ASSEMBLÉE PARLEMENTAIRE DE LA FRANCOPHONIE

COMMISSION
Affaires Parlementaires

Rapport sur La législation de protection des données personnelles dans l'espace francophone

Présenté par

M. Ouattara Abbas Imbassou, Député (Côte d'Ivoire)
et de M. Fathi Derder, Député (Suisse)

Rapporteurs

ABIDJAN (CÔTE D'IVOIRE) | 8-9 JUILLET 2019

Table des matières

Questionnaire et rapport intermédiaire sur la législation de protection des données personnelles au sein de l'espace francophone.

1. Réponses précises et argumentées de onze sections

Onze sections ont répondu au questionnaire: la Suisse, Monaco, la France, la Belgique, la Roumanie, la Hongrie, la Catalogne, le Sénégal, Bénin, le Canada et Québec. Cela donne une bonne vue d'ensemble, mais il va de soi que nous souhaitons compléter notre vision avec un maximum de participations pour ce sujet hautement stratégique dans un monde numérisé. Nous relancerons le questionnaire après la CAP d'Ottawa.

2. Résumé: tous les pays s'adaptent au défi de la protection des données

Tous les pays qui ont répondu disposent d'une loi sur la protection des données, et dans tous les cas mentionnés, la loi a été mise à jour récemment - ou est en cours de mise à jour - pour s'adapter à l'explosion de la diffusion des données personnelles, liée à la numérisation de la société, à l'utilisation des réseaux sociaux, aux objets connectés, ou à la numérisation de la médecine, tant pour la recherche scientifique que les dossiers de patients. Toutes suivent le même objectif, que résume la révision de la loi suisse:

- Améliorer la **transparence** des traitements.
- Améliorer le **contrôle** que les personnes peuvent exercer sur leurs données.
- Préciser et étendre les **obligations** des responsables de traitement.
- Renforcer les compétences et pouvoirs des **autorités de protection des données**.
- Revoir et étendre les **sanctions pénales**.

Le Règlement général sur la protection des données (RGPD) du 27 avril 2016 a été introduit dans les pays membres de l'Union européenne dans le même esprit. Il introduit ou consolide les notions suivantes:

- Le **droit de la personne**;
- La **transparence** des informations, des communications, et les modalités d'exercice des droits de la personne;
- Le **droit à l'information**;
- Le **droit d'accès aux données**;
- Le **droit de modifier des données** / le droit à la rectification;
- Le **droit à l'opposition**;
- Le **droit de saisir la justice**;
- Le **droit à l'oubli**;
- Le **droit à la restriction du traitement** des données;
- Le **droit à la portabilité** des données.

La **portabilité** des données, a été introduit dans le RGPD, mais relevons que cette notion ne fait pas l'unanimité au sein des pays francophones. **La Suisse, le Canada ou Québec**, notamment, ne l'ont pas prévu. On constate également une divergence entre pays membres sur **la charge de la preuve**, parfois incombant au citoyen, parfois à l'entité chargée du traitement des données. Par contre, la notion de **consentement** fait l'unanimité: les usagers doivent donner leur accord et être informés de l'utilisation de leurs données (article 7 du RGPD). Même si, comme le relève le **Canada** le principe est difficile, voire impossible à mettre en oeuvre à l'heure des mégadonnées et des algorithmes. De nouvelles pistes doivent être explorées, comme la transparence des algorithmes. Enfin, notons qu'aucun n'état n'envisage

de définir dans la loi une **propriété** des citoyens sur leurs données, confirmant ainsi la vision de l'AFAPDP (cf déclaration du 18 octobre 2018 ci-jointe).

3. Le consentement du citoyen, un élément central (qui a ses limites)

La notion de consentement est centrale pour tous les pays consultés. Cette notion est centrale notamment dans le **RGPD**, comme le rappelle **la France**: « *Des mesures ont été prises pour renforcer la protection des données personnelles, notamment avec la loi de juin 2018 qui met en application le RGPD. D'abord la notion de consentement est introduite, c'est-à-dire que les usagers doivent donner leur accord et être informés de l'utilisation de leurs données (article 7). Une mesure spécifique s'adresse aux mineurs dans l'article 7-1 «Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur ».*

L'absence de consentement peut être lourde de conséquences pénales, comme le souligne **le Sénégal**: *« Pour appuyer les mesures prises par la loi de 2008-12, 1a loi 2016-29 portant révision du Code pénal contient des dispositions visant à protéger les données à caractère personnel et la vie privée. La loi criminalise par exemple l'acte de « conserver sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales ou qui sont relatives à la santé de celui-ci». Elle criminalise également « celui qui au moyen d'un procédé quelconque, porte volontairement atteinte à l'intimité de la vie privée d'autrui en captant, enregistrant, transmettant ou diffusant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ; en fixant, enregistrant, transmettant ou diffusant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. »*

Précision importante de **Monaco**: « *Le consentement ne peut être donné que pour une durée limitée, laquelle ne peut excéder celle correspondant aux relations contractuelles entre l'usager et l'opérateur ou le prestataire de services* ».

Le consentement est un élément central, mais qui a ses limites. Comme le relève **le Canada**: « *Reconnu comme la pierre angulaire de la loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada, le consentement est l'outil qui permet aux individus d'affirmer leur autonomie et d'exercer un contrôle sur leurs renseignements personnels. La loi oblige les organisations qui souhaitent recueillir, utiliser ou communiquer des renseignements personnels à solliciter et à obtenir le consentement des intéressés. Toutefois, les avancées technologiques comme les mégadonnées, l'Internet des objets, l'intelligence artificielle et la robotique posent de sérieux défis pour les parties impliquées dans une transaction. Les organisations soutiennent qu'elles ne sont pas toujours en mesure de déterminer ou prévoir toutes les raisons pour lesquelles les renseignements personnels pourraient être utilisés ou communiqués dans le marché d'aujourd'hui en constante évolution et axé sur les données. Dans ce contexte, les efforts déployés pour expliquer les pratiques de protection de la vie privée prennent généralement la forme de politiques ou ententes sur les conditions d'utilisation formulées dans un jargon juridique, souvent incompréhensibles, qui ne cessent de changer. Il serait injuste de s'attendre à ce que les individus soient en mesure d'exercer un véritable contrôle sur leurs renseignements personnels ou de toujours prendre des décisions éclairées lorsqu'il s'agit de donner leur consentement. Voilà en quoi consiste le dilemme, qui ne peut que devenir plus complexe ».*

Il faut donc aller plus loin, estime **le Canada**: « Le consentement demeure au cœur de l'autonomie personnelle, mais il faut ajouter d'autres mécanismes pour l'appuyer et ainsi protéger la vie privée plus efficacement. Notamment, des organismes de réglementation indépendants qui renseignent les citoyens, orientent l'industrie, lui demandent des comptes et *sanctionnent les comportements inacceptables. On doit aussi envisager d'autres outils de protection de la vie privée dans des situations exceptionnelles et justifiables où cela est pratiquement impossible d'obtenir le consentement* ».

Le Canada recommande, notamment, de prévoir explicitement l'adhésion facultative par défaut, renforcer la transparence algorithmique, ou prévoir la révocation du consentement.

4. A qui incombe la charge de la preuve? Divergences de vue

Les pays francophones ont deux approches de la question de la charge de preuve. La question est: le responsable du traitement doit-il démontrer qu'il traite les données de manière licite? Ou le citoyen doit-il démontrer qu'un traitement est illicite? Pour **l'UE, le Sénégal et Québec**, la charge de la preuve incombe à l'entreprise privée ou l'organisme responsable, et non le citoyen.

Comme le rappelle **la Hongrie**, *« selon les règles du RGPD, le responsable de la gestion de données doit certifier qu'il respecte les exigences (article 5, paragraphe 2, du GDPR), de sorte que la charge de la preuve incombe au responsable de la gestion de données dans tous les cas »*. **La Catalogne** précise: « *Une des nouveautés que présentent le RGPD et la LOPDGDD est l'évolution vers un modèle basé sur le principe de la responsabilité active qui exige une évaluation préalable, de la part du responsable ou de la personne en charge du traitement, du risque que le traitement puisse générer. Par conséquent, c'est le responsable ou la personne en charge du traitement qui doit garantir et doit pouvoir démontrer que le traitement est conforme à la réglementation sur la protection des données et qu'il a adopté les mesures les plus appropriées pour garantir les droits et les libertés des personnes dont il traite les données »*. Complétons avec les remarques de **la France**: « *Le titre I de l'article 39 de la Loi du 6 janvier 1978 (modifiée par l'article 34 de la loi du 20 juin 2018) dispose que « Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel ». Le titre II dispose quant à lui que « Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées. » L'article 40 prévoit quant à lui que « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent. En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.* »

Le Sénégal a également pris cette option: *« Selon la loi 2008-12, précisément en ses articles 66 et 69, la charge de la preuve incombe au responsable du traitement des données et auprès de qui les demandes sont formulées. L'article 66 traite du droit d'accès aux données et l'article 69 du droit de rectification et de suppression des données et dans tous les deux cas s'il y a contentieux, la charge de la preuve incombe responsable du traitement »*. Enfin, pour le

Québec, « *l'entreprise privée ou l'organisme en cause et non le citoyen doit démontrer que le renseignement demandé est nécessaire* ».

