - Report*, Publications Office, 2019, p. 16 ; X, « Final Report Summary - CONSENT », disponible sur www.cordis.europa.eu, 7 août 2014 ; X, « Europäischer Datenschutztag: Umfrage zeigt: Mehrheit der Deutschen findet Datenschutz im Netz zu kompliziert », disponible sur www.eco.de, 27 janvier 2025.

[43] F. H. CATE, « The Failure of Fair Information Practice Principles », *Consumer Protection in the Age of the Information Economy*, J. K. Winn (dir.), Washington, Ashgate, 2006, p. 361 ; T. SIGMUND, *op. cit.*, p. 2 ; D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 606.

[44] D. J. SOLOVE, *id.*, p. 625.

[45] *Id.*, p. 626.

[46] D. J. SOLOVE, *id.*, p. 605-606 ; RGPD précité, consid. 32.

[47] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 606.

[48] R. B. KAR et X. YU, « The Contractual Death and Rebirth of Privacy », *Harv. J. L. & Tech.*, vol. 38, 2024, p. 1126-1127.

[49] *Id.*, p. 1127.

[50] I. WAGNER, « Privacy Policies Across the Ages : Content and Readability of Privacy Policies 1996-2021 », *A.C.M. Trans. Priv. Sec.*, vol. 26, n° 3, art. 32, 2023, p. 1.

[51] *Ibid*.

informations sont bien mises à disposition, mais leur compréhension reste difficile pour la plupart des utilisateurs. Ces documents sont souvent longs, structurés selon des logiques juridiques peu familières et rédigés dans un langage complexe[52]. La question n'est donc pas seulement la disponibilité de l'information, mais son accessibilité réelle.

Le RGPD impose une obligation d'information[53], mais pas une de compréhension effective. Être informé ne signifie pas avoir compris et un consentement donné sans compréhension suffisante perd une grande partie de sa portée[54]. Malgré l'exigence d'un langage clair et simple, les politiques de confidentialité restent largement inadaptées à leur public[55].

Chapitre 3 : Le manque de connaissances des utilisateurs

Le problème ne réside pas seulement dans la forme des documents. Les responsables du traitement doivent fournir une information précise et complète[56]. Mais cette précision aboutit souvent à des documents trop techniques pour être réellement compréhensibles[57]. À l'inverse, une simplification excessive rend l'information trop vague pour être utile[58]. Les deux exigences se contredisent et l'équilibre est difficile à trouver.

S'ajoute à cela le niveau de connaissance des utilisateurs. Évaluer les enjeux liés à la protection des données suppose de comprendre des mécanismes complexes, comme les risques d'agrégation, d'inférence ou d'utilisation secondaire, qui dépassent largement la compréhension de la plupart des personnes[59]. Beaucoup surestiment leur niveau de protection ou pensent à tort que l'existence d'une politique de confidentialité garantit la

---

[52] A. ACQUISTI, A. IDRIS et L. BRANDIMARTE, « Gone in 15 Seconds: The Limits of Privacy Transparency and Control », *I.E.E.E. Sec. & Priv.*, vol. 11, n° 4, p. 73 ; J. KORUNOVSKA, B. KAMLEITNER et S. SPIEKERMANN, « The Challenges and Impact of Privacy Policy Comprehension », *Privacy Policy Comprehension: Challenges and Impact*, J. Korunovska et al. (dir.), 2020, p. 2 ; D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 615 ; A. ACQUISTI, L. BRANDIMARTE et G. LOEWENSTEIN, « Privacy and human behavior in the age of information », *Science*, vol. 347, n° 6221, p. 513 ; I. WAGNER, *op. cit.*, p. 1.

[53] RGPD précité, art. 13.

[54] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 615 ; N. S. KIM, *op. cit.*, p. 125.

[55] D. J. SOLOVE, *id.*, p. 616 ; D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1885.

[56] F. H. CATE, *op. cit.*, p. 362 ; C. F. KERRY, *op. cit.*

[57] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 616-617 ; C. F. KERRY, *ibid.* ; D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1885-1886.

[58] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 617 ; D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1885-1886.

[59] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *id.*, p. 618-620 ; D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *id.*, p. 1886.

confidentialité totale de leurs données[60]. Ces croyances affaiblissent encore la portée réelle du consentement[61].

Mais le problème va plus loin. Même si un utilisateur lit et comprend ce à quoi il consent, les conséquences réelles de ce consentement lui échappent souvent au moment de la décision. Les implications futures du traitement des données sont généralement imprévisibles lors de la collecte, rendant toute décision pleinement éclairée difficile, voire impossible[62].

Titre IV : Les obstacles à la révocation du consentement

Le RGPD exige que retirer son consentement soit aussi simple que de le donner[63]. Cependant, même si cette exigence est respectée, la révocation se heurte à un obstacle plus profond. Pour révoquer un consentement, il faut savoir ce à quoi on a consenti. Or, les utilisateurs ayant accepté via un bouton par défaut se souviennent rarement de leur choix et la plupart changent d'avis quand on leur en explique la portée réelle[64]. Révoquer un consentement dont on ignore l'étendue est donc très difficile en pratique.

***

Le problème ne résulte donc pas d'une mauvaise application des règles existantes. Il montre que le consentement, tel qu'il a été conçu, fonctionne difficilement dans l'environnement numérique actuel. Il ne s'agit donc plus seulement de mieux l'encadrer, mais de repenser sa place dans ce contexte.

---

[60] C. J. HOOFNAGLE et J. M. URBAN, « Alan Westin's Privacy Homo Economicus », *Wake Forest L. Rev.*, vol. 49, 2014, p. 305 ; K. MARTIN, « Privacy Notices as Tabula Rasa : An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online », *J.P.P. & M.*, 2014 ; A. SMITH, « Half of online Americans don't know what a privacy policy is », disponible sur www.pewresearch.org, 4 décembre 2014 ; D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *id.*, p. 1886.

[61] D. J. SOLOVE, « Murky consent: an approach to the fictions of consent in privacy law », *op. cit.*, p. 618.

[62] D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1893 et 1902.

[63] RGPD précité, art. 7, §3.

[64] D. MACHULETZ et R. BÖHME, *op. cit.*, p. 491-493.

PARTIE III : LE CONSENTEMENT, UN MÉCANISME À RENFORCER

Titre I : Renforcer le consentement

Les développements précédents ont montré que le consentement rencontre de nombreux obstacles en pratique. Malgré ces difficultés, le droit européen a maintenu ce mécanisme, tout en renforçant l'encadrement de sa demande et de son utilisation. Ce sujet présente les outils adoptés à cette fin, en distinguant ceux qui visent directement les pratiques des entreprises de ceux qui encadrent le consentement au niveau des principes structurels du règlement.

Chapitre 1 : Les mécanismes qui agissent sur les pratiques

Section 1 : L'encadrement des interfaces numériques

I. Le consentement face aux cookies et autres traceurs

Les cookies sont de petits fichiers texte déposés sur l'appareil de l'utilisateur pendant sa navigation[65]. Ils servent à reconnaître le navigateur, à retenir les préférences ou à suivre l'activité en ligne[66].

Le droit européen pose un cadre à deux niveaux. La directive « ePrivacy » exige d'obtenir le consentement de l'utilisateur avant tout dépôt ou lecture d'information sur son appareil, sauf pour les traceurs strictement nécessaires au service[67]. Cependant, cette règle a malheureusement entraîné la prolifération des bannières cookies, dont l'impact sur les utilisateurs a été analysé en Partie II.

Face à cette situation, la Commission européenne a présenté en 2017 un projet de règlement pour remplacer la directive. L'article 10 proposait que les utilisateurs règlent leurs préférences directement dans leur navigateur, évitant ainsi les demandes répétées sur chaque site[68]. Toutefois, après huit ans de blocage, la Commission a finalement retiré ce projet en 2025, le jugeant dépassé par les évolutions législatives récentes[69].

---

[65] V. MBAEZUE, « "Allow/Accept Cookie". Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) and the E-privacy Directive 2002/58/EC (amended in 2009) stance on Web Cookies », disponible sur www.ssrn.com, 7 juillet 2024, p. 1.

[66] E. KOSTA, « Peeking into the cookie jar: the European approach towards the regulation of cookies », *Int. J. L. Inf. Technol.*, vol. 21, n° 4, 2013, p. 380.

[67] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, J.O.C.E., L 201, 31 juillet 2002, modifiée par la directive 2009/136/CE du 25 novembre 2009, J.O.U.E., L 337, 18 décembre 2009, art. 5, §3.

[68] Commission européenne, proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, COM(2017) 10 final, 10 janvier 2017, art. 10, §§1-2.

[69] C. BOUCKAERT, « Le règlement e-Privacy : c'est fini », disponible sur www.idfrights.org, 12 février 2025.

Mais la réforme ne s'est pas arrêtée là. En novembre 2025, la Commission a présenté la proposition de règlement « Digital Omnibus ». Elle intègre les règles sur les cookies directement dans le RGPD, via deux nouveaux articles 88 *bis* et *ter*[70]. Le texte prévoit l'expression du consentement en un seul clic, la gestion centralisée des préférences via le navigateur et l'interdiction de renouveler une demande pendant au moins six mois après un refus[71]. Ces innovations montrent que le législateur européen ne cherche plus seulement à encadrer le consentement, mais à en repenser les modalités.

II. Le consentement face aux dark patterns

Les interfaces trompeuses désignent des parcours numériques conçus pour orienter l'utilisateur vers une décision qu'il n'aurait pas prise librement, souvent au profit de la plateforme et au détriment de ses propres intérêts. Les bandeaux cookies en sont le terrain d'application le plus courant[72].

Depuis l'entrée en vigueur du RGPD, plusieurs études ont montré que ces interfaces utilisent fréquemment de telles techniques[73]. Le droit européen encadre ces pratiques par différents outils. Le principe de loyauté interdit les traitements trompeurs ou préjudiciables. La définition du consentement, qui exige un choix libre et éclairé, exclut les pratiques influençant indûment la décision[74]. L'article 25 du RGPD impose quant à lui que les choix proposés soient présentés de manière objective et non manipulatoire[75].

Ces principes ont conduit à des sanctions concrètes. En 2021, la Commission Nationale de l'Informatique et des Libertés a sanctionné Google et Facebook pour avoir rendu le refus des cookies plus difficile que leur acceptation, en violation de l'exigence d'un consentement aussi facile à refuser qu'à accepter[76]. Le C.E.P.D. a également publié des lignes directrices détaillant les situations problématiques et proposant des recommandations concrètes pour concevoir des interfaces conformes[77].

L'encadrement des dark patterns vise à garantir que le choix exprimé reflète une volonté réelle et non le résultat d'une interface conçue pour influencer la décision. Sans ce contrôle, le consentement pourrait respecter la forme tout en restant dépourvu de sens.

---

[70] Commission européenne, proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/679 en ce qui concerne les règles relatives au consentement et les règles relatives aux cookies, COM(2025) 765 final, 19 novembre 2025.

[71] *Id*., art. 88 bis et ter

[72] E.D.P.B., « Lignes directrices 03/2022 relatives aux interfaces trompeuses », disponible sur www.edpb.europa.eu, 13 octobre 2022, p. 4.

[73] M. OURRAHTE, F.-E. ZIANI et A. EL-YAHYAOUI, « Between Compliance and Illusion: An International Comparative Study of Cookie Consent Mechanisms », disponible sur www.papers.ssrn.com, 13 octobre 2025, p. 7.

[74] E.D.P.B., « Lignes directrices 03/2022 relatives aux interfaces trompeuses », *op. cit.*, p. 13 et 16.

[75] E.D.P.B., *id*., § 16 ; RGPD précité, art. 5, §1, a).

[76] Commission nationale de l'informatique et des libertés (ci-après « C.N.I.L. »), formation restreinte, délibération n° SAN-2021-023, 31 décembre 2021, disponible sur www.legifrance.gouv.fr, pt. 85 et s. ; C.N.I.L., formation restreinte, délibération n° SAN-2021-024, 31 décembre 2021, disponible sur www.legifrance.gouv.fr, pt. 57 et s.

[77] E.D.P.B., « Lignes directrices 03/2022 relatives aux interfaces trompeuses », *op. cit.*, p. 6 et 9.

Section 2 : Le rôle des autorités de contrôle

Le RGPD pose des conditions strictes pour la validité du consentement qui ne sont effectives que si elles sont vérifiées. C'est précisément le rôle des autorités de contrôle[78].

Le règlement leur confie la surveillance de son application, le traitement des plaintes, la conduite d'enquêtes, l'ordonnance de mises en conformité et la sanction des manquements[79]. Cette structure institutionnelle est l'un des piliers du régime européen de protection des données[80].