La Suisse, Monaco, et le Bénin, estiment par contre que *« c'est à la personne auprès de laquelle des informations nominatives ont été recueillies qu'il incombe de prouver que ces informations ont été utilisées sans son accord »*, comme l'affirme Monaco. En Suisse, « *le projet de LPD révisée ne prévoit pas de renversement du fardeau de la preuve en faveur de la personne dont les données sont traitées, même si cela a pu être évoqué un temps* ». Mais le Parlement peut encore modifier cette proposition du gouvernement.

Au Canada, *« lorsqu'une plainte est déposée, le commissaire à la protection de la vie privée est chargé d'enquêter et de recueillir l'information pertinente. Lorsqu'une plainte faite au Commissariat à la protection de la vie privée se rend devant la Cour fédérale, la charge de la preuve incombe aux citoyens ou au commissaire à la protection de la vie privée lorsqu'il s'agit de démontrer qu'une obligation prévue à dans la LPRP ou dans la LPRPDE a été violée »*.

5. La portabilité: une nouveauté du RGPD qui ne fait pas l'unanimité

C'est une des importantes nouveautés du RGPD: le **droit à la portabilité** rend aux usagers la maîtrise de leurs données, ou pour être précis, la possibilité pour eux de récupérer leurs données personnelles ou d'obtenir leur transfert à un autre prestataire. Les pays membres de l'UE mentionnent l'introduction de la portabilité dans leur loi, sans détailler les avantages ou tirer un bilan de cette introduction.

En parallèle, les pays qui ont renoncé à le faire - la Suisse, le Québec, le Canada, ou Monaco - ne détaillent pas les raisons de leurs réticences. Et la porte n'est pas fermée au Canada: « *Dans son rapport sur la LPRPDE, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique recommande « Que le gouvernement du Canada modifie la Loi sur la protection des renseignements personnels et les documents électroniques afin d'y prévoir un droit à la portabilité des données* ».

Le gouvernement suisse, de son côté, recommande d'attendre que l'UE tire un bilan de son introduction. L'instauration d'un droit à la portabilité des données n'est actuellement pas prévue. Le Conseil fédéral s'y oppose pour l'instant en soulignant que cette disposition relève d'abord du droit de la concurrence, qu'elle est difficilement applicable et générerait des coûts importants sans garantie d'effets.

Dans tous les cas, pour ou contre la portabilité, l'argumentaire des uns et des autres méritent d'être détaillés. Un nouvel envoi du questionnaire doit être envisagé.

6. Le citoyen propriétaire de ses données? Un « non » unanime

La CAP de l'APF a souhaité ouvrir le débat sur la propriété des données. Peut-on l'attribuer au citoyen? Une telle mesure renforcerait-elle la protection des données personnelles? La consultation menée est claire: c'est un « non » unanime.

La Belgique est catégorique: *« Le Règlement européen n'autoriserait pas le législateur national à prendre des dispositions spécifiques en la matière. Dès lors, la législation belge ne consacre pas le droit de la propriété des données. Ce concept n'a d'ailleurs pas de statut légal en Belgique. Par contre, il existe différents mécanismes de protection des données, dont le RGPD. Actuellement, la propriété relative aux données ne peut porter que sur la création intellectuelle (droit d'auteur, marque, brevet, …) »*. On ne peut pas définir de propreté sur les données, mais on doit prendre des mesures pour les protéger. C'est aussi le constat de **la France**, avec les quatre missions principales de la CNIL : *« Informer/protéger les particuliers*

et les professionnels en les sensibilisant à la protection et au traitement des données personnelles, accompagner/conseiller les organismes sur les démarches de conformité, contrôler/sanctionner le respect de la loi de protection des données et, finalement, anticiper les technologies et nouveaux usages pouvant avoir des impacts sur la vie privée ».

Pour **la Suisse**, *« les données à caractère personnel sont des éléments constitutifs de la personne humaine, qui dispose, dès lors, de droits inaliénables sur celles-ci. Il n'est pas souhaitable d'envisager une situation qui ne ferait qu'accentuer le déséquilibre existant entre les personnes dont les données sont collectées et les responsables de traitement, et ne permettrait pas aux personnes de créer les conditions d'une relation contractuelle équitable »*. La Suisse précise: *« La LPD permet aux individus d'exercer pleinement les droits inaliénables attachés à leurs données personnelles, en leur garantissant un haut niveau de maîtrise sur celles-ci »*. Elle rejoint ici le point de vue de l'**AFAPDP**, qui souligne dans une récente résolution que *« les données à caractère personnel sont des éléments constitutifs de la personne humaine, qui dispose, dès lors, de droits inaliénables sur celles-ci »*.

Même raisonnement à **Monaco**, qui souligne que *« la loi monégasque ne raisonne pas en termes de propriété des données, mais rattache au contraire ces dernières à la catégorie des droits extrapatrimoniaux, dans la mesure où elle vise, à travers la protection des données personnelles, à protéger la personne elle-même, ainsi que sa vie privée. En droit monégasque, la personne est par conséquent titulaire de ses informations personnelles, mais n'en est pas juridiquement propriétaire, puisque ces dernières constituent des droits extrapatrimoniaux et non des biens mobiliers incorporels sur lesquels pourrait s'exercer un droit réel »*.

La **Catalogne** complète: *« Il convient de rappeler que le droit à la protection des données, comme tout autre droit, n'est pas un droit absolu et que des exceptions au contrôle des données personnelles peuvent être fixées, par exemple lorsque la loi l'établit ainsi. Notre réglementation en matière de protection des données règle une série de droits que le citoyen détient pour contrôler ses données, par exemple, le droit de ne pas être soumis à des décisions individuelles automatisées, en incluant ceux sur l'élaboration de profils, droits d'accès, de rectification, de suppression, de limitation du traitement, de la portabilité et d'opposition, en plus du droit à l'information. Finalement, elle réglemente les procédures en cas de violation éventuelle des réglementations sur la protection des données et le régime de sanctions, par conséquent, notre législation essaye de donner au citoyen le contrôle, la visibilité et les plus amples connaissances possibles de l'utilisation de ses données »*.

Et comme le rappelle le **Canada**, le respect de la vie privée passe avant tout par le consentement mentionné plus haut: *« La LPRPDE, qui s'applique aux organisations du secteur privé, ne discute pas spécifiquement de la propriété des données. Malgré tout, au Canada, l'autonomie des individus quant à leurs renseignements personnels est discutée sous plusieurs angles. Ces angles incluent, entre autres, le consentement, la réputation en ligne ainsi que le modèle de surveillance de la loi »*.

7. Conclusion: une bonne vue d'ensemble, mais qui doit être complétée

En conclusion (provisoire), le rapport nous permet d'avoir une vision très complète et détaillée de la politique des sections membre en matière de protection des données. Nous avons tout à gagner à poursuivre ce travail dans ce domaine sensible, inconnu et peu expérimenté ou tout reste encore à faire. Le partage d'expérience est essentiel pour adopter des lois efficaces et utiles. Nous allons donc renvoyer le questionnaire aux sections qui n'ont pas répondu pour les encourager à le faire.

Un point mérite en outre d'être approfondi: comme évoqué, les sections qui ont répondu détaillent peu les raisons pour lesquelles elles ont adopté ou non adopté la portabilité. Les arguments mériteraient d'être détaillés et approfondis. Nous renverrons là aussi le questionnaire pour compléter ce point précis auprès des sections qui ont déjà répondu.

En outre, de nombreux domaines restent encore à explorer: comme l'intelligence artificielle (**Belgique**), les transferts internationaux de données (**Belgique et Catalogne**), ou la transparence des algorithmes (**Canada**). Nous ferons la synthèse des réponses sur les pistes à explorer lors du rapport final présenté à Abidjan.

Notons enfin que la question de l'encouragement du partage de données a été mal formulée, car aucune section (sauf une) a compris la question: il s'agit d'identifier des mesures pour encourager réellement les citoyens à partager leurs données (anonymisées, protégées) pour les besoins de la science notamment. Seul **le Québec** a répondu:

« Les ministères et organismes gouvernementaux sont assujettis depuis 2008 au Règlement sur la diffusion adopté en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A2.1, r. 2. Ce règlement prévoit la diffusion proactive de « données ouvertes » sur le portail Données Québec. Dans son rapport quinquennal de 2016, la Commission d'accès à l'information a recommandé au gouvernement d'adopter des dispositions de même nature qui viseraient les secteurs de l'éducation et de la santé, et les municipalités du Québec ».

Ces points seront complétés dans les semaines à venir, par envoi de questionnaire ou échange directe à Ottawa, afin de finaliser le rapport en vue de de la CAP et l'Assemblée générale d'Abidjan.