Leur intervention est d'autant plus essentielle que les utilisateurs ne comprennent pas toujours pleinement ce à quoi ils consentent. Les traitements sont souvent complexes, impliquent de nombreux acteurs et leurs conséquences sont difficiles à anticiper[81]. Dans ces conditions, le consentement seul ne garantit pas une protection effective.

La Cour de justice l'a rappelé à deux reprises. Dans *Schrems I*, elle a exigé que les autorités nationales examinent avec diligence les plaintes des personnes concernées[82]. Dans *Schrems II*, elle a précisé qu'elles doivent, si nécessaire, suspendre ou interdire un traitement lorsque les garanties prévues par le droit de l'Union ne sont pas respectées[83].

En pratique, cette intervention prend plusieurs formes : publication de lignes directrices, recommandations et sanctions. La décision de la CNIL condamnant Google et Facebook pour avoir rendu le refus des cookies plus difficile que leur acceptation en est un exemple[84]. Ce type de décision confère au consentement une portée concrète que le texte seul ne peut garantir.

Cette protection dépend toutefois des moyens dont disposent les autorités. Un volume élevé de plaintes et des ressources limitées peuvent réduire leur capacité d'intervention[85].

---

[78] C. J. HOOFNAGLE, B. VAN DER SLOOT et F. ZUIDERVEEN BORGESIUS, « The European Union General Data Protection Regulation: what it is and what it means », *Information & Communications Technology Law*, 2019, vol. 28, p. 93.

[79] RGPD précité, art. 57 et 58 ; Charte des droits fondamentaux de l'Union européenne (ci-après « Ch. dr. fond. UE »), J.O.U.E., C 326, 26 octobre 2012, art. 8, §3.

[80] O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, 2015, p. 26-28.

[81] D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1882-1884 et 1894.

[82] C.J. (gde ch.), arrêt Schrems c. Data Protection Commissioner, 6 octobre 2015, C-362/14, EU:C:2015:650, points 63 à 65.

[83] C.J. (gde ch.), arrêt Data Protection Commissioner c. Facebook Ireland Ltd et Schrems, 16 juillet 2020, C-311/18, EU:C:2020:559, pnt 135 ; D. ERDOS, « Towards Effective Supervisory Oversight? », *Cambridge Legal Studies Research Paper*, 2022, p. 1-3 et 6-7.

[84] C.N.I.L., formation restreinte, délibération n° SAN-2021-023 précitée, dispositif ; C.N.I.L., formation restreinte, délibération n° SAN-2021-024 précitée, dispositif.

[85] C. J. HOOFNAGLE, B. VAN DER SLOOT et F. ZUIDERVEEN BORGESIUS, *op. cit.*, p. 93 ; D. ERDOS, *op. cit.*, p. 1-3.

Chapitre 2 : Les principes qui encadrent le consentement en amont

Section 1 : Les principes structurels

I. L'accountability

Le RGPD ne se contente pas d'exiger que le consentement soit valablement recueilli. Il impose également au responsable du traitement d'être en mesure d'en démontrer l'existence et la validité[86]. Cette exigence découle directement de l'article 5, §2, selon lequel le responsable du traitement doit non seulement respecter les principes du règlement, mais aussi pouvoir en apporter la preuve[87].

La protection des données ne dépend pas seulement de la vigilance de la personne concernée. Le responsable du traitement doit mettre en place des mesures organisationnelles et techniques pour garantir un consentement libre, spécifique, éclairé et univoque. Il doit également adapter ses interfaces, procédures et documentation en conséquence[88].

En pratique, le consentement ne peut plus être réduit à une simple formalité. Il doit pouvoir être justifié et vérifié à tout moment. Cette logique de responsabilité continue en renforce la portée réelle[89].

II. La transparence

La transparence conditionne directement la validité du consentement. Pour qu'il soit éclairé, la personne concernée doit avoir reçu au préalable une information concise, accessible et rédigée en termes clairs et simples[90].

Cette information doit inclure les éléments essentiels du traitement : l'identité du responsable du traitement, les finalités poursuivies et la possibilité de retirer son consentement[91]. Les lignes directrices sur la transparence insistent sur l'importance d'un langage clair, d'une information structurée et de l'absence de formulations vagues ou inutilement techniques[92].

La transparence ne consiste pas seulement à rendre l'information disponible. Elle exige qu'elle soit réellement compréhensible. Sinon, le consentement donné manque de fondement concret et perd l'essentiel de sa valeur[93].

---

[86] RGPD précité, art. 7, §1 et consid. 42.
[87] *Id.*, art. 5, §2 et consid. 74.
[88] *Id*., art. 24, §1, 25, §1 et consid. 78.
[89] O. LYNSKEY, *op. cit.,* p. 260-261 ; C. J. HOOFNAGLE, B. VAN DER SLOOT et F. ZUIDERVEEN BORGESIUS, *op. cit.*, p. 79-80.
[90] RGPD précité, art. 12, §1 et consid. 39 et 58.
[91] *Id*., art. 13, §1, a) et c), et art. 13, §2, c) ; E.D.P.B., *Lignes directrices 05/2020 sur le consentement au sens du règlement (UE) 2016/679*, *op. cit.*, §§ 64 et 67.
[92] GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, « Guidelines on consent under Regulation 2016/679 », *op. cit*., p. 7-9, 13-14 et 16-17.
[93] D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1880-1882 ; D. J. SOLOVE, « Murky consent », *op. cit.*, p. 614-617.

L'*accountability* et la transparence poursuivent une même logique. L'une place la responsabilité sur le responsable du traitement, l'autre garantit que la personne concernée dispose des informations nécessaires pour faire un choix réel. Ensemble, elles visent à faire du consentement un acte qui engage véritablement celui qui le recueille et celui qui le donne et non une simple formalité.

Section 2 : La pluralité des bases légales

Le consentement n'est pas la seule base juridique prévue par le RGPD. L'article 6 en prévoit plusieurs, permettant de justifier un traitement sans recourir à l'accord de la personne concernée. Par exemple, le traitement peut être nécessaire à l'exécution d'un contrat, au respect d'une obligation légale ou à la réalisation d'une mission d'intérêt public[94].

Cette diversité de bases juridiques est essentielle. Elle évite que le consentement soit utilisé par défaut dans des situations inadaptées. Le consentement n'est pas approprié lorsque le traitement est nécessaire à l'exécution d'un contrat ou lorsque la personne concernée ne dispose pas d'une réelle liberté de choix[95]. Recourir au consentement dans ces situations ne ferait que créer une apparence de contrôle là où il n'en existe pas.

En réservant le consentement aux situations où un véritable choix existe, le système lui rend sa fonction initiale. Il sert alors à exprimer une préférence réelle et non à justifier des traitements imposés ou inévitables. Ce recentrage préserve la valeur du consentement[96].

***

Le droit européen a donc mis en place des mécanismes concrets pour soutenir le consentement. Corriger les excès ne revient pas à résoudre le problème de fond. D'autres systèmes ont tenté d'aller plus loin.

---

[94] RGPD précité, art. 6, §1 et consid. 40 et 44.

[95] *Id.*, consid. 43 ; E.D.P.B., *Lignes directrices 05/2020 sur le consentement au sens du règlement (UE) 2016/679*, *op. cit.*, §§ 155-163.

[96] O. LYNSKEY, *op. cit.*, p. 31-32 ; C. J. HOOFNAGLE, B. VAN DER SLOOT et F. ZUIDERVEEN BORGESIUS, *op. cit.*, p. 78-80.

Titre II : S'inspirer d'autres modèles

Chapitre 1 : L'exemple américain : un consentement inversé

La protection des données aux États-Unis suit une logique très différente de celle du RGPD. Alors que l'Europe demande un accord avant toute collecte, les États-Unis autorisent la collecte sauf si une règle l'interdit. C'est donc à chaque personne de s'opposer si elle le souhaite. Ce changement de responsabilité, typique du modèle *notice and choice*, guide tout ce chapitre.

Section 1 : Le cadre général

Il n'existe pas de loi fédérale unique sur la protection des données aux États-Unis. Le système s'appuie sur plusieurs lois sectorielles et locales, ce qui crée des niveaux de protection différents selon les domaines[97]. Contrairement à l'Union européenne, la collecte de données est généralement permise, sauf interdiction spécifique[98]. Le législateur intervient seulement pour répondre à des besoins précis, sans chercher à encadrer tous les traitements de données personnelles[99].

Dans ce système fragmenté, la *Federal Trade Commission* occupe une place centrale. Grâce au *FTC Act*, elle peut sanctionner les pratiques déloyales ou trompeuses, notamment si une entreprise ne respecte pas sa politique de confidentialité[100]. Avec le temps, ces décisions sont devenues la principale source de régulation en matière de données personnelles[101].

Section 2 : La place du consentement

Le système américain suit surtout le modèle *notice and choice*. Les entreprises publient des politiques de confidentialité qui expliquent comment elles collectent et utilisent les données[102]. C'est ensuite à chaque personne de s'opposer si elle le souhaite. Par défaut, le traitement est autorisé tant qu'il n'y a pas d'opposition claire[103]. La protection des données dépend donc de l'action de l'individu, qui doit agir pour limiter l'usage de ses informations.

---

[97] D. J. SOLOVE, *Understanding Privacy*, Cambridge, Harvard University Press, 2008, p. 3 ; S. S. BAKARE, A. O. ADENIYI, C. U. AKPUOKWE et N. E. ENEH, « Data privacy and compliance : a comparative review of the EU GDPR and USA regulations », *Computer Science & IT Research Journal*, vol. 5, n° 3, 2024, p. 530.

[98] D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1897 ; P. M. SCHWARTZ, « The EU-US Privacy Collision : A Turn to Institutions and Procedures », *Harv. L. Rev.*, vol. 126, 2013, p. 1976.

[99] P. M. SCHWARTZ, *id*., p. 1976.

[100] A. B. SERWIN, « The Federal Trade Commission and Privacy : Defining Enforcement and Encouraging the Adoption of Best Practices », *San Diego L. Rev.*, vol. 48, 2011, p. 814 et 817 ; D. J. SOLOVE et W. HARTZOG, « The FTC and The New Common Law of Privacy », *Colum. L. Rev.*, vol. 114, 2014, p. 588.

[101] D. J. SOLOVE et W. HARTZOG, *ibid*.

[102] *Id*., p. 592 ; S. S. BAKARE, A. O. ADENIYI, C. U. AKPUOKWE et N. E. ENEH, *op. cit.*, p. 532.

[103] D. J. SOLOVE et W. HARTZOG, *id.*, p. 592 ; D. J. SOLOVE, « Privacy Self-Management and the Consent Dilemma », *op. cit.*, p. 1883-1884.

Ce système d'*opt-out* existe dans plusieurs lois fédérales. Par exemple, le *CAN-SPAM Act* autorise l'envoi d'e-mails publicitaires tant que le destinataire ne demande pas à se désinscrire[104]. Le *Telephone Consumer Protection Act* permet aussi aux démarcheurs d'appeler des particuliers, sauf si ceux-ci s'inscrivent sur le registre national d'opposition ou expriment leur refus[105]. Dans les deux cas, la protection ne fonctionne que si l'utilisateur agit lui-même.

Depuis 2018, la Californie a apporté des changements importants. Le *California Consumer Privacy Act*, renforcé par le *California Privacy Rights Act*, donne des droits d'accès, de suppression, de portabilité et d'opposition à la vente des données[106]. Il impose aussi un lien clair « Do Not Sell or Share My Personal Information » pour que l'utilisateur puisse facilement exercer son droit d'opposition[107]. D'autres États ont adopté des mesures similaires, ce qui montre une tendance à renforcer les droits individuels tout en gardant le principe du retrait[108].

Section 3 : Les mécanismes d'exercice du droit d'opt-out en droit californien

Le mécanisme « *Do Not Sell or Share My Personal Information* » est l'outil principal d'*opt-out* en Californie. Le lien doit mener directement à un outil pour exercer ce droit, sans étapes inutiles ni démarches compliquées[109]. Les entreprises ne peuvent pas cacher cette option dans leur politique de confidentialité ni utiliser des méthodes qui influencent la décision de l'utilisateur[110]. En pratique, ce mécanisme fonctionne site par site. L'utilisateur doit donc exercer son droit auprès de chaque entreprise, ce qui reste une charge importante pour lui[111].

Pour répondre à cette limite, le *Global Privacy Control* a été créé. Ce système envoie automatiquement un signal via le navigateur pour indiquer aux sites que l'utilisateur refuse la vente ou le partage de ses données[112]. Les lois californiennes acceptent ce signal comme un moyen valable d'exercer le droit d'opt-out[113]. Cela permet à l'utilisateur d'exprimer sa préférence une seule fois, pour tous les sites, au lieu de répéter la démarche à chaque visite.

---

[104] États-Unis, Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. § 7704(a)(3), 2003.

[105] États-Unis, Telephone Consumer Protection Act, 47 U.S.C. § 227, 1991.