8. Annexe (réponses des sections au questionnaire sur la législation de protection des données personnelles dans l'espace francophone

1. Disposez-vous d'une loi sur la protection des données ? (De quand date-t-elle ?, A-t-elle été révisée récemment ? Si non, des mesures portant sur la protection des données sont-elles intégrées dans une autre loi ?	
Suisse	Oui. La loi fédérale sur la protection des données (LPD) date du 19 juin 1992 et est entrée en vigueur le 1er juillet 1993.[1] La LPD est actuellement en cours de révision. Le 15 septembre 2017, le Conseil fédéral a présenté un projet de révision totale de la loi.[2] Le 11 janvier 2018, la Commission des institutions politiques du Conseil national (Chambre basse) a décidé de scinder la révision en deux volets et de ne traiter dans un premier temps que les modifications législatives indispensables à l'intégration de l'acquis de Schengen : a. La loi sur la protection des données Schengen (LPDS) qui est entré en vigueur le 1er mars 2019. Cette adaptation de la législation suisse au droit européen était nécessaire à l'intégration de l'acquis de Schengen. Elle est conçue comme une loi de transition et comprend diverses nouvelles dispositions.[3] b. La révision totale de la LPD : les travaux sont toujours en cours. Les buts de la révision sont : • Améliorer la transparence des traitements • Améliorer le contrôle que les personnes peuvent exercer sur leurs données • Préciser et étendre les obligations des responsables de traitement • Renforcer les compétences et pouvoirs du Préposé fédéral • Revoir et étendre les sanctions pénales[4]
Monaco	La loi monégasque relative à la protection des données personnelles est la loi n° 1.165 du 23 décembre 1993, relative à la protection des informations nominatives, modifiée. La dernière réforme d'importance de cette loi a eu lieu à l'occasion du vote de la loi n° 1.353 du 4 décembre 2008 modifiant la loi n° 1.165 précitée. Toutefois, pour adapter les pouvoirs d'investigation de la Commission de Contrôle des Informations Nominatives, organe chargé notamment de veiller à la régularité des traitements d'informations nominatives, aux exigences de la jurisprudence monégasque, la loi n° 1.165 a également été modifiée par la loi n° 1.420 du 1er décembre 2015.

[1] Lien direct vers la Loi : https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html
[2] Informations sur le projet de révision : https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html
[3] Informations supplémentaires sur cette loi : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/police--defense-et-migration/les-accords-de-schengen-et-de-dublin/Schengen-DSG.html
[4] Les délibérations parlementaires encore en cours se trouvent via le lien suivant : https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059

	En outre, des mesures portant sur la protection des données ont été intégrées dans la loi n° 1.435 du 8 novembre 2015 relative à la lutte contre la criminalité technologique, qui consacre, au sein du Code pénal monégasque, les délits d'extraction ou d'altération de données informatiques, lesquelles englobent les données personnelles.
France	Oui, la France dispose de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite « Loi CNIL » en référence à la Commission Nationale de l'Informatique et des Libertés) qui a été modifiée par la Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique et la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Cette dernière modification fait suite à l'application du Règlement Général sur la Protection des Données (RGPD) le 25 mai 2018.
Belgique [5]	A l'instar des autres pays membres, les nouvelles règles en matière de protection de la vie privée sont d'application depuis le 25 mai 2018. C'est la conséquence de l'entrée en vigueur du Règlement général sur la protection des données (RGPD) du 27 avril 2016[6]. Ce règlement s'applique directement dans notre pays. Celui-ci a été complété **(quest. 1):** - par **la loi[7] du 30 juillet 2018** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (annexe 1). Cette loi, publiée au Moniteur belge du 5 septembre 2018, abroge la loi sur la vie privée du 8 décembre 1992 ; - la **loi du 5 septembre 2018** instituant le comité de sécurité de l'information (CSI) a été publiée au moniteur belge du 10 septembre (annexe 2). Le CSI est constitué d'une chambre sécurité sociale et d'une chambre autorité fédérale (art. 2, §2). Il fournira des avis sur certaines communications de données à caractère personnel au sein de l'autorité fédérale, sur la transmission de données via la Banque-Carrefour de la sécurité sociale ou sur la transmission de données concernant la santé. Dans le cadre de ces avis, le CSI examinera si la communication est conforme aux principes de base du RGPD. En outre, il y a lieu de noter que par une loi du 30 juillet 2018, le législateur belge a modifié sa loi relative aux caméras de surveillance en vue de sa conformité au RGPD. **Les principales nouveautés portent sur les points suivants :** **1. Enfants** Le législateur belge a abaissé de 16 à 13 ans l'âge de consentement valable des enfants dans le cadre des services de la société de l'information (art. 7 de la loi).

[5] Afin de permettre une meilleure compréhension de la nouvelle législation belge en la matière, la section Belgique/Communauté française/Wallonie-Bruxelles a préféré faire état des caractéristiques des lois complétant le Règlement européen qui lui est directement applicable plutôt que de répondre systématiquement à toutes les questions

[6] Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JO L 119 du 4 mai 2016.

[7] Il s'agit en réalité d'une loi à vocation générale. Elle inclut non seulement l'exécution du Règlement sensu stricto mais aussi la transposition de la directive 2016/680 relative aux traitements des données liées à la commission d'infractions pénales et à leurs sanctions, ainsi que des règles spécifiques concernant certaines autorités publiques dont les traitements sont hors champ d'application du droit européen (services de renseignements, de sécurité etc…).

Cfr. considérant 6 et 7 portant sur « *l'évolution rapide des technologies et la mondialisation* » - **quest. 2**) ; Art 5, 6, 8, 12 à 23 et 24 à 43 sur les mesures spécifiques visant à assurer et/ou à renforcer la protection des données personnelles **(quest. 3)** ; art 32 et sur la sécurisation des données à caractère personnel ; le chap. V, art 44 et ss sur les transferts des données à caractère personnel vers des pays tiers ou à des organisations internationales **(quest. 4)** ; notamment art. 7, §1 sur la charge de la preuve **(quest. 5)** ; art. 5, 1. B) et 13 concernant la finalité des collectes **(quest. 6)**

	2. Traitement de données sensibles Le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale est, en principe, interdit. Tout comme le traitement de données génétiques, de données biométriques aux fins d'identifier une personne physique de manière unique, de données concernant la santé ou de données concernant la vie sexuelle ou l'orientation sexuelle (art. 9 de la loi). Le traitement des données relatives aux condamnations ou infractions pénales doit être encadré par certaines mesures de sécurité (art. 10 de la loi). **3. Délégué à la protection des données** L'article 21 de la loi dispose qu'un organisme privé qui traite des données à caractère personnel pour le compte d'une autorité publique fédérale ou à qui une autorité publique fédérale a transféré des données à caractère personnel doit désigner un délégué à la protection des données, connu sous le nom de *Data Protection Officier* (DPO) lorsque le traitement de ces données peut engendrer un risque élevé pour les droits et les libertés de personnes physiques, tel que visé à l'article 35 du Règlement. **4. Fins journalistiques, et d'expression universitaire, artistique ou littéraire** La Belgique décharge de certaines obligations du Règlement, le traitement des données à caractère personnel à des fins journalistiques et à des fins académiques, artistiques ou littéraires (art. 24 de la loi). La Belgique fait usage de cette possibilité, non sans prévoir une série de garanties pour les droits et libertés des personnes concernées (art. 36 & ss de la loi). **5. Voies de recours – Charge de la preuve** Les personnes qui estiment être victimes d'une violation de la législation en matière de protection des données ou qui se sentent entravées dans l'exercice de leurs droits, disposent des moyens d'action suivants: – une plainte auprès de l'autorité de contrôle compétente (pas nécessairement l'autorité belge) ; – une action en cessation auprès du tribunal pour faire cesser la violation ; – réclamer des dommages et intérêts devant le tribunal. La loi belge sur la Protection des données prévoit la possibilité de se faire représenter par une organisation ou une association qui est active en matière de protection des données. Cette organisation ou association peut alors déposer une plainte ou aller devant un tribunal au nom de la personne physique concernée. Cette organisation ou association doit cependant en recevoir la demande et ne peut pas saisir l'APD ou un tribunal d'une demande de sa propre initiative. **6. Action en cessation** Lorsqu'une personne ou l'APD veut faire cesser une violation de la législation en matière de protection des données ou veut faire respecter l'exercice de ses droits, une action en cessation peut être introduite auprès du président du tribunal de première instance, siégeant comme en référé.(art. 209 de la loi)

Il est par conséquent question d'une procédure avec des délais réduits en vue de rendre possible une action rapide. Le président du tribunal de première instance peut prévoir les mesures suivantes dans son « ***ordonnance de cessation » (art ; 214-215 de la loi)***:

– laisser un délai pour mettre fin à la violation ou pour accueillir une demande d'exercice d'un droit ;

– publication : affichage de la décision (ou d'un résumé de celle-ci) dans ou hors de l'entreprise et/ou de sa publication dans les journaux ;

– si des données personnelles incorrectes, incomplètes ou non pertinentes, ou des données personnelles dont la conservation est interdite ont été communiquées à des tiers, le traitant ou le responsable du traitement peut se voir obligé de faire connaitre à ce tiers la limitation, la rectification ou l'effacement de ces données personnelles.

S'il existe des motifs sérieux de craindre que des éléments de preuve soutenant la demande en cessation disparaissent ou soient rendus inaccessibles, le demandeur peut demander au président du tribunal de première instance par voie de requête unilatérale d'adopter des mesures prévenant la dissimulation, disparition ou inaccessibilité.