[106] États-Unis (Californie), California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et s., 2018 ; États-Unis (Californie), California Privacy Rights Act (ci-après CPRA), Cal. Civ. Code §§ 1798.100 et s., 2020; D. J. SOLOVE, « The limitations of privacy rights », *Notre Dame L. Rev.*, vol. 98, n° 3, 2023, p. 983.

[107] D. J. SOLOVE, *id.*, p. 1028 ; CPRA précitée, § 1798.135(a).

[108] D. J. SOLOVE, *id.*, p. 983 ; États-Unis (Virginie), Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-575 et s., 2021 ; États-Unis (Colorado), Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301 et s., 2021.

[109] CALIFORNIA PRIVACY PROTECTION AGENCY, « CPRA Rulemaking Documents - Final Regulations Text », disponible sur www.cppa.ca.gov, 2023.

[110] *Ibid.* ; CALIFORNIA ATTORNEY GENERAL, *Final Statement of Reasons : California Consumer Privacy Act Regulations,* Sacramento, Department of Justice, 2020.

[111] A. BAIG et O. I. MALIK, « CPRA Do Not Sell or Share My Personal Information », disponible sur www.securiti.ai, 10 juin 2024.

[112] *World Wide Web Consortium* (W3C), « Global Privacy Control (GPC) », disponible sur www.w3.org, 19 février 2026.

[113] S. ZIMMECK, O. WANG, K. ALICKI, J. WANG et S. ENG, « Usability and Enforceability of Global Privacy Control », *Proceedings on Privacy Enhancing Technologies*, 2023/2, p. 265-267.

Section 4 : Analyse critique et enseignements pour le droit européen

Le modèle américain compte surtout sur l'inertie des utilisateurs. Il part du principe que chacun lit les politiques de confidentialité et utilise ses droits. En réalité, ces documents sont rarement lus et l'opt-out est peu utilisé[114]. Sur ce point, le modèle américain rejoint certaines critiques faites au consentement européen. Dans les deux cas, la protection réelle dépend d'un utilisateur attentif et actif, ce qui devient de plus en plus rare à l'ère numérique.

Mais ce constat ne doit pas faire oublier deux points positifs du modèle américain pour l'Europe. D'abord, l'obligation d'un lien clair « *Do Not Sell or Share My Personal Information* » rend le droit plus pratique pour l'utilisateur, contrairement aux interfaces européennes souvent complexes. Ensuite, le Global Privacy Control prouve qu'on peut simplifier l'exercice des droits sans demander sans cesse le consentement. Ces deux idées devraient être prises en compte dans une réforme du système européen.

Chapitre 2 : L'exemple canadien : un consentement raisonnable

Le droit canadien intéresse l'Europe non pas parce qu'il est très différent, mais parce qu'il aborde les mêmes questions avec d'autres méthodes. Comme le RGPD, il place le consentement au centre du système, mais il ajoute le critère des attentes raisonnables, qui limite ce que le consentement autorise et adopte une approche plus concrète pour le demander.

Section 1 : Le cadre général

Au Canada, la protection des données à caractère personnel est principalement assurée par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), adoptée en 2000 et destinée aux organisations du secteur privé[115]. Cette loi concerne surtout les entreprises sous compétence fédérale et celles qui mènent des activités commerciales entre provinces ou à l'international[116]. Certaines provinces ont mis en place leurs propres lois, considérées comme équivalentes à la loi fédérale, qui les remplacent alors[117]. Dans les autres provinces, c'est la LPRPDE qui s'applique par défaut[118].

---

[114] D. J. SOLOVE, « The limitations of privacy rights », *op. cit.*, p. 998 et 1027 ; D. J. SOLOVE, « Murky consent : an approach to the fictions of consent in privacy law », *op. cit.*, p. 600.

[115] Canada, Loi sur la protection des renseignements personnels et les documents électroniques (ci-après « LPRPDE »), L.C. 2000, ch. 5; T. SCASSA, « Data Protection and the Internet : Canada », in D. MOURA VICENTE (dir.), *Data Protection in the Internet. Ius Comparatum*, vol. 38, Cham, Springer, 2020, p. 55.

[116] L. PILGRAM, A. FINEBERG, E. JONKER et K. EL EMAM, « An assessment of synthetic data generation, use and disclosure under Canadian privacy regulations », *AI and Ethics*, vol. 5, 2025, p. 6227 ; T. SCASSA, « Data Protection and the Internet : Canada », *op. cit.*, p. 55-56.

[117] T. SCASSA, « Data Protection and the Internet : Canada », *id*., p. 56 ; Canada (Alberta), *Personal Information Protection Act* (PIPA), S.A. 2003, c. P-6.5 ; Canada (Colombie-Britannique), *Personal Information Protection Act* (PIPA), S.B.C. 2003, c. 63 ; Canada (Québec), *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25), L.Q. 2021, c. 25.

[118] L. PILGRAM, A. FINEBERG, E. JONKER et K. EL EMAM., *op. cit.*, p. 6227.

En 2015, le *Digital Privacy Act* a modifié la loi et renforcé les exigences concernant le consentement[119]. Ce qui distingue surtout le modèle canadien, c'est le critère des attentes raisonnables. Même si une personne donne son accord, une organisation ne peut utiliser ses données que dans des situations qu'une personne raisonnable jugerait acceptables[120]. Pour appliquer ce critère, la Cour fédérale a mis en place un test qui évalue la nécessité du traitement, son efficacité et la proportionnalité de l'atteinte à la vie privée[121]. Ce critère fixe donc une limite importante car même obtenu correctement, le consentement ne peut pas justifier un traitement inattendu ou disproportionné.

Section 2 : La place du consentement

Dans la LPRPDE, le consentement est le principe fondamental pour collecter, utiliser ou communiquer des renseignements personnels[122]. La loi prévoit quelques exceptions, comme en cas d'urgence, lors d'une enquête sur une infraction ou si la collecte est clairement dans l'intérêt de la personne[123]. En dehors de ces cas, le consentement reste la principale base juridique[124].

Le droit canadien accepte différentes formes de consentement. Il peut être exprès ou implicite, selon le contexte et la sensibilité des données[125]. Le consentement exprès est exigé pour les informations sensibles, les traitements qui dépassent les attentes raisonnables ou qui présentent un risque important de préjudice[126]. À l'inverse, un consentement implicite suffit pour des données moins sensibles et des traitements correspondant aux attentes raisonnables[127]. Cette flexibilité évite de transformer chaque interaction à faible risque en formalité juridique.

Pour répondre aux limites du consentement classique, le Commissariat à la protection de la vie privée a publié en 2019 des lignes directrices sur le consentement significatif (*meaningful*

---

[119] Canada, Loi sur la protection des renseignements personnels numériques, L.C. 2015, c. 32 ; B. FREEDMAN, « Digital Privacy Act - new requirement for valid consent to use personal information », disponible sur www.lexology.com, 25 juin 2015.

[120] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Guidelines for obtaining meaningful consent », disponible sur www.priv.gc.ca, 2019 ; LPRPDE précitée, art. 5(3).

[121] L. M. AUSTIN, « Reviewing PIPEDA : Control, Privacy and the Limits of Fair Information Practices », *Can. Bus. L.J.*, vol. 44, 2006, p. 45 ; C.F., Eastmond c. Canadian Pacific Railway, 11 juin 2004, 2004 CF 852, § 13.

[122] L. PILGRAM, A. FINEBERG, E. JONKER et K. EL EMAM, *op. cit*., p. 6229 ; LPRPDE précitée, annexe 1, art. 4.3

[123] LPRPDE précitée, art. 7(1) et 7(2) ; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Consent and privacy », disponible sur www.priv.gc.ca, 10 septembre 2019.

[124] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *ibid*. ; L. PILGRAM, A. FINEBERG, E. JONKER et K. EL EMAM, *op. cit.*, p. 6230.

[125] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Interpretation Bulletin : Form of Consent », disponible sur www.priv.gc.ca, 11 décembre 2015 ; C.A.F., Englander c. TELUS Communications Inc., 17 novembre 2004, 2004 CAF 387, § 60.

[126] LPRPDE précitée, annexe 1, art. 4.3.5 et 4.3.6 ; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Guidelines for obtaining meaningful consent », *op. cit.*

[127] LPRPDE précitée, annexe 1, art. 4.3.6 ; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Interpretation Bulletin : Form of Consent », *op. cit*.

consent)[128]. Leur objectif est de rendre le consentement plus clair et plus utile dans la pratique. Les organisations doivent mettre en avant les points essentiels du traitement, comme les données collectées, les objectifs, les éventuels partages avec des tiers et les risques pour les personnes concernées[129]. Elles sont encouragées à adopter des politiques à plusieurs niveaux, avec d'abord une information résumée puis des détails supplémentaires si besoin[130]. Des outils interactifs, comme des notifications au bon moment, sont aussi recommandés pour demander le consentement au moment précis où une donnée est utilisée[131].

Section 3 : Analyse critique et enseignements pour le droit européen

Le modèle canadien rencontre les mêmes difficultés que les autres systèmes fondés sur le consentement. Dans un monde numérique où les données sont collectées en permanence, il est difficile pour les personnes de comprendre et de contrôler tous les traitements qui les concernent. Les politiques de confidentialité sont souvent longues et complexes et les utilisateurs acceptent souvent des traitements sans vraiment en connaître les conséquences[132].

Cependant, deux points sont à retenir. Le critère des attentes raisonnables est un outil très utile pour la réflexion européenne. Il montre qu'un consentement ne peut pas justifier un traitement inattendu ou disproportionné et rappelle que la validité du consentement dépend aussi du caractère raisonnable du traitement. Le droit européen pourrait s'en inspirer pour mieux encadrer les traitements qui, même consentis, dépassent ce que la personne pouvait raisonnablement prévoir.

L'approche du *meaningful consent* propose aussi des solutions concrètes pour améliorer la qualité du consentement sans en changer la nature. L'information à plusieurs niveaux, les notifications adaptées au contexte et des choix clairs répondent directement aux difficultés du consentement éclairé. Cela montre qu'il est possible d'améliorer la façon de demander le consentement sans remettre en cause le système lui-même.

Chapitre 3 : L'exemple indien : un consentement centralisé

Le droit indien de la protection des données est intéressant pour l'Europe car il propose une solution concrète à la fatigue liée au consentement. Plutôt que de multiplier les demandes

---

[128] T. SCASSA, « Data Protection and the Internet : Canada », *op. cit*., p. 60 ; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Guidelines for obtaining meaningful consent », *op. cit*.

[129] LPRPDE précitée, annexe 1, art. 4.3.2 ; A. CAMERON, D. FABIANO et R. SPILLETTE, « Privacy Commissioner issues key guidelines for consent and inappropriate data practices », *C.P.L.R.*, vol. 15, n° 9, 2018, p. 70-71.

[130] A. CAMERON, D. FABIANO et R. SPILLETTE, *id.*, p. 71 ; T. SCASSA, « Data Protection and the Internet : Canada », *op. cit*., p. 60-61.

[131] A. CAMERON, D. FABIANO et R. SPILLETTE, *ibid.* ; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Guidelines for obtaining meaningful consent », *op. cit.*

[132] T. SCASSA, « Chapter 5 : AI and Data Protection Law », in *Artificial Intelligence and the Law in Canada*, Toronto, LexisNexis, 2021, p. 8 et 10 ; L. M. AUSTIN, « Enough About Me : Why Privacy is About Power, Not Consent (or Harm) », in A. SARAT (dir.), *A World Without Privacy : What Can/Should Law Do*, Cambridge, Cambridge University Press, 2015, p. 133.

auprès de chaque entreprise, il centralise la gestion du consentement autour d'un acteur dédié qui défend les intérêts des utilisateurs.

Section 1 : Le cadre général

Le *Digital Personal Data Protection Act* de 2023 est la première loi indienne complète sur la protection des données personnelles[133]. Elle s'applique à toutes les entités qui traitent des données numériques, qu'elles soient publiques ou privées, regroupées sous le terme *Data Fiduciary*, c'est-à-dire l'acteur qui décide des finalités et des moyens du traitement[134]. La loi s'applique aussi aux étrangers si le traitement concerne des personnes résidant en Inde[135]. Cependant, elle ne couvre que les données à caractère personnel numériques, ce qui exclut les traitements uniquement sur support papier[136].

Le contrôle de l'application est confié au *Data Protection Board of India*, qui veille au respect du *DPDP Act*, règle les litiges et peut imposer des sanctions financières. Cependant, il ne peut pas s'auto-saisir, ce qui limite son action aux cas qui lui sont signalés[137].

Section 2 : La place du consentement

Le *DPDP Act* fait du consentement la base légale principale. Toute collecte ou utilisation de données à caractère personnel doit normalement être précédée de l'accord de la personne concernée[138]. Ce consentement doit être libre, spécifique, éclairé, inconditionnel et sans ambiguïté et se manifester par une action affirmative claire[139]. Il doit concerner une finalité précise et se limiter aux données nécessaires à cette finalité[140]. Le silence, l'inaction, les cases précochées et les acceptations globales ne sont pas considérés comme des formes valables de consentement[141]. C'est au *Data Fiduciary* de prouver, en cas de litige, qu'un avis conforme a été donné et que le consentement a bien été obtenu[142].

Pour être éclairé, le consentement doit s'appuyer sur une information claire concernant la finalité du traitement, la nature des données collectées et l'identité de l'organisation

---

[133] Inde, Digital Personal Data Protection Act, 2023 (ci-après « DPDP Act »), Act No. 22 of 2023, Gazette of India Extraordinary, Part II, Section 1, 11 août 2023 ; K. DHARMENDRA, « Balancing privacy and innovation : analyzing the DPDP Act, 2023 in India's Cyber Law Framework », *Int. Res. J. Modern. Eng. Technol. Sci.*, vol. 07, 2025, p. 543.

[134] G. GREENLEAF, « India's 2023 Data Privacy Act : Business/government Friendly, Consumer Hostile », disponible sur www.ssrn.com, 16 août 2023, p. 1 et 2 ; Data Secure, « Consent Management Under India's DPDP ACT : Best Practices for Compliance », disponible sur www.dpo-india.com, 30 avril 2025.

[135] K. DHARMENDRA, *op. cit.*, p. 545.

[136] G. GREENLEAF, *India's 2023 Data Privacy Act : Business/government Friendly, Consumer Hostile*, *op. cit.*, p. 2.

[137] G. GREENLEAF, *id.*, p. 9 ; K. DHARMENDRA, *op. cit.*, p. 545.

[138] DPDP Act précitée, art. 4(1) ; D. BARAT, « Yes Means Yes : Managing Consent Under India's New Data Protection Law », disponible sur www.chambers.com, 20 septembre 2023.

[139] DPDP Act précitée, art. 6(1) ; Data Secure, *op. cit.*

[140] DPDP Act précitée, art. 6(1) ; B. DEBORSHI, « Notice And Consent Requirements In India's New Digital Data Regime », disponible sur www.mondaq.com, 20 juin 2023.

[141] Data Secure, *op. cit*.

[142] DPDP Act précitée, art. 6(10) ; B. DEBORSHI, « Notice And Consent Requirements In India's New Digital Data Regime », *op. cit.*

responsable[143]. Le *DPDP Act* impose que cet avis soit disponible en anglais ou dans l'une des vingt-deux langues officielles de l'Inde, ce qui montre la volonté d'adapter le consentement à la diversité linguistique du pays[144].

Le DPDP Act prévoit aussi des situations où le consentement n'est pas nécessaire, regroupées sous la notion de *deemed consent*. Cela concerne l'exercice de fonctions étatiques, les urgences médicales, la santé publique, les relations de travail ou les cas où la personne a volontairement fourni ses données dans un contexte où leur utilisation est raisonnablement attendue[145].

Section 3 : Le Consent Manager

L'innovation la plus notable du droit indien est la création du *Consent Manager*. Cette entité, enregistrée auprès du *Data Protection Board*, permet à chaque personne de donner, gérer, consulter et retirer son consentement auprès de plusieurs responsables du traitement grâce à une interface unique[146].

Ce système se distingue des plateformes européennes de gestion du consentement par son indépendance. Le *Consent Manager* ne décide pas des finalités ou des moyens du traitement. Il agit seulement pour la personne concernée à qui il rend directement compte[147]. Il doit respecter des obligations strictes d'enregistrement et de contrôle et peut être sanctionné en cas de manquement[148].

Dans la pratique, le système permet de définir des préférences par défaut. Lorsqu'une nouvelle entreprise demande l'accès à des données, ces préférences s'appliquent automatiquement, sauf si l'utilisateur décide autrement[149]. Le Consent Manager ne gère que les preuves de consentement et n'a jamais accès aux données à caractère personnel elles-mêmes[150]. L'objectif est de réduire la répétition des demandes et de permettre à l'utilisateur de suivre et de modifier ses choix au fil du temps, sans être submergé de sollicitations.

---

[143] B. DEBORSHI, *ibid* ; DPDP Act précitée, art. 5(1).

[144] DPDP Act précitée, art. 5(3) ; A. SHARMA, « Consent, Control, and Compliance : Assessing India's Digital Personal Data Protection Laws », *Indian Journal of Law and Legal Research*, 2023, vol. 5, n° 2, p. 1713.

[145] DPDP Act précitée, art. 7 ; B. DEBORSHI, « Daring To Deem ? 'Deemed' Consents Under India's Proposed Data Protection Law », disponible sur www.mondaq.com, 4 juillet 2023.

[146] DPDP Act précitée, art. 2(g) ; B. DEBORSHI, « Notice And Consent Requirements In India's New Digital Data Regime », *op. cit.*

[147] DPDP Act précitée, art. 6(7) et 8 ; S. ABRAHAM, « Law & the Digital Society : Fine-tuning Digital Personal Data Protection Rules 2025 for Effective Implementation », disponible sur www.thehinducentre.com, 15 mars 2025.

[148] Data Secure, *op. cit.* ; X, « Role of Consent Managers », disponible sur www.dpdpaedu.org, *s.d.,* consulté le 20 février 2026.

[149] R. RAKTIMA, « Top 10 operational impacts of India's DPDPA - Consent management », disponible sur www.iapp.org, 11 juillet 2024.

[150] S. ABRAHAM, *op. cit.* ; X, « Role of Consent Managers », *op. cit.*

Section 4 : Analyse critique et enseignements pour le droit européen

Le *DPDP Act* présente plusieurs faiblesses importantes. Il ne distingue pas les catégories de données selon leur sensibilité, ce qui laisse les données de santé, biométriques ou financières sans protection spécifique[151]. L'utilisation fréquente du *deemed consent* rend la frontière entre consentement et autres bases juridiques floue, ce qui nuit à la cohérence du système[152]. Enfin, le *Data Protection Board* ne peut pas s'auto-saisir, ce qui limite l'efficacité du contrôle.

Malgré ces limites, il ne faut pas sous-estimer l'apport du modèle indien. Le *Consent Manager* répond directement à la multiplication des demandes de consentement et à la fatigue qui en résulte. En centralisant la gestion des autorisations autour d'un tiers indépendant, il allège la charge pour l'utilisateur et facilite le retrait du consentement. Ce modèle offre une solution concrète pour le droit européen, qui pourrait mieux encadrer les plateformes de gestion du consentement afin de mieux protéger les utilisateurs.

Chapitre 4 : L'exemple singapourien : un consentement relativisé

Le modèle singapourien est intéressant parce qu'il ne met pas le consentement au cœur du système. Ici, la protection des données dépend surtout des obligations imposées aux organisations, ce qui transfère la responsabilité de la protection des personnes vers celles qui traitent leurs données.

Section 1 : Le cadre général

Le *Personal Data Protection Act* de 2012 (PDPA) est la base du système singapourien[153]. La loi cherche clairement à équilibrer les besoins des entreprises et les droits des utilisateurs[154]. Ici, la protection des données n'est pas vue comme un droit fondamental mais comme un cadre permettant l'utilisation légitime des données dans un contexte économique[155]. L'accent est donc mis sur la régulation des pratiques des organisations plutôt que sur la reconnaissance de droits individuels.

La *Personal Data Protection Commission* (PDPC) gère et applique le PDPA[156]. Elle vise à concilier la protection des données avec le besoin des organisations de les utiliser à des fins légitimes[157]. La PDPC agit surtout sur la base des plaintes mais publie aussi de nombreuses

---

[151] A. SHARMA, *op. cit.*, p. 1714 ; G. GREENLEAF, *India's 2023 Data Privacy Act : Business/government Friendly, Consumer Hostile*, *op. cit.*, p. 2.

[152] G. GREENLEAF, *id.*, p. 6 ; B. DEBORSHI, « Daring To Deem ? 'Deemed' Consents Under India's Proposed Data Protection Law », *op. cit.*

[153] Singapour, Personal Data Protection Act 2012 (ci-après « PDPA »), Act No. 26 of 2012, Government Gazette, 3 décembre 2012 ; M. YIP, *op. cit.*, p. 266 ; B. WONG YONGQUAN, « Data privacy law in Singapore », *Int. Data Priv. Law*, vol. 7, 2017, p. 287.

[154] M. YIP, *op. cit.*, p. 266 ; PDPA précitée, préambule.

[155] S. CHESTERMAN, *Data Protection Law in Singapore : Privacy and Sovereignty in an Interconnected World*, Singapour, Academy Publishing, 2021, p. xii.

[156] B. WONG YONGQUAN, *op. cit.*, p. 291.

[157] C. GIROT et D. PAULGER, *Singapore : Status of Consent for Processing Personal Data*, ABLI-FPF Convergence Series, Asian Business Law Institute et Future of Privacy Forum, août 2022, p. 3.

lignes directrices régulièrement mises à jour pour aider les organisations à comprendre et appliquer la loi[158].

Section 2 : Un système centré sur les obligations des organisations

Le PDPA fonctionne surtout selon une logique d'obligations[159]. Ici, la protection des données n'est pas un droit que l'individu doit faire valoir mais un ensemble de devoirs pour l'organisation. Les organisations doivent notamment prendre en charge les données qu'elles possèdent, nommer un *Data Protection Officer*, mettre en place des mesures internes de conformité, informer les personnes concernées sur les finalités et rendre leurs politiques accessibles[160].

Le système singapourien se distingue également par le critère de raisonnabilité des finalités. Une organisation ne peut traiter des données que pour des fins qu'une personne raisonnable jugerait appropriées dans la situation[161]. Même sans violation formelle du consentement, une organisation peut enfreindre le PDPA si la finalité est excessive ou inattendue[162]. Cela permet de limiter les clauses de consentement trop larges et de contrôler les traitements qui vont au-delà de ce qu'une personne raisonnable pouvait prévoir.

Section 3 : La place du consentement

Le consentement est le point de départ du système[163]. Une organisation ne peut collecter, utiliser ou divulguer des données que si la personne a donné son accord, est supposée l'avoir donné ou si la loi le permet[164]. L'organisation doit aussi pouvoir prouver qu'elle a obtenu ce consentement[165].

Le texte prévoit plusieurs formes de consentement supposé. Le consentement par conduite s'applique quand une personne donne volontairement ses données pour un but précis et qu'il est raisonnable de penser qu'elle le fait pour cette raison[166]. Le consentement par nécessité contractuelle permet de transmettre des données à une autre organisation si cela est raisonnablement nécessaire pour exécuter un contrat[167]. Enfin, le consentement par

---

[158] C. GIROT et D. PAULGER, *op. cit.*, p. 3.; B. WONG YONGQUAN, *op. cit.*, p. 291 et 301.

[159] B. WONG YONGQUAN, *op. cit.*, p. 287 et 291.

[160] Personal Data Protection Commission (ci-après « PDPC »), « Data Protection Obligations », disponible sur www.pdpc.gov.sg, 8 novembre 2023 ; PDPC, « Accountability », disponible sur www.pdpc.gov.sg, 14 septembre 2021 ; M. YIP, *op. cit.*, p. 269.

[161] PDPA précitée, art. 18 ; B. WONG YONGQUAN, *op. cit.*, p. 293 ; C. GIROT et D. PAULGER, *op. cit.*, p. 2.

[162] M. YIP, *op. cit.*, p. 273-276.

[163] *Id.*, p. 269 ; B. WONG YONGQUAN, *op. cit.*, p. 292.

[164] B. WONG YONGQUAN, *ibid.* ; PDPA précitée, section 13 ; PDPC, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, 16 mai 2022, p. 38.

[165] R. WALTERS et M. COGHLAN, « Data Protection and Artificial Intelligence Law : Europe Australia Singapore », *Am. J. Sci. Eng. Tech.*, vol. 4, 2019, p. 61.

[166] PDPC, *Advisory Guidelines on Key Concepts in the PDPA*, *op. cit.*, p. 42-43 ; M. YIP, *op. cit.*, p. 270 ; B. WONG YONGQUAN, *op. cit.*, p. 292.

[167] PDPC, *Advisory Guidelines on Key Concepts in the PDPA*, *op. cit.*, p. 44.

notification permet à une organisation d'informer la personne d'une finalité précise et autorise le traitement si elle ne s'y oppose pas dans le délai prévu[168].

Le PDPA prévoit aussi des exceptions au consentement pour des traitements jugés socialement ou légalement acceptables : urgences mettant en danger la vie ou la sécurité, intérêt national, données accessibles au public ou situations où il faut agir dans l'intérêt de la personne sans pouvoir obtenir son accord à temps[169]. Ces exceptions sont larges et laissent beaucoup de marge d'interprétation aux organisations[170]. Les modifications de 2020 ont encore élargi ces possibilités, si bien que beaucoup de traitements peuvent maintenant se faire sans consentement explicite, tant qu'ils répondent à des finalités raisonnables[171].