A la suite de l'action en cessation, le demandeur peut réclamer la réparation de son dommage conformément à la responsabilité contractuelle ou extracontractuelle (art. 216 de la loi).

7. **Représentation**

   Quiconque estime qu'il y a eu violation de sa vie privée peut se faire représenter par un organe, une organisation ou une ASBL, qui peut alors introduire une réclamation en son nom et exercer en son nom les recours administratifs ou juridictionnels, soit auprès de l'autorité de contrôle compétente, soit auprès de l'ordre judiciaire, et à condition toutefois d'être actif depuis au moins trois ans dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel.(art. 220 de la loi)

8. **Sanctions**

   Des sanctions administratives sont prévues pour la quasi-totalité des obligations du Règlement. Les infractions graves sont assorties de sanctions pénales.

9. **Mise en œuvre** de cette nouvelle législation au sein de l'un des parlements dont les membres sont représentés au sein de la section Belgique/Communauté française/Wallonie-Bruxelles, **à savoir le Parlement de la Fédération Wallonie-Bruxelles.**

   Le Parlement de la Fédération Wallonie-Bruxelles, l'un des parlements dont les membres francophones font partie de la section Belgique faisant partie de la section Belgique/Communauté française/Wallonie-Bruxelles poursuit sa mise en conformité au RGPD. Cette mise en conformité est un concept qui s'inscrit dans la durée et fait l'objet d'avancement régulier. Les principales avancées effectuées par le Parlement depuis l'entrée en vigueur du RGPD sont :

   - ✓ La mise en place d'un projet de mise en conformité ;
   - ✓ La nomination d'un DPO et d'une équipe RGPD ;
   - ✓ La constitution d'un registre des traitements ;
   - ✓ L'identification des traitements à risque (portant sur des données sensibles) ;
   - ✓ L'amélioration continue de l'infrastructure informatique (sécurité, compartimentation, …) :
   - ✓ La documentation de la mise en conformité.

	La relation entre notre assemblée et le Parlement est assez limitée dans la mesure où l'autorité belge (APD) n'est pas encore pleinement opérationnelle. Néanmoins, un premier contact a été établi afin de communiquer l'identité de notre DPO à l'APD.
Roumanie	Le 4 mai 2016, ont été publiés au Journal Officiel de l'Union Européenne les deux actes normatifs qui composent le paquet législatif sur la protection des données au niveau de l'Union Européenne: **a.** Le **Règlement (UE) 2016/679 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 (Le Règlement général sur la protection des données – RGPD) ; **b.** La **Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données**, et abrogeant la Décision-cadre 2008/977/JAI du Conseil. En ce qui concerne **a** (**Règlement (UE) 2016/679**): En général, les dispositions du Règlement sont directement applicables sur le territoire de l'UE, sans être nécessaire de prévoir des mesures de transposition ou d'implémentation. Toutefois, le Règlement prévoit qu'en situations spécifiques sont nécessaires des dispositions d'implémentation au niveau national et que les états membres sont habilités d'adopter certaines dispositions légales. Donc, en 2018, le cadre juridique roumaine en domaine, datant de 2001 et 2005, a été remplacé par le nouveau Règlement UE qui a été directement appliqué dans son intégralité. De plus, pour faciliter son application, les autorités roumaines ont adoptée deux nouvelles lois en abrogeant les lois existantes devenues inutiles et pour adapter les institutions et les procédures en place à répondre aux nouvelles exigences en matière: - La **Loi 129/2018** pour la modification et la complétion de la Loi 102/2005 sur la *création et le fonctionnement de l'Autorité de surveillance nationale pour le traitement des données personnelles* et pour l'abrogation de la Loi 677/2001 *sur la protection des personnes à l'égard du traitement des données à caractère personnel et la libre circulation de ces données.* - *La **Loi 190/2018** concernant des mesures pour la mise en œuvre du Règlement (UE) 2016/679 du Parlement Européen et du Conseil de 27 avril 2016 pour la protection des personnes physiques concernant le traitement des données à caractère personnel et leur libre circulation* et pour l'abrogation de la Directive 95/46/CE. En même temps, conformément aux provisions de la nouvelle loi, à commencer de juin 2018, toutes les références à la *Loi 677/2001 sur la protection des personnes à l'égard du traitement des données à caractère personnel et la libre circulation de ces données* contenues par les différents actes normatifs sont interprétées comme des références au RGPD et à la législation visant son implémentation.

	En ce qui concerne **b (Directive (UE) 2016/680):** La Directive de l'Union Européenne est entrée en vigueur le mai 2016 et a été transposé dans la législation nationale par la *Loi no 363/2018 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention, de la détection, des enquêtes, des poursuites et de la lutte contre les infractions pénales ou de l'exécution des sanctions ; des mesures en matière d'éducation et de sécurité et la libre circulation de ces données.*
Hongrie	La loi LXIII de 1992 sur la protection des données à caractère personnel et la publicité des données d'intérêt public a été remplacée par la loi CXII de 2011 (Loi sur les infos) sur l'autodétermination de l'information et la liberté de l'information. Un changement majeur a été apporté à la loi sur l'information en juillet 2018 spécifiquement en vue de l'entrée en vigueur du Règlement général sur la protection des données (GDPR) [sur l'amendement relatif à la réforme de la protection des données de l'Union européenne de la loi CXII de 2011 sur l'autodétermination de l'information et la liberté d'information, ainsi que la loi XXXVIII de 2018 modifiant d'autres lois connexes]. L'amendement à la loi sur l'information applique essentiellement les règles GDPR à tous les traitements de données qui ne sont pas couverts par la "directive pénale" [Directive du Parlement européen et du Conseil (UE) 2016/680].
Catalogne	Effectivement, en premier lieu, nous disposons du Règlement (UE) 2016/679, du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Dans le cadre de l'Etat espagnol, la Loi organique 3/2018 du 5 décembre sur la protection des données personnelles et la garantie des droits numériques (ci-après LOPDGDD) a été approuvée. Elle est entrée en vigueur le 7 décembre 2018. L'élaboration de cette nouvelle loi organique qui remplace la Loi organique 15/1999 du 13 décembre sur la protection des données à caractère personnel (bien que les articles 23 et 24 soient toujours en vigueur et qu'elle continue d'être en vigueur dans le domaine de la Directive 2016/680) est venue compléter, dans le cadre de la règlementation espagnole, le Règlement (UE) 2016/679, et en compléter les dispositions. Elle vise également à garantir les droits numériques de la citoyenneté, conformément aux dispositions de l'article 18.4 de la Constitution espagnole. En ce qui concerne le cadre de la réglementation juridique catalane, la Loi 32/2010 du 1er octobre de l'Autorité Catalane de Protection des Données (ci-après APDCAT) a été approuvée. L'Autorité Catalane de Protection des Données est un organisme indépendant de droit public qui a pour objectif de garantir, dans le domaine des compétences de la Generalitat, les droits à la protection des données personnelles et d'accès à l'information qui y est attaché.
Sénégal	Oui, il s'agit de la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel. Adoptée le 30 novembre 2007 par l'Assemblée nationale et le 15 janvier par le Sénat, elle est publiée le 25 janvier 2008. Non, mais la révision ne saurait tarder, l'Administration ayant suggéré par la voix du Président dans le courant du mois de janvier 2019 que la modification de cette loi de 2008 « devrait être accélérée afin de rendre dans les meilleurs délais les dispositions mieux adaptées et adéquates » aux enjeux économiques et sécuritaires de l'heure.

assez large, il s'agit notamment de :
5 janvier 2008 sur la Cybercriminalité
0 août 2008 sur la Cryptologie
5 janvier 2008 sur les transactions électroniques
5 janvier 2008 portant loi d'orientation sur la Société de l'Information.
n le 24 juin 2016 de la convention de l'UA sur la cyber sécurité et la protection des données à caractère

novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal
novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale
2 décembre 2018 portant Code des Communications électroniques

16 juin 2017 portant code du numérique en République du Bénin. Cette loi est récente.