Section 4 : Analyse critique et enseignements pour le droit européen

Le modèle singapourien a une limite évidente. Plus les cas de consentement supposé et les exceptions augmentent, plus le consentement perd de son importance. Il reste dans la loi mais son rôle réel diminue. La protection dépend alors surtout de l'appréciation des organisations et du contrôle de la PDPC, plutôt que de la volonté de la personne. Les exceptions très larges renforcent cette impression en laissant aux organisations une grande liberté d'interprétation.

Cependant, deux points sont à retenir. Le critère de raisonnabilité des finalités complète le consentement. Il sert à limiter les clauses de consentement trop larges et à encadrer les traitements qui, même s'ils sont officiellement consentis, vont au-delà de ce qu'une personne raisonnable pouvait prévoir. Cette approche, proche du critère canadien des attentes raisonnables, pourrait être utile au modèle européen.

La logique d'obligations apporte aussi un point de vue intéressant. En mettant la responsabilité de la protection sur les organisations et non sur les personnes, le modèle singapourien montre que la protection des données ne peut pas dépendre seulement de la capacité des utilisateurs à gérer leurs informations. Cette idée, déjà présente dans le droit européen avec le principe d'accountability, est encore plus centrale à Singapour.

Chapitre 5 : L'exemple australien : un consentement objectivé

Le droit australien de la protection des données fonctionne selon une logique différente de celle du RGPD. Le consentement existe mais il ne concerne que certaines catégories de données et il est souvent remplacé par un test d'attente raisonnable. Ce système, qui considère le consentement comme une base parmi d'autres et non comme un principe central, offre un point de comparaison intéressant pour l'Europe.

---

[168] PDPC, *Advisory Guidelines on Key Concepts in the PDPA*, *op. cit.*, p. 45 ; PDPA précitée, s. 15A.

[169] PDPA précitée, section 17 ; M. YIP, *op. cit.*, p. 272 ; B. WONG YONGQUAN, *op. cit.*, p. 292-293.

[170] G. GREENLEAF, « Singapore's Personal Data Protection Act 2012 : Scope and principles », *P.L. & B. Int. Report*, n° 120, 2012, p. 5-6 ; M. YIP, *op. cit.*, p. 272.

[171] C. GIROT et D. PAULGER, *op. cit.*, p. 3.

Section 1 : Le cadre général

Le droit australien de la protection des données repose sur le *Privacy Act* de 1988, remanié en 2014 avec l'introduction de treize *Australian Privacy Principles*[172]. Ces principes s'appliquent aux agences fédérales et aux organisations du secteur privé dont le chiffre d'affaires dépasse trois millions de dollars australiens[173]. Les entités en dessous de ce seuil sont en principe exemptées, ce qui laisse sans protection une part importante de la population dans ses interactions avec de nombreux prestataires[174].

L'*Office of the Australian Information Commissioner* supervise l'application de la loi et a vu ses pouvoirs renforcés depuis 2022[175]. Malgré cela, le système est resté peu actif. En vingt-trois ans, il n'y a eu que neuf décisions formelles, ce qui donne l'impression que le respect des règles n'entraîne pas de véritable risque. Ce manque d'application a directement affecté le régime du consentement, dont la validité est rarement contrôlée en pratique[176].

Section 2 : La place du consentement

En Australie, le consentement n'a pas le même rôle central que dans le RGPD. Pour les données ordinaires, la collecte est autorisée si elle est raisonnablement nécessaire aux activités de l'entité, sans qu'il soit nécessaire d'obtenir un consentement[177]. Le consentement n'est exigé que pour les données sensibles[178]. Il peut être exprès ou implicite, mais il doit respecter quatre conditions : la personne doit être informée, son accord doit être volontaire, actuel et spécifique et elle doit comprendre ce à quoi elle consent[179].

Pour les usages secondaires, l'APP 6.2(a) permet de ne pas demander de consentement si la personne pouvait raisonnablement s'y attendre et si la finalité est liée à celle de la collecte initiale[180]. Ce test d'attente raisonnable ne doit pas être confondu avec le test du caractère juste et raisonnable que la réforme propose d'introduire. Le premier justifie l'absence de consentement, tandis que le second encadrerait le traitement même si le consentement a été

---

[172] Australie, Privacy Act 1988 (Cth), Act No. 119 of 1988, Commonwealth of Australia Gazette (ci-après « Privacy Act ») ; Australie, Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), Act No. 197 of 2012, Commonwealth of Australia Gazette.

[173] Privacy Act précitée, s. 6C et 6D.

[174] *Id*., s. 6D(4).

[175] Australie, Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth), Act No. 113 of 2022, Commonwealth of Australia Gazette.

[176] N. WATERS et G. GREENLEAF, « A critique of Australia's proposed *Privacy Amendment (Enhancing Privacy Protection) Bill* 2012 », soumission au Parlement australien, 14 août 2012, p. 5 ; G. GREENLEAF, « Privacy in Australia », in J. RULE et G. GREENLEAF (éd.), *Global Privacy Protection: The First Generation*, Cheltenham, Edward Elgar, 2008, p. 19.

[177] Privacy Act précitée, annexe 1, APP 3.1 ; OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (ci-après « OAIC »), « Australian Privacy Principles Guidelines », disponible sur www.oaic.gov.au, 22 juillet 2019, § 3.3.

[178] Privacy Act précitée, annexe 1, APP 3.3(a) ; OAIC, « Australian Privacy Principles Guidelines », op.cit., § 3.22.

[179] OAIC, « Australian Privacy Principles Guidelines, chapitre B », disponible sur www.oaic.gov.au, 21 décembre 2022, § B.37-B.38.

[180] Privacy Act précitée, annexe 1, APP 6.2(a) ; OAIC, « Australian Privacy Principles Guidelines », op.cit., § 6.18 - 6.22.

donné. Ces deux mécanismes ont des objectifs différents[181]. Il existe aussi d'autres bases non liées au consentement, comme l'autorisation légale, l'urgence ou les activités de police, ce qui limite encore plus le rôle du consentement dans la pratique[182].

Le régime du démarchage direct illustre bien cette différence. L'APP 7 autorise l'utilisation des données à des fins de marketing sans accord préalable, à condition que la personne puisse raisonnablement s'y attendre et qu'elle puisse refuser par *opt-out*[183]. Cela fonctionne à l'opposé du RGPD et de la directive ePrivacy, qui exigent un accord préalable.

Section 3 : La réforme en cours

Le *Privacy Act* fait l'objet d'une révision importante depuis 2020. Le rapport publié en février 2023 propose d'aligner la définition du consentement sur les standards internationaux, en exigeant qu'il soit volontaire, éclairé, actuel, spécifique et non ambigu et d'introduire un consentement affirmatif pour la revente commerciale des données personnelles[184]. Mais la proposition la plus marquante vise à imposer que toute collecte, utilisation ou divulgation soit objectivement juste et raisonnable dans les circonstances, selon le point de vue d'une personne raisonnable, même si un consentement a été obtenu[185]. Un traitement ne serait donc plus valable uniquement parce qu'une personne a consenti. L'entité devrait aussi prouver que ce traitement est proportionné et équitable.

En novembre 2024, une première série de réformes a été adoptée, comprenant notamment un recours direct en cas d'atteinte grave à la vie privée. Cependant, le test du caractère juste et raisonnable et la réforme de la définition du consentement ont été repoussés à une deuxième phase législative[186].

Section 4 : Analyse critique et enseignements pour le droit européen

Le système actuel a des limites importantes. L'absence d'exigence de consentement pour les données ordinaires, l'acceptation du consentement implicite, le recours à l'opt-out pour le démarchage direct et l'exemption des petites entreprises laissent de nombreux traitements sans véritable contrôle. Plus généralement, le modèle *notice and consent* est jugé insuffisant.

---

[181] ATTORNEY-GENERAL'S DEPARTMENT, Privacy Act Review Report, Canberra, février 2023, Proposals 12.1-12.3 ; G. GREENLEAF, « Australia's never-ending privacy reform process », (2023) 186 *Privacy Laws & Business International Report* 11, p. 3.

[182] Privacy Act précitée, annexe 1, APP 6.2(b) - (e) ; OAIC, « Australian Privacy Principles Guidelines », *op. cit.*, § 6.29 et s.

[183] OAIC, *id.*, § 7.1 à 7.3 ; Privacy Act précitée, annexe 1, APP 7.

[184] ATTORNEY-GENERAL'S DEPARTMENT, Privacy Act Review Report, *op. cit.*, Proposals 11.1 et 20.4 ; G. GREENLEAF, « Australia's never-ending privacy reform process », *op. cit.*, p. 3.

[185] ATTORNEY-GENERAL'S DEPARTMENT, *id.*, Proposals 12.1 - 12.3 ; G. GREENLEAF, *id.*, p. 3.

[186] G. GREENLEAF, *id.*, p. 5.

Les gens lisent rarement les formulaires de consentement et sur les plateformes numériques, le déséquilibre de pouvoir entre entreprises et utilisateurs rend cet accord souvent fictif[187].

Ce constat ne doit pas faire oublier ce que ce système peut apporter à la réflexion européenne. La présence d'un test d'attente raisonnable pour les usages secondaires et d'un test objectif en préparation pour tous les traitements montre une évolution importante. La protection des données ne peut pas dépendre uniquement de l'accord de la personne concernée. Cette approche rejoint celle du droit canadien et singapourien, mais va plus loin en proposant un standard objectif et systématique. Ce qui distingue le test australien proposé, c'est qu'il s'appliquerait à tous les traitements, même ceux fondés sur le consentement, en exigeant aussi l'équité et la proportionnalité. Même si la personne a donné son accord, l'entité devrait encore prouver que le traitement est justifié.

Titre III : Réformer le système

Le consentement, tel que le RGPD l'imagine, se heurte aujourd'hui à de véritables obstacles. Comme nous l'avons montré dans la Partie II, il ne s'agit pas d'une simple question de mauvaise rédaction ou d'un défaut ponctuel d'application. Le véritable problème, c'est le fossé entre l'intention du législateur et la réalité numérique. La plupart des utilisateurs ne lisent pas les politiques de confidentialité, ne comprennent pas toujours ce qu'ils acceptent, n'ont souvent pas d'alternative réelle et peinent à retirer leur consentement. Dans ce contexte, renforcer les conditions formelles du consentement ne suffit pas.

La question n'est pas d'abandonner le consentement, qui reste utile lorsqu'un véritable choix est possible. L'enjeu, c'est de le réformer pour lui redonner du sens et de l'articuler avec d'autres outils de protection, là où il ne suffit plus. Le droit comparé présenté dans le Titre II est riche d'enseignements. Aucun système n'est à recopier tel quel, mais chacun offre des pistes pertinentes. Ce Titre III s'en inspire en croisant ces outils avec ceux du droit européen pour proposer deux axes de réforme.

D'abord, il s'agit de repenser la place du consentement dans le système, le réserver aux situations où il a du sens et renforcer les obligations pesant sur les responsables du traitement. Ensuite, il faut améliorer les conditions dans lesquelles le consentement s'exprime, en simplifiant ses mécanismes et en l'encadrant par des limites matérielles, indépendantes de la seule volonté individuelle.

Chapitre 1 : Renforcer les obligations des responsables du traitement

Recentrer le consentement sur les situations où il est adapté ne suffit pas à lui seul. Il faut aussi s'interroger sur ce qui se passe lorsque le consentement reste la base retenue. Dans ce cas, la protection effective des individus ne peut pas reposer uniquement sur leur propre vigilance. Elle doit aussi peser sur ceux qui traitent les données.

---

[187] G. GREENLEAF, N. WATERS, K. LANE, B. ARNOLD et R. CLARKE, « Bringing Australia's *Privacy Act* up to international standards », soumission de l'Australian Privacy Foundation, 18 décembre 2020, p. 7, 17 et 20.

Ce constat ne surprend pas en droit européen. Le principe d'*accountability*, posé à l'article 5, paragraphe 2 du RGPD, impose déjà au responsable du traitement de démontrer qu'il respecte les principes applicables[188]. Il existe aussi l'obligation de tenir un registre des activités, de réaliser des analyses d'impact pour les traitements à risque élevé ou encore de mettre en place des mesures de protection dès la conception et par défaut[189]. Ces outils existent, mais ils restent insuffisants. Ils n'imposent pas de vérification préalable et systématique pour l'ensemble des traitements, ni de standards concrets sur ce qui peut être collecté dans chaque contexte. Deux pistes permettraient d'y remédier.