fédéral, dispose de deux lois en matière de protection des renseignements personnels.
n des renseignements personnels
s renseignements personnels[8] (LPRP), qui est entrée en vigueur en 1983, s'applique aux institutions
u'elles recueillent des renseignements personnels. La LPRP s'applique aux institutions fédérales qui sont
e. Notamment, la LPRP impose des obligations juridiques aux institutions fédérales en ce qui a trait à la
server, d'utiliser et de communiquer les renseignements personnels qu'elles détiennent. De plus, la LPRP
droit d'accès aux renseignements personnels qui les concernent et qui sont détenus par des institutions
t de demander que ceux-ci soient corrigés. Finalement, la LPRP prévoit la désignation d'un haut
nt indépendant chargé de la surveillance de l'application de la loi, le Commissaire à la protection de la vie

pas été modifiée de manière significative.
n des renseignements personnels et les documents électroniques
s renseignements personnels et les documents électroniques[9] (LPRPDE), adoptée en 2001[10], s'applique aux
privé. La LPRPDE vise à concilier le droit des individus au respect de la vie privée et le besoin raisonnable
e recueillir, utiliser et communiquer des renseignements à des fins économiques. La LPRPDE s'applique à
l'égard des renseignements personnels :
e ou communique dans le cadre d'activités commerciales;

ses employés ou l'individu qui postule pour le devenir et qu'elle recueille, utilise ou communique dans le
e fédérale[11].
DE ne s'applique pas aux institutions fédérales auxquelles s'applique la LPRP, aux renseignements personnels
muniqués par un individu à des fins personnelles ou privées et aux organisations qui recueillent, utilisent ou
gnements personnels à des fins journalistiques, artistiques ou littéraires. De plus, si une province
i essentiellement similaire à la LPRPDE, le gouverneur en conseil peut, par décret, soustraire les
tés visées par cette loi provinciale à l'application de la LPRPDE[12].
ction de la vie privée du Canada est chargé de la surveillance de l'application de la LPRPDE.
[13] en 2015[14] afin, notamment :
munication de renseignements personnels à l'insu de l'intéressé ou sans son consentement dans certaines

tions à prendre diverses mesures dans les cas d'atteinte à la sécurité des données, notamment la
e des atteintes aux mesures de sécurité;
le fait de ne pas remplir ses obligations en cas d'atteinte à la sécurité des données;
missaire à la protection de la vie privée, dans certaines circonstances, de conclure un accord de conformité
[15].
aucune réforme de la LPRPDE n'a eu lieu depuis 2001.

ent sur la protection des données :
documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1 (Loi

e aux documents détenus par un organisme public dans l'exercice de ses fonctions, que la conservation de
it assurée par l'organisme ou par un tiers. La loi s'applique, quelle que soit la forme de ces documents :
sonore, visuelle, informatisée ou autre.

lberta, de la Colombie-Britannique et du Québec. Voir, Commissariat à la protection de la vie privée du canada, Aperçu des lois sur la protection des

	2. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 (Loi sur le secteur privé). Elle a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du *Code civil du Québec* en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers dans le cadre de l'exploitation d'une entreprise. Les deux lois mentionnées ci-dessus ont été adoptées respectivement en 1982 et en 1993. Elles ont été modifiées notamment en 2006. Elles n'ont pas été révisées récemment (dans les deux cas)[16]. Des mesures portant sur la protection des données sont intégrées dans : ○ Les articles 44 et 45 de la Loi concernant le cadre juridique des technologies de l'information, L.Q. 2001, c. 32 (RLRQ c. C-1.1) portent sur la protection des renseignements biométriques. ○ Une législation fédérale, la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5 traite des transferts internationaux et interprovinciaux de renseignements personnels en matière commerciale ou qui concernent un employé d'une entreprise de compétence fédérale.
2. La loi a-t-elle été adaptée récemment à la numérisation de la société ? **Des dispositions ont-elles été récemment introduites** permettent de renforcer la protection des données ? Et si oui, lesquelles ?	
Suisse	Comme indiqué plus haut, la LPD est actuellement en cours de révision.
Monaco	La dernière modification de la loi n° 1.165 précitée, a eu lieu en 2015, dans le but d'adapter les pouvoirs d'investigations de l'organe chargé de veiller à la régularité des traitements d'informations nominatives. Cependant le Gouvernement a informé le Conseil National qu'un projet de loi inspiré des dispositions du Règlement Général sur la Protection des Données et de celles de Protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 révisée) serait prochainement déposé sur le bureau de l'Assemblée.
France	Les modifications apportées à la Loi CNIL accompagnent la numérisation de la société et touchent différents aspects de la protection de données : d'abord en redéfinissant le champ des données sensibles, en considérant que les données génétiques, biométriques et l'orientation sexuelle en font désormais partie (article 8). Ensuite, avec l'attribution de nouvelles prérogatives à la CNIL pour renforcer son action. Par exemple les sanctions de la CNIL sont étendues et une coopération est rendue possible entre cette Commission et les Etats membres de l'UE (article 49). Parmi ses missions, la CNIL est notamment amenée à « *condui*[re] *une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques* » (article 11).

[16] Le projet de loi nº 179, *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* a été présenté à l'Assemblée nationale le 17 mai 2018. Ce projet de loi est devenu caduc en raison de la dissolution de l'Assemblée en août 2018.

Roumanie	Oui. On peut affirmer que le cadre législatif roumain actuel répond entièrement aux exigences européennes en matière de protection des données.
Hongrie	Loi L de 2013 sur la sécurité de l'information électronique des organes de l'État et des administrations locales (Ibtv.).
Catalogne	La LOPDGDD (Titre X) reconnaît une série de droits numériques et de garanties des citoyens conformément à l'ordre établi par la Constitution espagnole. En particulier, les droits et libertés susceptibles de s'appliquer à Internet tels que la neutralité du réseau et l'accès universel ou les droits à la sécurité et l'éducation numérique ainsi que les droits à l'oubli, à la portabilité et au testament numérique sont objets de réglementation, ainsi que la reconnaissance du droit à la déconnexion numérique dans le cadre du droit à la vie privée lors de l'utilisation d'appareils numériques sur le lieu de travail et la protection des mineurs sur Internet, et finalement, la garantie de la liberté d'expression et du droit de rectification et de mise à jour des informations sur Internet et dans les médias numériques. Afin de garantir ces droits numériques, des modifications ont été apportées à d'autres lois, notamment la Loi organique 2/2006 du 3 mai sur l'éducation, la Loi organique 6/2001 du 21 décembre sur les universités, ainsi que le texte révisé de la Loi sur le statut des travailleurs et le texte révisé de la Loi sur le statut de base de l'employé public.
Sénégal	Oui, des dispositions ont été récemment introduites par la loi 2018-28 du 12 décembre 2018 portant Code des Communications électroniques. Cette loi propose dans l'exposé des motifs « La mise en place d'une protection spécifique des données personnelles des utilisateurs de services de télécommunications, en accord avec les impératifs de sécurité et d'ordre public ». Elle pose comme mesures nouvelles de protection en son article 39, l'effacement ou anonymisation des données techniques et, en son article 40 la protection des droits des personnes figurant dans les listes d'abonnés. La loi renvoie à plusieurs reprises à la Commission de protection des Données personnelles (CDP) créée par la loi 2008-12 du 25 janvier 2008 et traite en son chapitre V de la « Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques ».
Bénin	Oui
Canada	**a. *Loi sur la protection des renseignements personnels*** En 2016, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a présenté un rapport à la Chambre des communes intitulé *Protéger la vie privée des Canadiens : Examen de la* Loi sur la protection des renseignements personnels[17]. Dans son rapport, le Comité illustre le besoin de réformer la LPRP qui n'a pas été adaptée aux changements technologiques et fait plusieurs recommandations à cet égard. Dans le cadre de l'étude, le commissaire à la protection de la vie privée du Canada a présenté un mémoire au Comité et a fait plusieurs recommandations afin de

17 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), *Protéger la vie privée des Canadiens : Examen de la* Loi sur la protection des renseignements personnels, quatrième rapport, 1re session, 42e législature, décembre 2016.

	moderniser la LPRP. Dans la réponse du gouvernement au Comité, l'ancienne ministre de la Justice indique qu'elle procédait à un examen visant la modernisation de la LPRP. **b. *Loi sur la protection des renseignements personnels et les documents électroniques*** En février 2018, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique a déposé un rapport à la Chambre des communes intitulé *Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*[18]. Dans son rapport, le Comité expose les différents examens parlementaires et tentatives de réformes législatives de la LPRPDE. Le Comité fait aussi différentes recommandations afin de moderniser la LPRPDE. Dans sa réponse au Comité, le gouvernement du Canada convient qu'une réforme à la LPRPDE est requise, mais que cette réforme requiert davantage de réflexion. Dans le cadre de l'étude du Comité, le commissaire à la protection de la vie privée du Canada a soumis un mémoire dans lequel il propose quatre domaines d'intervention au Comité afin de moderniser la LPRPDE : - le consentement valable; - la réputation et le respect de la vie privée; - les pouvoirs d'exécution du commissaire; - le caractère adéquat de la LPRPDE par rapport au Règlement général sur la protection des données (RGPD) de l'Union européenne (UE). Le commissaire à la protection de la vie privée a également tenu des consultations sur deux sujets : la notion du consentement valable et la réputation en ligne. En ce qui a trait au consentement, le commissaire a publié dans son *Rapport annuel au parlement 2016-2017* des consultations et sa prise de position. De la même manière, le commissaire a publié un Projet de position exposant ses conclusions et constatations relativement aux enjeux liés à la réputations en ligne, incluant les moteurs de recherches.
Québec	Les lois du Québec mentionnées ci-dessus n'ont pas été modifiées récemment à cette fin. Le Parlement du Canada a adopté la *Loi sur la protection des renseignements personnels numériques*, L.C. 2015, c. 32. Cette législation apporte des modifications à la *Loi sur la protection des renseignements personnels et les documents électroniques* de 2000.

18 ETHI, *Vers la protection de la vie privée dès la conception : Examen de la* Loi sur la protection des renseignements personnels et les documents électroniques, douzième rapport, 1re session, 42e législature, février 2018.

3. **Quelles mesures** spécifiques assurent et ou renforcent la protection des données personnelles ?	
Suisse	Le projet de révision en cours prévoit entre autres : - Une analyse d'impact relative à la protection des données personnelles (*PIA*), exigée lorsque le traitement envisagé est susceptible d'entraîner un risque élevé (art. 20s P-LPD[19]) ; - L'obligation pour les responsables du traitement et les sous-traitants de tenir un registre des activités de traitement ; - La possibilité de se faire certifier par des organismes de certification agréés et indépendants ; - L'introduction des principes de la protection des données dès la conception et par défaut ; - Les dispositions sur la communication de données à l'étranger sont clarifiées ; - Le devoir d'informer la personne concernée en cas de décision individuelle automatisée (art. 19 P-LPD[20]) est complété par un droit de la personne concernée de demander à ce que la décision soit revue par une personne physique ; - L'introduction d'une obligation d'annonce en cas de failles de sécurité.
Monaco	La loi n° 1.165 susmentionnée protège les informations personnelles par l'intermédiaire d'une procédure de déclaration préalable applicable à l'ensemble des traitements, hormis ceux ayant pour fin, notamment, la recherche dans le domaine de la santé, pour laquelle une autorisation préalable de la Commission de Contrôle des Informations Nominatives est requise. De surcroît, cette loi précise la qualité des informations personnelles qu'il est possible de collecter, ainsi que des conditions de licéité du traitement dont elles peuvent faire l'objet. En outre, cette loi permet aux personnes physiques dont les données personnelles ont été collectées de s'adresser au responsable du traitement afin d'accéder à leurs données et, le cas échéant, de s'opposer à leur collecte ou d'obtenir qu'elles soient rectifiées. Par ailleurs, ladite loi impose au responsable de traitement de prendre des mesures adéquates pour assurer la sécurité et la confidentialité de ce dernier.
France	Des mesures ont été prises pour renforcer la protection des données personnelles, notamment avec la loi de juin 2018 qui met en application le RGPD. D'abord la notion de **consentement** est introduite, c'est-à-dire que les usagers doivent donner leur accord et être informés de l'utilisation de leurs données (article 7). Une mesure spécifique s'adresse aux **mineurs** dans l'article 7-1 «*Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur* ». Ensuite de nouveaux droits sont donnés, comme le **droit à la portabilité** qui rend aux usagers la maîtrise de leurs données Autre exemple, le **champ des données sensibles** a été élargi (article 8) et le **profilage** basé sur l'une d'entre elles est interdit (article 70-9).

[19] Voir les art. 20 s du projet de révision de la LPD à la page 6824 s du document suivant : https://www.admin.ch/opc/fr/federal-gazette/2017/6803.pdf
[20] Ibid.

<table>
<tr><td>Roumanie</td><td>
<table>
<tr><th>Les droits de la personne</th><th>Le cadre juridique roumain avant 2018</th><th>Le RGPD</th></tr>
<tr><td>La transparence des informations, des communications et les modalités d’exercice des droits de la personne</td><td></td><td>✓</td></tr>
<tr><td>Le droit à l’information</td><td>✓</td><td>✓</td></tr>
<tr><td>Le droit d’accès aux données</td><td>✓</td><td>✓</td></tr>
<tr><td>Le droit de modifier les données/ le droit à la rectification</td><td>✓</td><td>✓</td></tr>
<tr><td>Le droit à l’opposition</td><td>✓</td><td>✓</td></tr>
<tr><td>Le droit de ne pas subir une décision individuelle prie en base d’un traitement automatique des données</td><td>✓</td><td>✓</td></tr>
<tr><td>Le droit de saisir la justice</td><td>✓</td><td>✓</td></tr>
<tr><td>Le droit de supprimer les données - le droit à l’oublie</td><td></td><td>✓</td></tr>
<tr><td>Le droit à la restriction du traitement des données</td><td></td><td>✓</td></tr>
<tr><td>Le droit à la portabilité des données</td><td></td><td>✓</td></tr>
</table>
Le RGPD a introduit dans la législation européenne et roumaine des nouvelles mesures, parmi lesquelles on mentionne:

Les entreprises dont les travaux sont principalement axés sur le traitement et la surveillance des données personnelles sont tenus à désigner une personne autorisée à assumer la responsabilité de la protection des données personnelles - il s'agit d'un employé de l’entreprise qui occupe le poste d’officier de la protection des données personnelles (DPO).
Le consentement à la reprise des données personnelles est traité d’une manière plus sérieuse et comprenne un ensemble de règles beaucoup plus rigoureuses. La demande d’accord est présentée sous une forme beaucoup plus accessible, dans un langage plus simple et plus concis et, très important, c’est inacceptable de conditionner le consent.
Les propriétaires des données bénéficient de plusieurs droits, notamment la portabilité - la liberté de transférer des données à caractère personnel d'un opérateur à un autre -, d’une manière sécurisée. En outre, ils peuvent s'opposer à l'utilisation d'informations confidentielles à des fins diverses, telles que le marketing direct, comme suit:

un renvoi abusif de newsletters, sans enregistrement préalable des consommateurs;
un SMS marketing, sans que les utilisateurs n’aient donné le numéro de téléphone à l’opérateur etc.

Apres l'adoption du RPGD, on attend et on constate déjà, un accroissement de la transparence du processus du traitement des données personnelles afin que les utilisateurs puissent être informés qui est le responsable de la protection de leurs informations personnelles et quelle est la période du stockage dans la base de données respective.
Des amendes de dizaines de millions d’euros représentent une nouveauté apportée par le RPGD. On ajoute ici le fait que ceux qui constatent la violation d’un de leurs droits en matière de protection des données personnelles peuvent obtenir compensations importantes en faisant appel aux tribunaux.
</td></tr>
<tr><td>Hongrie</td><td>--</td></tr>
</table>

Catalogne	La LOPDGDD établit certaines mesures supplémentaires à celles prévues par le RGPD, telles que, par exemple, les suivantes: - Réglementer la possibilité de l'exercice de droits des personnes liées à une personne décédée, - Établir l'âge de consentement pour le traitement des données à 14 ans, - Réglementer les systèmes d'information de crédit, - Réglementer les systèmes de ciblage d'exclusion de la publicité, - Réglementer les systèmes d'alerte internes de dénonces pour garantir la confidentialité, - Réglementer les systèmes de vidéosurveillance, - Établir certaines hypothèses pour lesquelles il sera obligatoire de désigner un délégué à la protection des données, - Concrétiser des aspects spécifiques du régime de sanctions, - En ce qui concerne les mesures de sécurité, elle établit que les entités du secteur public doivent se conformer aux mesures de sécurité correspondantes conformément au Schéma National de Sécurité. Et il est également stipulé que le Schéma National de Sécurité devra prendre en compte le risque du traitement des données personnelles conformément à la RGPD.
Sénégal	Pour appuyer les mesures prises par la loi de 2008-12, 1a loi 2016-29 portant révision du Code pénal contient des dispositions visant à protéger les données à caractère personnel et la vie privée. La loi criminalise par exemple l'acte de « conserver sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales ou qui sont relatives à la santé de celui-ci». Elle criminalise également « celui qui au moyen d'un procédé quelconque, porte volontairement atteinte à l'intimité de la vie privée d'autrui en captant, enregistrant, transmettant ou diffusant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ; en fixant, enregistrant, transmettant ou diffusant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. »
Bénin	La création de l'Autorité de protection des données à caractère personnel par la loi n.2017-20 du 16 juin 2017 portant code du numérique en République du Bénin.
Canada	a. *La Loi sur la protection des renseignements personnels* La LPRP prévoit certaines garanties quant aux renseignements personnels, mais ne vise pas particulièrement la protection des renseignements personnels. Par exemple, l'article 7 de la LPRP prévoit que sans le consentement d'un individu, une institution fédérale ne peut se servir de renseignements personnels collectés « qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins » et « qu'aux fins auxquelles ils peuvent lui être communiqués en vertu du paragraphe 8(2) » qui liste les seuls cas autorisés de communication de renseignements personnels. En effet, l'article 8 de la LPRP prévoit que « les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article ». Malgré tout, le Secrétariat du Conseil du Trésor a élaboré certaines politiques et directives qui s'appliquent aux institutions fédérales et qui incluent des mesures visant la protection des renseignements personnels :

- *Directive sur les pratiques relatives à la protection de la vie privée* qui « fournit une orientation aux institutions gouvernementales sur la façon de mettre en œuvre des pratiques efficaces de protection de la vie privée ».
- *Directive sur l'évaluation des facteurs relatifs à la vie privée* qui « fournit une orientation aux institutions gouvernementales sur la façon d'évaluer les incidences sur la vie privée des activités ou des programmes nouveaux ou ayant fait l'objet de modifications importantes qui nécessitent la création, la collecte et le traitement de renseignements personnels ».
- *Lignes directrices sur les atteintes à la vie privée* qui expliquent « aux institutions gouvernementales la façon de gérer les atteintes à la vie privée ».