Section 1 : Élargir l'analyse d'impact

L'article 35 du RGPD impose une analyse d'impact préalable dès qu'un traitement risque d'entraîner un risque élevé pour les droits et libertés des personnes concernées[190]. Cette exigence ne concerne qu'un nombre restreint de cas : le profilage automatisé aux conséquences significatives, le traitement massif de données sensibles et la surveillance systématique[191]. En dehors de ces situations, la plupart des traitements fondés sur le consentement n'entrent pas dans ce champ.

Le responsable du traitement doit bien inscrire le choix de la base légale dans le registre des traitements[192]. Mais cette documentation reste purement interne. Elle n'est examinée qu'après coup, lors d'un contrôle ou d'une plainte et rien n'impose un examen avant le début du traitement[193]. Un consentement formellement régulier peut donc masquer un traitement disproportionné ou inattendu, sans qu'aucune évaluation préalable ne l'ait révélé.

Élargir l'analyse d'impact aux traitements fondés sur le consentement qui présentent un risque, même modéré, permettrait de combler ce manque. Il ne s'agirait pas d'introduire une nouvelle exigence d'évaluation de la nécessité ou de la proportionnalité, mais d'imposer que cette démarche soit conduite de façon formelle, documentée et placée sous le contrôle des autorités, en amont, plutôt que laissée au seul jugement interne du responsable. Le droit australien en cours d'élaboration va dans ce sens, en prévoyant un test préalable et systématique du caractère juste et raisonnable de tout traitement[194]. C'est précisément cette dimension préventive qui fait défaut aujourd'hui en droit européen.

---

[188] RGPD précité, art. 5, § 2 ; O. TAMBOU, *op. cit.*, p. 129.

[189] RGPD précité, art. 25, 30 et 35.

[190] RGPD précité, art. 35, §1.

[191] *Id*., art. 35, §3 ; GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, « Lignes directrices sur l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si un traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 », adoptées le 4 octobre 2017, p. 9-11.

[192] RGPD précité, art. 5, §2 et 30.

[193] *Id*., art. 30, §4.

[194] ATTORNEY-GENERAL'S DEPARTMENT, *Privacy Act Review Report*, *op. cit.*, Proposals 12.1-12.3 ; G. GREENLEAF, « Australia's never-ending privacy reform process », *op. cit.*, p. 3.

Section 2 : Rendre la minimisation plus concrète

Le principe de minimisation s'applique à tous les traitements, peu importe la base légale choisie[195]. Par conséquent, un consentement valable n'autorise pas en théorie une collecte excessive. Pourtant, ce principe reste difficile à faire respecter concrètement. Sans référentiel précis sur ce qu'il est raisonnable de collecter dans chaque contexte de service, chaque responsable garde une grande liberté pour décider ce qui lui semble « nécessaire ». Un consentement formulé de façon large est alors souvent utilisé pour justifier une collecte étendue.

Le RGPD propose un mécanisme d'adaptation sectorielle avec les codes de conduite prévus à l'article 40. Ces codes permettent aux associations professionnelles de définir, pour leur secteur, la façon d'appliquer le règlement[196]. Cependant, ils reposent sur le volontariat[197] et dans les faits, ils restent très peu utilisés[198].

Des lignes directrices sectorielles, contraignantes et adaptées à chaque type de service, viendraient combler ce vide. Elles fixeraient clairement quelles données peuvent être collectées selon le contexte, limitant ainsi l'usage du consentement formel comme prétexte à des collectes disproportionnées. Ces standards précis réduiraient l'asymétrie d'information entre responsables et personnes concernées. Le principe de minimisation deviendrait alors réellement effectif et le consentement retrouverait un véritable périmètre.

Chapitre 2 : Améliorer les conditions dans lesquelles le consentement opère

Section 1 : Simplifier l'expression et la gestion du consentement

Même lorsque le consentement constitue la base légale la plus adaptée, les dispositifs actuels de demande et de gestion produisent souvent l'effet opposé à celui recherché. La multiplication des bannières de cookies, des fenêtres de paramétrage et des politiques de confidentialité a fait surgir un véritable paradoxe. Plus on sollicite le consentement, moins il est réel. Bon nombre d'utilisateurs cliquent par automatisme, non parce qu'ils font un choix éclairé, mais simplement pour faire disparaître une fenêtre envahissante[199]. Ce consentement répond alors aux exigences formelles du RGPD, tout en perdant sa substance réelle.

Le législateur européen a lui-même reconnu qu'il devenait urgent de simplifier ces mécanismes. En novembre 2025, la proposition Digital Omnibus prévoit d'introduire des signaux automatisés transmis par les navigateurs et imposerait aux sites de les respecter, afin

---

[195] RGPD précité, art. 5, §1, c) et 6, §1.

[196] RGPD précité, art. 40, §2 ; E.D.P.B., « Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de surveillance en vertu du règlement (UE) 2016/679 », adoptées le 4 juin 2019, p. 7.

[197] E.D.P.B., *id*.

[198] C.N.I.L., « Certifications et codes de conduite : la CNIL cartographie le déploiement des outils RGPD en Europe », disponible sur www.cnil.fr, 14 janvier 2026 : la CNIL recense une trentaine de codes de conduite et certifications approuvés au niveau national ou européen depuis l'entrée en application du RGPD en 2018.

[199] D. J. SOLOVE, « Murky consent : an approach to the fictions of consent in privacy law », *op. cit.*, p. 600 ; D. J. SOLOVE, « The limitations of privacy rights », *op. cit.*, p. 998.

de mettre un terme à la répétition des demandes[200]. Cette mesure marque une avancée notable. Mais la réforme ne règle pas tout. Elle concentre la gestion du consentement au niveau des navigateurs, sans prévoir d'indépendance réelle vis-à-vis des responsables du traitement. D'autres pistes complémentaires méritent donc d'être examinées.

I. Permettre une expression globale et automatisée des préférences

La première piste repose sur l'idée de permettre une expression globale et automatisée des préférences. Le *Global Privacy Control*, testé aux États-Unis, démontre qu'un utilisateur peut, sur le plan technique, exprimer une préférence générale sur le traitement de ses données. Cette préférence s'applique automatiquement à tous les sites visités, sans avoir à recommencer le choix à chaque fois[201]. Le système fonctionne grâce à un signal envoyé par le navigateur pour indiquer aux sites que l'utilisateur refuse le partage ou la vente de ses données.

Instaurer ce mécanisme en Europe, en le rendant valable pour exprimer le consentement et opposable aux responsables du traitement, allégerait considérablement la charge qui pèse sur les utilisateurs, tout en maintenant leur niveau de protection. Cette solution permettrait de répondre à la fatigue du consentement évoquée en Partie II. La proposition Digital Omnibus de novembre 2025 va justement dans ce sens, puisqu'elle prévoit des signaux automatisés transmis par les navigateurs et oblige les sites à les respecter[202].

Le modèle indien du *Consent Manager* retient également l'attention à ce titre. Ce système repose sur une interface unique, administrée par un tiers indépendant, qui donne à chacun la possibilité de gérer tous ses consentements auprès de différents responsables du traitement[203]. L'utilisateur y gagne une réduction sensible de la charge mentale et un accès simplifié à son droit de retrait.

Le point fort du système indien, comparé à ce que propose l'Europe, réside dans l'indépendance du gestionnaire. Sur le continent européen, les plateformes restent souvent entre les mains des responsables du traitement ou de prestataires qui leur sont liés. La proposition Digital Omnibus envisage bien une centralisation par les navigateurs, mais elle ne va pas jusqu'à imposer une indépendance réelle vis-à-vis des responsables du traitement[204]. Adopter un encadrement aussi strict qu'en Inde transformerait ces plateformes en outils de protection concrets, bien au-delà de la simple formalité.

Un tiers indépendant jouerait aussi un rôle clé dans la traçabilité des consentements donnés ou retirés. Cela répond directement à la difficulté, évoquée en Partie II, de retirer un consentement dont l'utilisateur ne se souvient plus avec précision.

---

[200] Commission européenne, proposition Digital Omnibus, *op. cit.*, art. 88 *bis* et *ter*.

[201] *World Wide Web Consortium* (W3C), *op. cit.* ; S. ZIMMECK, O. WANG, K. ALICKI, J. WANG et S. ENG, *op. cit.*, p. 265-267.

[202] Commission européenne, proposition Digital Omnibus, *op. cit.*, art. 88 bis et ter.

[203] DPDP Act précité, art. 2(g) et 6(7) ; R. RAKTIMA, *op. cit.*

[204] ALLIANCE DIGITALE, « Digital Omnibus : les 17 recommandations d'Alliance Digitale pour simplifier efficacement le RGPD et la directive ePrivacy », disponible sur www.alliancedigitale.org, 1er avril 2026.

II. Rendre le droit d'opposition plus visible

Le RGPD prévoit un droit d'opposition au traitement des données[205]. Pourtant, aucune règle générale n'oblige à rendre ce droit visible et standardisé sur les interfaces des services numériques. Pour la prospection commerciale, la loi demande bien une information explicite, qui doit être donnée au plus tard lors de la première communication[206]. Dans tous les autres cas, rien n'exige qu'un lien ou un bouton dédié soit clairement affiché sur chaque plateforme.

La loi californienne propose une solution concrète. Le CCPA oblige les entreprises à afficher un lien standardisé, « *Do Not Sell or Share My Personal Information* », directement sur leur interface. L'accès se fait sans étapes superflues ni démarches compliquées[207]. Ce dispositif rend le droit d'opposition immédiatement visible et facile à exercer, sans que l'utilisateur ait à chercher comment l'activer. Si l'on transposait ce modèle en Europe, un lien unique permettrait, en un seul clic, d'accéder à tous les droits de la personne concernée : opposition, retrait du consentement, effacement. Ce mécanisme rendrait ces droits réellement accessibles et non plus simplement théoriques.

Section 2 : Encadrer le consentement par des limites matérielles

Même obtenu de façon régulière, le consentement ne devrait jamais servir à légitimer n'importe quel traitement. Certains usages posent problème, non pas parce que le consentement serait mal recueilli, mais parce que le traitement va trop loin ou surprend la personne concernée. Le RGPD rappelle bien que le consentement ne dispense pas du respect des principes de minimisation et de limitation des finalités[208]. Pourtant, il n'introduit pas de test spécifique basé sur ce que la personne pouvait raisonnablement attendre, dès lors que le consentement est la base légale. Ce critère existe dans le RGPD, mais il ne joue que pour l'intérêt légitime ou les traitements ultérieurs[209]. Pour les traitements basés sur le consentement, une fois l'accord donné selon les règles, rien ne permet de s'opposer à un usage qui dépasse ce que la personne pouvait anticiper.

C'est cette faille que le droit comparé met en lumière : au Canada, le critère des attentes raisonnables, à Singapour, l'exigence de finalités raisonnables et en Australie, le test du caractère juste et raisonnable. Tous ces systèmes aboutissent au même constat. La légitimité d'un traitement ne tient pas seulement à l'accord formel de la personne, mais aussi au caractère raisonnable et proportionné du traitement lui-même. Ils imposent un contrôle de fond, indépendant du consentement, qui s'applique même lorsque l'accord a été recueilli dans les règles.

Introduire le critère des attentes raisonnables pour les traitements fondés sur le consentement, comme c'est déjà le cas dans le RGPD pour d'autres bases légales, comblerait

---

[205] RGPD précité, art. 21.

[206] *Id*., art. 21, §4.

[207] CCPA précité, Cal. Civ. Code §1798.135 ; CPRA précité, §1798.135(a).

[208] RGPD précité, art. 5, §1, b) et c).

[209] *Id*., consid. 47 et 50 et art. 6, §1, f) ; CNIL, « L'intérêt légitime : comment fonder un traitement sur cette base légale ? », disponible sur www.cnil.fr, 2 décembre 2019.

ce vide. Le responsable du traitement aurait alors l'obligation de prouver, non seulement que le consentement est valable, mais aussi que le traitement correspond à ce que la personne pouvait raisonnablement prévoir au moment de son accord. Ce critère reste contextuel, les attentes raisonnables se jugent en fonction de la relation entre la personne et le responsable, de la nature du service, du public visé et du type de données. Un traitement qui ne surprendrait pas un professionnel pourrait quand même être jugé illicite s'il va au-delà de ce qu'un utilisateur ordinaire pouvait prévoir. Si le traitement échoue à ce test, il serait illicite, même avec un consentement recueilli selon les règles.

Ce choix est ambitieux. Il demande de revoir la conception du consentement, non plus comme une simple autorisation qui validerait n'importe quel traitement en bonne et due forme, mais comme l'expression d'une volonté encadrée par des exigences fondées sur les attentes raisonnables des personnes concernées. Ce changement ne réduit pas la valeur du consentement. Il lui redonne au contraire son sens premier, permettre à chacun de décider, en connaissance de cause, du devenir de ses données.

Section 3 : Graduer le consentement selon le risque

Le test des attentes raisonnables sert à encadrer le contenu du consentement. Le droit canadien va plus loin et adapte aussi sa forme. La LPRPDE prévoit que la façon de recueillir le consentement dépend du niveau de sensibilité des renseignements et des attentes liées à chaque situation. Le consentement implicite suffit pour les traitements à faible risque qui correspondent à ce que l'on peut attendre raisonnablement, alors que le consentement explicite devient indispensable pour les données sensibles ou lorsque le traitement dépasse ces attentes[210]. De son côté, le RGPD impose toujours un acte positif et clair, en précisant que le silence ou l'inactivité ne valent jamais consentement[211].

Cette approche rigide a un effet immédiat, elle nourrit la lassitude face au consentement. Quand chaque interaction, même banale, requiert un acte positif explicite, le consentement finit par devenir un automatisme vidé de sa substance. Instaurer une gradation entre consentement exprès et consentement implicite, en réservant le premier aux opérations sensibles ou inattendues et en acceptant le second pour les usages à faible risque qui répondent aux attentes normales, recentrerait l'attention des utilisateurs là où elle compte vraiment. Une telle gradation ne diminuerait pas la protection offerte, elle la rendrait au contraire plus précise et donc plus efficace.

***

Les pistes avancées dans ce Titre III n'ont pas pour but de supprimer le consentement, mais plutôt de le replacer là où il garde tout son sens. Le premier axe vise à corriger le problème d'un consentement trop souvent utilisé, même quand il ne reflète pas un véritable choix et que d'autres fondements juridiques seraient plus appropriés. Le second axe part d'un autre

---

[210] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Guidelines for obtaining meaningful consent », *op. cit.* ; OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Consent and privacy », *op. cit.*, p. 8-9.

[211] RGPD précité, art. 4, §11 et consid. 32.

constat qui est que même lorsque le consentement est pertinent, les dispositifs actuels ne permettent ni de l'exprimer ni de le gérer réellement de manière efficace.

L'analyse du droit comparé montre que ces deux problèmes ne sont pas nouveaux, ils ont déjà été repérés ailleurs et des solutions concrètes existent. Aucune n'est parfaite, mais elles vont toutes dans le même sens. On ne peut plus fonder la protection des données uniquement sur l'idée que chacun est capable de gérer ses propres informations. Il faut aussi que la responsabilité pèse sur ceux qui manipulent les données, avec des exigences objectives qui s'imposent, qu'il y ait ou non un accord.

Réformer le consentement dans ce sens ne l'affaiblirait pas. Au contraire, cela lui redonnerait de la crédibilité.

CONCLUSION

Le consentement tient une place à la fois centrale et fragile dans le droit européen de la protection des données. Ce travail a voulu faire comprendre les raisons de cette situation et trouver des pistes pour y remédier.

Le modèle du consentement tel que conçu par le RGPD n'arrive plus à jouer pleinement son rôle protecteur. Ce n'est pas une question de mauvaise rédaction du texte, mais plutôt d'une hypothèse de départ qui ne colle plus au monde numérique, celle d'un individu qui comprend réellement ce à quoi il consent, qui a une vraie alternative et qui arrive à gérer ses préférences dans le temps. Les obstacles évoqués dans la Partie II ne sont pas de simples dysfonctionnements. Ils révèlent un décalage profond entre le mécanisme et la réalité dans laquelle il s'applique.

Il n'existe pas une solution unique au problème du consentement. Ce que montre le droit comparé, c'est qu'une réforme crédible repose au moins sur trois piliers. D'abord, recentrer le consentement sur les situations où il a un vrai sens et arrêter d'en faire la base par défaut quand il ne s'agit pas d'un choix libre. Ensuite, faire porter davantage la responsabilité de la protection sur ceux qui traitent les données, plutôt que sur les individus qui n'ont ni le temps ni les moyens de se protéger seuls. Enfin, encadrer le consentement par des limites concrètes qui s'imposent même en l'absence d'un accord pour éviter qu'un consentement formellement valable ne serve à légitimer des usages disproportionnés ou inattendus.

Ces pistes n'ont rien de révolutionnaire. Certaines s'appuient sur des mécanismes déjà prévus par le droit européen mais peu exploités. D'autres s'inspirent d'exemples étrangers qu'il faudrait adapter au contexte européen. Aucune, prise isolément, n'est suffisante. C'est leur combinaison qui pourrait rendre au consentement la crédibilité qu'il a perdue au fil du temps.

Reste une question ouverte, sans doute la plus délicate. Même si les pistes proposées sont solides sur le plan technique, leur application suppose des choix politiques que le droit, à lui seul, ne peut pas imposer. Jusqu'où limiter la liberté des entreprises de collecter des données ? Jusqu'où simplifier les mécanismes du consentement, au risque de les vider de leur sens ? Jusqu'où introduire des limites objectives, indépendantes de la volonté individuelle ? Ce sont autant de questions qui échappent au simple cadre juridique. Elles renvoient à la façon dont nos sociétés arbitrent entre la protection des personnes et la liberté économique.

La vraie question, au fond, ce n'est pas seulement de savoir si le consentement peut encore remplir sa fonction. C'est surtout de décider quelle protection on veut vraiment offrir à ceux dont les données sont traitées et si l'on est prêt à en accepter le prix.

BIBLIOGRAPHIE

LÉGISLATION

Droit européen et belge

Droit positif

Charte des droits fondamentaux de l'Union européenne (ci-après « Ch. dr. fond. UE »), *J.O.U.E.*, C 326, 26 octobre 2012, art. 8, §3.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L 201, 31 juillet 2002, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, *J.O.U.E.*, L 337, 18 décembre 2009.

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 (ci-après « RGPD »), *J.O.U.E.*, L 119, 4 mai 2016.

Proposition

Commission européenne, proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/679 en ce qui concerne les règles relatives au consentement et les règles relatives aux cookies, COM(2025) 765 final, 19 novembre 2025.

Commission européenne, proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, COM(2017) 10 final, 10 janvier 2017.

Droit étranger

Australie

Australie, *Privacy Act* 1988 (Cth), Act No. 119 of 1988, Commonwealth of Australia Gazette.

Australie, *Privacy Amendment (Enhancing Privacy Protection) Act* 2012 (Cth), Act No. 197 of 2012, Commonwealth of Australia Gazette.

Australie, *Privacy Legislation Amendment (Enforcement and Other Measures) Act* 2022 (Cth), Act No. 113 of 2022, Commonwealth of Australia Gazette.

Canada

Canada, *Loi sur la protection des renseignements personnels et les documents électroniques* (ci-après « LPRPDE »), L.C. 2000, ch. 5.

Canada (Alberta), *Personal Information Protection Act* (PIPA), S.A. 2003, c. P-6.5.

Canada (Colombie-Britannique), *Personal Information Protection Act* (PIPA), S.B.C. 2003, c. 63.

Canada, *Loi sur la protection des renseignements personnels numériques*, L.C. 2015, c. 32.

Canada (Québec), *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25), L.Q. 2021, c. 25.

États-Unis

États-Unis, *Telephone Consumer Protection Act*, 47 U.S.C. § 227, 1991.

États-Unis, *Controlling the Assault of Non-Solicited Pornography and Marketing Act*, 15 U.S.C. § 7704(a)(3), 2003.

États-Unis (Californie), *California Consumer Privacy Act*, Cal. Civ. Code §§ 1798.100 et s., 2018.

États-Unis (Californie), *California Privacy Rights Act* (ci-après CPRA), Cal. Civ. Code §§ 1798.100 et s., 2020.

États-Unis (Virginie), *Virginia Consumer Data Protection Act*, Va. Code Ann. §§ 59.1-575 et s., 2021.

États-Unis (Colorado), *Colorado Privacy Act*, Colo. Rev. Stat. §§ 6-1-1301 et s., 2021.

Inde

Inde, *Digital Personal Data Protection Act*, 2023 (ci-après « DPDP Act »), Act No. 22 of 2023, *Gazette of India Extraordinary*, Part II, Section 1, 11 août 2023.

Singapour

Singapour, *Personal Data Protection Act* 2012 (ci-après « PDPA »), Act No. 26 of 2012, *Government Gazette*, 3 décembre 2012.

JURISPRUDENCE

Jurisprudence européenne

C.J. (gde ch.), arrêt *Data Protection Commissioner c. Facebook Ireland Ltd et Schrems*, 16 juillet 2020, C-311/18, EU:C:2020:559.

C.J. (gde ch.), arrêt *Schrems c. Data Protection Commissioner*, 6 octobre 2015, C-362/14, EU:C:2015:650.

Jurisprudence étrangère

France

Commission nationale de l'informatique et des libertés (ci-après « C.N.I.L. »), formation restreinte, délibération n° SAN-2021-023, 31 décembre 2021, disponible sur www.legifrance.gouv.fr.

C.N.I.L., formation restreinte, délibération n° SAN-2021-024, 31 décembre 2021, disponible sur www.legifrance.gouv.fr.

Canada

C.A.F., *Englander c. TELUS Communications Inc.*, 17 novembre 2004, 2004 CAF 387.

C.F., *Eastmond c. Canadian Pacific Railway*, 11 juin 2004, 2004 CF 852.

DOCTRINE

Ouvrages

CHESTERMAN, S., *Data Protection Law in Singapore : Privacy and Sovereignty in an Interconnected World*, Singapour, Academy Publishing, 2021.

ELVY, S.-A., *A Commercial Law of Privacy and Security for the Internet of Things*, Cambridge, Cambridge University Press, 2021.

KIM, N. S., *Consentability: Consent and Its Limits*, Cambridge, Cambridge University Press, 2019.

LYNSKEY, O., *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, 2015.

SOLOVE, D. J., *Understanding Privacy*, Cambridge, Harvard University Press, 2008.

TAMBOU, O., *Manuel de droit européen de la protection des données à caractère personnel*, Bruxelles, Bruylant, 2020.

Articles de revue

ACQUISTI, A., BRANDIMARTE, L. et LOEWENSTEIN, G., « Privacy and human behavior in the age of information », *Science*, vol. 347, n° 6221, p. 509 à 514.

ACQUISTI, A., IDRIS, A. et BRANDIMARTE, L., « Gone in 15 Seconds: The Limits of Privacy Transparency and Control », *I.E.E.E. Sec. & Priv.*, vol. 11, n° 4, p. 72 à 74.

AUSTIN, L. M., « Reviewing PIPEDA : Control, Privacy and the Limits of Fair Information Practices », *Can. Bus. L.J.*, vol. 44, 2006, p. 1 à 53.

BAKARE, S. S., ADENIYI, A. O., AKPUOKWE, C. U. et ENEH, N. E., « Data privacy and compliance : a comparative review of the EU GDPR and USA regulations », *Computer Science & IT Research Journal*, vol. 5, n° 3, 2024, p. 528 à 543.

CAMERON, A., FABIANO, D. et SPILLETTE, R., « Privacy Commissioner issues key guidelines for consent and inappropriate data practices », *C.P.L.R.*, vol. 15, n° 9, 2018, p. 69 à 74.

CHOI, H., PARK, J. et JUNG, Y., « The role of privacy fatigue in online privacy behavior », *Computers in Human Behavior*, vol. 81, 2018, p. 42 à 51.

CORREN, E., « The Consent Burden in Consumer and Digital Markets », *Harv. J.L. & Tech.*, vol. 36, 2023, p. 551 à 613.

DHARMENDRA, K., « Balancing privacy and innovation : analyzing the DPDP Act, 2023 in India's Cyber Law Framework », *Int. Res. J. Modern. Eng. Technol. Sci.*, vol. 07, 2025, p. 543 à 548.

ERDOS, D., « Towards Effective Supervisory Oversight? », *Cambridge Legal Studies Research Paper*, 2022, p. 1 à 36.

GREENLEAF, G., « Australia's never-ending privacy reform process », (2023) 186 *Privacy Laws & Business International Report*, p. 1 à 5.

GREENLEAF, G., « Singapore's Personal Data Protection Act 2012 : Scope and principles », *P.L. & B. Int. Report*, n° 120, 2012, p. 5 à 7.

HOOFNAGLE, C. J. et URBAN, J. M., « Alan Westin's Privacy Homo Economicus », *Wake Forest L. Rev.*, vol. 49, 2014, p. 261 à 317.

HOOFNAGLE, C. J., VAN DER SLOOT, B. et ZUIDERVEEN BORGESIUS, F., « The European Union General Data Protection Regulation: what it is and what it means », *Information & Communications Technology Law*, vol. 28, 2019, p. 65 à 98.

KAR, R. B. et YU, X., « The Contractual Death and Rebirth of Privacy », *Harv. J. L. & Tech.*, vol. 38, 2024, p. 1104 à 1164.

KOSTA, E., « Peeking into the cookie jar: the European approach towards the regulation of cookies », *Int. J. L. Inf. Technol.*, vol. 21, n° 4, 2013, p. 380 à 406.