Veuillez noter que, dans son rapport sur la LPRP, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique fait les recommandations suivantes à l'égard de la protection des renseignements personnels par les institutions fédérales :

RECOMMENDATION 7

Que la *Loi sur la protection des renseignements personnels* soit modifiée afin d'obliger explicitement les institutions à protéger les renseignements personnels en prenant des mesures physiques, organisationnelles et technologiques correspondant au niveau de sensibilité des données.

RECOMMANDATION 8

Que la *Loi sur la protection des renseignements personnels* soit modifiée pour énoncer des conséquences précises au défaut de protéger les renseignements personnels.

De même, dans son mémoire au Comité, le commissaire à la protection de la vie privée du Canada énonce ce qui suit :

> À l'heure actuelle, la *Loi sur la protection des renseignements personnels* n'oblige pas explicitement les institutions fédérales à protéger les renseignements personnels.
>
> Même si la *Loi* ne mentionne pas les mesures de sécurité, la politique du Secrétariat du Conseil du Trésor (SCT) prévoit des exigences visant à protéger les actifs du gouvernement fédéral, y compris les renseignements personnels. À notre avis, le moment est venu de consacrer dans une loi ces protections prévues dans une politique administrative interne.
>
> En exigeant explicitement dans la *Loi sur la protection des renseignements personnels* des mesures de sécurité, on assurerait une meilleure protection des renseignements personnels détenus par le gouvernement. Ces dernières années, d'importantes atteintes à la vie privée se sont produites à l'échelle de la fonction publique fédérale et elles ont touché des centaines de milliers de Canadiens. Les vérifications et enquêtes menées ensuite par le Commissariat ont montré que les mesures de sécurité actuelles sont insuffisantes. Soulignons aussi qu'il est anormal d'imposer par voie législative des mesures de sécurité au secteur privé, mais non aux institutions gouvernementales.
>
> Nous recommandons d'intégrer à la *Loi sur la protection des renseignements personnels* des exigences en matière de mesures de sécurité, afin que les obligations prévues par la loi soient en harmonie avec celles imposées par d'autres lois à l'échelle nationale ou internationale qui obligent les organisations à prendre des mesures physiques, organisationnelles et technologiques correspondant au niveau de sensibilité des données.

b. La *Loi sur la protection des renseignements personnels et les documents électroniques*

Les organisations assujetties à la LPRPDE doivent, entre autres, respecter le septième principe de l'annexe 1 de la *Loi* qui prévoit des mesures de sécurité des renseignements personnels :

> **4.7 Septième principe – Mesures de sécurité**
>
> Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.
>
> **4.7.1**
>
> Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.
>
> **4.7.2**
>
> La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.
>
> **4.7.3**
>
> Les méthodes de protection devraient comprendre :
>
> a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;
>
> b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif;
>
> c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.
>
> **4.7.4**
>
> Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.
>
> **4.7.5**
>
> Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3).

De même, les articles 10.1 (et les articles qui suivent ce dernier) de la LPRPDE prévoient des obligations pour les organisations lorsqu'il y a atteinte aux mesures de sécurité des renseignements personnels. Notamment, une organisation doit déclarer « au commissaire [à la protection de la vie privée] toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu » (article 10.1(1) de la LPRPDE) et doit « aviser l'intéressé de toute atteinte aux mesures de sécurité qui a trait à des renseignements personnels le concernant et dont elle a la gestion, s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à son endroit » à moins qu'une autre règle de droit l'interdise (10.1(3) de la LPRPDE).

Québec	L'article 5 de la *Charte des droits et libertés de la personne du Québec*, RLRQ, c. C-12 porte sur le droit fondamental au respect de la vie privée. **Art. 5** Toute personne a droit au respect de sa vie privée. De plus, la *Loi sur l'accès* prévoit des droits en matière de renseignements qui concernent une personne physique et qui permettent de l'identifier, à savoir : ○ sauf exception, le droit à la confidentialité des renseignements personnels; ○ le droit pour toute personne physique d'avoir accès aux renseignements personnels qui la concernent; ○ le droit pour toute personne physique de faire rectifier des renseignements qui la concernent. Outre les trois points immédiatement ci-dessus, la *Loi sur le secteur privé* traite des aspects qui suivent : ○ le droit pour la personne de faire retrancher d'une liste nominative des renseignements personnels la concernant, en tout temps, au moyen d'une demande verbale ou écrite, auprès de toute personne qui détient ou qui utilise cette liste ; le droit pour la personne de faire supprimer un renseignement personnel qui la concerne si la collecte de celui-ci n'est pas autorisée par la Loi.
4. La loi prévoit-elle des mesures pour encourager **le partage des données** dans un cadre sécurisé ?	
Suisse	Art. 12 LPD : « Quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. 2 Personne n'est en droit notamment de: a. traiter des données personnelles en violation des principes définis aux art. 4, 5, al. 1, et 7, al. 1; b. traiter des données contre la volonté expresse de la personne concernée sans motifs justificatifs; c. communiquer à des tiers des données sensibles ou des profils de la personnalité sans motifs justificatifs. 3 En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement. »[21]
Monaco	La loi n° 1.165 précitée dispose que le transfert d'informations nominatives hors de la Principauté ne peut s'effectuer que sous réserve que le pays ou l'organisme vers lequel s'opère le transfert dispose d'un niveau de protection adéquat. A défaut, le transfert est possible uniquement si la personne à laquelle se rapportent les informations a consenti à leur transfert ou si ce transfert est nécessaire, notamment, à la sauvegarde de la vie de la personne, au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice.

[21] Voir l'article directement dans la Loi : https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html#a12

France	Oui, la loi prévoit des mesures pour encourager le partage des données dans un cadre sécurisé. En effet, l'article 68 prévoit que le transfert de données à caractère personnel ne puissent être transférées vers un Etat qui n'est pas membre de l'Union Européenne uniquement si « *cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.*
Roumanie	En ce qui concerne le transfert des données à caractère personnel vers un pays non membre de l'UE ou vers une autre organisation internationale, ce transfert est possible dans les conditions de la loi, à condition que l'état respectif, le territoire, les divisions administratives - territoriales ou l'organisation internationale respective assure le niveau de protection requis. Le cadre législatif roumain stipule également que pour la réalisation des enquêtes et pour les activités menées à combattre les infractions, les systèmes d'évidence des données à caractère personnel, ou selon le cas, les moyens automatiques de traitement des données à caractère personnel détenues par des opérateurs distincts, peuvent devenir inter-opérationnelles à l'aide du *Registre national des personnes*, du *Registre national des passeports simples*, du *Registre national des permis de conduire et des véhicules immatriculés*.
Hongrie	--
Catalogne	Dans le contexte de la transformation numérique de notre société, la LOPDGDD établit des politiques visant à promouvoir les droits numériques. En particulier, le Gouvernement catalan, en collaboration avec les communautés autonomes, doit élaborer un plan d'accès à Internet avec les objectifs suivants: a) pallier les brèches numériques et garantir l'accès à Internet des collectifs vulnérables ou ayant des besoins particuliers et d'environnements familiaux et sociaux économiquement défavorisés, grâce, entre autres mesures, à un « bon » social permettant d'accéder à Internet; b) promouvoir l'existence d'espaces de connexion d'accès public; et c) favoriser des mesures éducatives qui promeuvent la formation en compétences et habiletés numériques de base des personnes et des collectifs exposés au risque d'exclusion numérique, ainsi que la capacité de tout un chacun à utiliser de manière autonome et responsable Internet et les technologies numériques. De même, un plan d'action doit être approuvé, visant à promouvoir les actions de formation, de diffusion et de sensibilisation nécessaires pour garantir que les mineurs utilisent de manière équilibrée et responsable les appareils numériques ainsi que les réseaux et services de la société de l'information équivalents d'Internet, dans le but de garantir le développement approprié de leur personnalité et de préserver leur dignité et leurs droits fondamentaux. En ce sens, l'APDCAT a créé le "Guide des mineurs sur Internet" pour surfer sur le Web sans problèmes et a également lancé la campagne "Sur Internet, tu contrôles?" destinée aux enfants et aux jeunes, afin que les mineurs fassent attention à leur identité et à la protection de leurs données personnelles à un moment où ils ont un accès très libre aux nouvelles technologies, aussi bien à la maison qu'à l'école. La campagne, développée au travers de différentes actions, est conçue pour faire arriver une série de recommandations et d'habitudes saines face à la technologie, de la manière la plus efficace possible. La campagne cherche également à faire en sorte que les mineurs sachent comment réagir face à des situations de risque possibles et qu'ils puissent exploiter en toute sécurité tout le potentiel offert par le réseau. C'est dans ce but que des ateliers d'appareils mobiles sont conçus