MACHULETZ, D. et BÖHME, R., « Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR », *Proc. Priv. Enhancing Technol.*, vol. 2020, n° 2, 2020, p. 481 à 498.

MARTIN, K., « Privacy Notices as Tabula Rasa : An Empirical Investigation into How Complying with a Privacy Notice is Related to Meeting Privacy Expectations Online », *J.P.P. & M.*, 2014, p. 68 à 85.

NOUWENS, M., LICCARDI, I., VEALE, M., KARGER, D. et KAGAL, L., « Dark Patterns after the GDPR : Scraping Consent Pop-ups and Demonstrating their Influence », *CHI'20*, 2020, p. 1 à 13.

PILGRAM, L., FINEBERG, A., JONKER, E. et EL EMAM, K., « An assessment of synthetic data generation, use and disclosure under Canadian privacy regulations », *AI and Ethics*, vol. 5, 2025, p. 6225 à 6240.

POULLET, Y., « Consentement et RGPD : des zones d'ombre ! », *D.C.C.R.*, 2019/1-2, n° 122-123, p. 3 à 37.

SCHERMER, B. W., CUSTERS, B. et VAN DER HOF, S., « The crisis of consent : how stronger legal protection may lead to weaker consent in data protection », *Ethics Inf. Technol.*, n° 16, 2014, p. 171 à 182.

SCHWARTZ, P. M., « The EU-US Privacy Collision : A Turn to Institutions and Procedures », *Harv. L. Rev.*, vol. 126, 2013, p. 1966 à 2009.

SERWIN, A. B., « The Federal Trade Commission and Privacy : Defining Enforcement and Encouraging the Adoption of Best Practices », *San Diego L. Rev.*, vol. 48, 2011, p. 809 à 856.

SHARMA, A., « Consent, Control, and Compliance : Assessing India's Digital Personal Data Protection Laws », *Indian Journal of Law and Legal Research*, vol. 5, n° 2, 2023, p. 1711 à 1722.

SIGMUND, T., « Attention Paid to Privacy Policy Statements », *Information*, vol. 12, n° 4, 2021, p. 1 à 17.

SOLOVE, D. J., « Murky consent: an approach to the fictions of consent in privacy law », *B. U. L. Rev.*, vol. 104, 2024, p. 593 à 639.

SOLOVE, D. J., « Privacy Self-Management and the Consent Dilemma », *Harv. L. Rev.*, vol. 126, 2013, p. 1880 à 1903.

SOLOVE, D. J., « The limitations of privacy rights », *Notre Dame L. Rev.*, vol. 98, n° 3, 2023, p. 975 à 1036.

SOLOVE, D. J. et HARTZOG, W., « The FTC and The New Common Law of Privacy », *Colum. L. Rev.*, vol. 114, 2014, p. 583 à 676.

TSCHIDER, C.A., « Meaningful Choice : A History of Consent and Alternatives to the Consent Myth », *N.C. J.L. & Tech.*, vol. 22, n° 4, 2021, p. 617 à 680.

UTZ, C., DEGELING, M., FAHL, S., SCHAUB, S. et HOLZ, T., « (Un)informed Consent : Studying GDPR Consent Notices in the Field », *C.C.S.'19*, 2019, p. 973 à 990.

WAGNER, I., « Privacy Policies Across the Ages : Content and Readability of Privacy Policies 1996-2021 », *A.C.M. Trans. Priv. Sec.*, vol. 26, n° 3, art. 32, 2023, p. 1 à 23.

WALTERS, R. et COGHLAN, M., « Data Protection and Artificial Intelligence Law : Europe Australia Singapore », *Am. J. Sci. Eng. Tech.*, vol. 4, 2019, p. 55 à 65.

WONG YONGQUAN, B., « Data privacy law in Singapore », *Int. Data Priv. Law*, vol. 7, 2017, p. 287 à 302.

ZIMMECK, S., WANG, O., ALICKI, K., WANG, J. et ENG, S., « Usability and Enforceability of Global Privacy Control », *Proceedings on Privacy Enhancing Technologies*, 2023/2, p. 265 à 281.

ZUIDERVEEN BORGESIUS, F., KRUIKEMEIER, S., BOERMAN, S. C. et HELBERGER, N., « Tracking Walls, Take-It-Or-Leave-It Choices, The GDPR, and The ePrivacy Regulation », *E.D.P.L.*, vol. 3, n° 3, p. 1 à 16.

Contributions à des ouvrages collectifs

AUSTIN, L. M., « Enough About Me : Why Privacy is About Power, Not Consent (or Harm) », A. SARAT (dir.), *A World Without Privacy : What Can/Should Law Do*, Cambridge, Cambridge University Press, 2015, p. 131 à 190.

BENSOUSSAN, A., « Consentement », *La protection des données à caractère personnel de A à Z*, Bruxelles, Bruylant, 2017, p. 45 à 52.

CATE, F. H., « The Failure of Fair Information Practice Principles », J. K. WINN (dir.), *Consumer Protection in the Age of the Information Economy*, Washington, Ashgate, 2006, p. 341 à 379.

CUSTERS, B., DECHESNE, F., PIETERS, W., SCHERMER, B. W. et VAN DER HOF, S., « Consent and Privacy », *The Routledge Handbook of the Ethics of Consent*, Londres, Routledge, 2019, p. 247 à 258.

GREENLEAF, G., « Privacy in Australia », J. RULE et G. GREENLEAF (éd.), *Global Privacy Protection: The First Generation*, Cheltenham, Edward Elgar, 2008, p. 1 à 55.

KORUNOVSKA, J., KAMLEITNER, B. et SPIEKERMANN, S., « The Challenges and Impact of Privacy Policy Comprehension », J. KORUNOVSKA et al. (dir.), *Privacy Policy Comprehension: Challenges and Impact*, 2020, p. 1 à 20.

SCASSA, T., « AI and Data Protection Law », *Artificial Intelligence and the Law in Canada*, Toronto, LexisNexis, 2021, p. 1 à 30.

SCASSA, T., « Data Protection and the Internet : Canada », D. MOURA VICENTE (dir.), *Data Protection in the Internet. Ius Comparatum*, vol. 38, Cham, Springer, 2020, p. 55 à 80.

YIP, M., « Personal Data Protection Act 2012 : Understanding the Consent Obligation », *Personal Data Protection Digest*, 2017, p. 265 à 285.

Documents officiels et rapports

Australie

ATTORNEY-GENERAL'S DEPARTMENT, *Privacy Act Review Report*, Canberra, février 2023.

GREENLEAF, G., WATERS, N., LANE, K., ARNOLD, B. et CLARKE, R., « Bringing Australia's *Privacy Act* up to international standards », soumission de l'Australian Privacy Foundation, 18 décembre 2020.

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER (ci-après « OAIC »), « Australian Privacy Principles Guidelines », disponible sur www.oaic.gov.au, 22 juillet 2019.

OAIC, « Australian Privacy Principles Guidelines, chapitre B », disponible sur www.oaic.gov.au, 21 décembre 2022.

WATERS, N. et GREENLEAF, G., « A critique of Australia's proposed *Privacy Amendment (Enhancing Privacy Protection) Bill* 2012 », soumission au Parlement australien, 14 août 2012.

Canada

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Consent and privacy », disponible sur www.priv.gc.ca, 10 septembre 2019.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Guidelines for obtaining meaningful consent », disponible sur www.priv.gc.ca, 2019.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, « Interpretation Bulletin : Form of Consent », disponible sur www.priv.gc.ca, 11 décembre 2015.

Singapour

GIROT, C. et PAULGER, D., *Singapore : Status of Consent for Processing Personal Data*, ABLI-FPF Convergence Series, Asian Business Law Institute et Future of Privacy Forum, août 2022.

PERSONAL DATA PROTECTION COMMISSION (ci-après « PDPC »), « Accountability », disponible sur www.pdpc.gov.sg, 14 septembre 2021.

PDPC, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act*, 16 mai 2022.

PDPC, « Data Protection Obligations », disponible sur www.pdpc.gov.sg, 8 novembre 2023.

Union européenne

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES (ci-après « E.D.P.B. »), « Lignes directrices 03/2022 relatives aux interfaces trompeuses », disponible sur www.edpb.europa.eu, 13 octobre 2022.

EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS et KANTAR, *The General Data Protection Regulation – Report*, Publications Office, 2019.

E.D.P.B., « Lignes directrices 05/2020 sur le consentement au sens du règlement (UE) 2016/679 », révisées et adoptées le 4 mai 2020.

E.D.P.B., « Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de surveillance en vertu du règlement (UE) 2016/679 », adoptées le 4 juin 2019.

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, « Guidelines on consent under Regulation 2016/679 », adoptées le 10 avril 2018.

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNEES, « Lignes directrices sur l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si un traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 », adoptées le 4 octobre 2017.

Sources en ligne

ABRAHAM, S., « Law & the Digital Society : Fine-tuning Digital Personal Data Protection Rules 2025 for Effective Implementation », disponible sur www.thehinducentre.com, 15 mars 2025.

ALLIANCE DIGITALE, « Digital Omnibus : les 17 recommandations d'Alliance Digitale pour simplifier efficacement le RGPD et la directive ePrivacy », disponible sur www.alliancedigitale.org, 1er avril 2026.

BAIG, A. et MALIK, O. I., « CPRA Do Not Sell or Share My Personal Information », disponible sur www.securiti.ai, 10 juin 2024.

BARAT, D., « Yes Means Yes : Managing Consent Under India's New Data Protection Law », disponible sur www.chambers.com, 20 septembre 2023.

BOUCKAERT, C., « Le règlement e-Privacy : c'est fini », disponible sur www.idfrights.org, 12 février 2025.

CALIFORNIA ATTORNEY GENERAL, *Final Statement of Reasons : California Consumer Privacy Act Regulations*, Sacramento, Department of Justice, 2020, disponible sur www.oag.ca.gov.

CALIFORNIA PRIVACY PROTECTION AGENCY, « CPRA Rulemaking Documents – Final Regulations Text », disponible sur www.cppa.ca.gov, 2023.

C.N.I.L., « Certifications et codes de conduite : la CNIL cartographie le déploiement des outils RGPD en Europe », disponible sur www.cnil.fr, 14 janvier 2026.

C.N.I.L., « L'intérêt légitime : comment fonder un traitement sur cette base légale ? », disponible sur www.cnil.fr, 2 décembre 2019.

DATA SECURE, « Consent Management Under India's DPDP ACT : Best Practices for Compliance », disponible sur www.dpo-india.com, 30 avril 2025.

DEBORSHI, B., « Daring To Deem ? 'Deemed' Consents Under India's Proposed Data Protection Law », disponible sur www.mondaq.com, 4 juillet 2023.

DEBORSHI, B., « Notice And Consent Requirements In India's New Digital Data Regime », disponible sur www.mondaq.com, 20 juin 2023.

FREEDMAN, B., « Digital Privacy Act – new requirement for valid consent to use personal information », disponible sur www.lexology.com, 25 juin 2015.

GREENLEAF, G., « India's 2023 Data Privacy Act : Business/government Friendly, Consumer Hostile », disponible sur www.ssrn.com, 16 août 2023.

KERRY, C. F., « Why protecting privacy is a losing game today – and how to change the game », disponible sur www.brookings.edu, 12 juillet 2018.

MBAEZUE, V., « Allow/Accept Cookie. Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) and the E-privacy Directive 2002/58/EC (amended in 2009) stance on Web Cookies », disponible sur www.ssrn.com, 7 juillet 2024.

OURRAHTE, M., ZIANI, F.-E. et EL-YAHYAOUI, A., « Between Compliance and Illusion: An International Comparative Study of Cookie Consent Mechanisms », disponible sur www.papers.ssrn.com, 13 octobre 2025.

RAKTIMA, R., « Top 10 operational impacts of India's DPDPA – Consent management », disponible sur www.iapp.org, 11 juillet 2024.

SMITH, A., « Half of online Americans don't know what a privacy policy is », disponible sur www.pewresearch.org, 4 décembre 2014.

TANCZER, L. M., CARR, M., BRASS, I., STEENMANS, I. et BLACKSTOCK, J., *IoT and Its Implications for Informed Consent*, PETRAS IoT Hub, STEaPP, Londres, 25 juillet 2017, disponible sur www.ssrn.com.

WORLD WIDE WEB CONSORTIUM (W3C), « Global Privacy Control (GPC) », disponible sur www.w3.org, 19 février 2026.

X, « Europäischer Datenschutztag: Umfrage zeigt: Mehrheit der Deutschen findet Datenschutz im Netz zu kompliziert », disponible sur www.eco.de, 27 janvier 2025.

X, « Final Report Summary – CONSENT », disponible sur www.cordis.europa.eu, 7 août 2014.

X, « Role of Consent Managers », disponible sur www.dpdpaedu.org, s.d., consulté le 20 février 2026.