	pour leur donner des directives afin d'utiliser la technologie mobile de manière efficace, sûre et intelligente. En outre, les écoles et les instituts de Catalogne disposent de matériel pédagogique pour aider les mineurs à édifier une culture de protection de leur vie privée sur Internet, afin de permettre une utilisation adéquate des données à caractère personnel et des technologies de l'information, entre les enfants et les jeunes de 9 à 17 ans. Finalement, le Gouvernement catalan doit soumettre chaque année, à la commission parlementaire correspondante du Congrès des Députés de l'Espagne, un rapport dans lequel il doit rendre compte de l'évolution des droits, des garanties et des commandements prévus dans le présent titre et des mesures nécessaires pour promouvoir son impulsion et son efficacité.
Sénégal	Au regard de la loi 2008-12, le consentement préalable des personnes concernées est obligatoire pour le partage des données, mais ne mentionne expressément pas de dispositions visant à encourager le partage de données dans un cadre sécurisé.
Bénin	Oui
Canada	a. *La Loi sur la protection des renseignements personnels* L'article 8(1) de la LPRP prévoit que « les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article ». L'article 8(2) de la LPRP prévoit les divers cas où la communication de renseignements personnels est autorisée. **b. La *Loi sur la protection des renseignements personnels et les documents électroniques*** Sous réserve de certaines exceptions, les organisations doivent se conformer aux obligations énoncées à l'annexe 1 de la LPRPDE (article 5 de la LPRPDE). Certains principes à l'annexe 1 visent la communication de renseignements personnels. Selon le troisième principe, « toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire ». De même, le cinquième principe spécifie que « les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige ».
Québec	Les ministères et organismes gouvernementaux sont assujettis depuis 2008 au *Règlement sur la diffusion* adopté en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* RLRQ, c. A-2.1, r. 2. Ce règlement prévoit la diffusion proactive de « données ouvertes » sur le portail *Données Québec*. Dans son rapport quinquennal de 2016, la Commission d'accès à l'information a recommandé au gouvernement d'adopter des dispositions de même nature qui viseraient les secteurs de l'éducation et de la santé, et les municipalités du Québec.

5. Selon votre loi, à qui incombe **la charge de la preuve** ? Appartient-il au citoyen de démontrer que ses données sont utilisées sans son accord, ou est-ce l'inverse ?	
Suisse	Au citoyen. En effet, le projet de LPD révisée ne prévoit pas de renversement du fardeau de la preuve en faveur de la personne dont les données sont traitées, même si cela a pu être évoqué un temps. Un renversement aurait obligé le responsable du traitement à démontrer qu'il traite les données de manière licite.
Monaco	La loi monégasque prévoit que c'est à la personne auprès de laquelle des informations nominatives ont été recueillies qu'il incombe de prouver que ces informations ont été utilisées sans son accord.
France	Le titre I de l'article 39 de la Loi du 6 janvier 1978 (modifiée par l'article 34 de la loi du 20 juin 2018) dispose que « *Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel* ». Le titre II dispose quant à lui que « *Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées*. » L'article 40 prévoit quant à lui que « *Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.* *Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.* *En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.* »
Hongrie	Selon les règles du GDPR, le responsable de la gestion de données doit certifier qu'il respecte les exigences (article 5, paragraphe 2, du GDPR), de sorte que la charge de la preuve incombe au responsable de la gestion de données dans tous les cas.
Catalogne	Une des nouveautés que présentent le RGPD et la LOPDGDD est l'évolution vers un modèle basé sur le principe de la responsabilité active qui exige une évaluation préalable, de la part du responsable ou de la personne en charge du traitement, du risque que le traitement puisse générer. Par conséquent, c'est le responsable ou la personne en charge du traitement qui doit garantir et doit pouvoir démontrer que le traitement est conforme à la réglementation sur la protection des données et qu'il a adopté les mesures les plus appropriées pour garantir les droits et les libertés des personnes dont il traite les données.

Sénégal	Selon la loi 2008-12, précisément en ses articles 66 et 69, la charge de la preuve incombe au responsable du traitement des données et auprès de qui les demandes sont formulées. L'article 66 traite du droit d'accès aux données et l'article 69 du droit de rectification et de suppression des données et dans tous les deux cas s'il y a contentieux, la charge de la preuve incombe responsable du traitement.
Bénin	La charge de la preuve incombe au citoyen (article 314 de la loi n.2017-20 sus-citée).
Canada	De manière générale, lorsqu'une plainte est déposée en vertu de la LPRP et de la LPRPDE, le commissaire à la protection de la vie privée est chargé d'enquêter et de recueillir l'information pertinente. Lorsqu'une plainte faite au Commissariat à la protection de la vie privée se rend devant la Cour fédérale, la charge de la preuve incombe aux citoyens ou au commissaire à la protection de la vie privée lorsqu'il s'agit de démontrer qu'une obligation prévue à dans la LPRP ou dans la LPRPDE a été violée.
Québec	L'entreprise privée ou l'organisme en cause et non le citoyen doit démontrer que le renseignement demandé est nécessaire.
6. La propriété des données échappe aujourd'hui souvent aux citoyens au profit d'entités privées. Votre pays étudie-t-il les pistes pour que le citoyen ait **un contrôle, une visibilité et une connaissance maximale de l'usage de ses données** et de leur commercialisation éventuelle ? La loi traite-t-elle **la question juridique de la propriété des données**? Une réflexion a -t-elle été faite en ce sens? Quelles sont les conclusions?	
Suisse	Les données à caractère personnel sont des éléments constitutifs de la personne humaine, qui dispose, dès lors, **de droits inaliénables** sur celles-ci. Il n'est pas souhaitable d'envisager une situation qui ne ferait qu'accentuer le déséquilibre existant entre les personnes dont les données sont collectées et les responsables de traitement, et ne permettrait pas aux personnes de créer les conditions d'une relation contractuelle équitable
Monaco	La loi n° 1.165 précitée oblige le responsable du traitement d'informations nominatives à informer les personnes auprès desquelles des informations nominatives ont été recueillies, de la finalité du traitement, de l'identité des destinataires ou des catégories de destinataires de ces informations, ainsi que de leur droit de s'opposer à l'utilisation pour le compte de tiers, ou à la communication à des tiers d'informations nominatives les concernant à des fins de prospection, notamment commerciale. De plus, la loi n° 1.435 susmentionnée impose aux opérateurs et prestataires de services chargés de l'exploitation des réseaux et des services de télécommunications et de communications électroniques, qui souhaitent réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, d'obtenir le consentement exprès de leurs abonnés. Elle précise, en outre, que ce consentement ne peut être donné que pour une durée limitée, laquelle ne peut excéder celle correspondant aux relations contractuelles entre l'usager et l'opérateur ou le prestataire de services.

	La loi monégasque ne raisonne pas en termes de propriété des données, mais rattache au contraire ces dernières à la catégorie des droits extrapatrimoniaux, dans la mesure où elle vise, à travers la protection des données personnelles, à protéger la personne elle-même, ainsi que sa vie privée. En droit monégasque, la personne est par conséquent titulaire de ses informations personnelles, mais n'en est pas juridiquement propriétaire, puisque ces dernières constituent des droits extrapatrimoniaux et non des biens mobiliers incorporels sur lesquels pourrait s'exercer un droit réel.
France	En effet, l'article 1er de la Loi relative à l'informatique, aux fichiers et aux libertés dispose que « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.* ». A ce titre, il existe une autorité nationale de protection de données, la CNIL (Commission Nationale de l'Informatique et des Libertés). Cette dernière accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits. Ainsi, quatre missions principales sont attribuées à la CNIL : **informer/protéger** les particuliers et les professionnels en les sensibilisant à la protection et au traitement des données personnelles, **accompagner/conseiller** les organismes sur les démarches de conformité, **contrôler/sanctionner** le respect de la loi de protection des données et, finalement, **anticiper** les technologies et nouveaux usages pouvant avoir des impacts sur la vie privée.
Hongrie	Ces lois (GDPR, Loi sur l'Info, et Ibtv.) contiennent des règles générales qui doivent être gardées à l'esprit pour tous les processus de gestion de données, et déterminent aussi les orientations pour la législation. Concernant le traitement de données spécifique, les règles détaillées spécifiques sont toujours définies par la loi sectorielle pertinente (qui est le responsable du traitement des données, quelle est la durée de la gestion des données, la portée des données traitées, le but de la gestion des données, quelles sont les conditions de la gestion des données, qui peut connaître les données à caractère personnel traitées). L'adaptation des lois sectorielles au GDPR est en cours, le projet de loi est déjà devant le Parlement dans le document T/4479.
Catalogne	Oui. Le droit à la protection des données personnelles a pour objectif de permettre à chaque personne de contrôler l'utilisation que des tiers font de ses données à caractère personnel. En particulier, le RGPD permet de contrôler qui a des informations sur nous, quelles sont ces informations, d'où elles proviennent, dans quel but ces données sont utilisées et à qui on les facilite. Ainsi, on prétend protéger le droit de garder sous notre contrôle les données à caractère personnel qui nous concernent et qui sont traitées par des tierces personnes, physiques ou juridiques, publiques ou privées, dans des buts bien précis. Quoi qu'il en soit, il convient de rappeler que le droit à la protection des données, comme tout autre droit, n'est pas un droit absolu et que des exceptions au contrôle des données personnelles peuvent être fixées, par exemple lorsque la loi l'établit ainsi.

	Notre réglementation en matière de protection des données règle une série de droits que le citoyen détient pour contrôler ses données, par exemple, le droit de ne pas être soumis à des décisions individuelles automatisées, en incluant ceux sur l'élaboration de profils, droits d'accès, de rectification, de suppression, de limitation du traitement, de la portabilité et d'opposition, en plus du droit à l'information. Finalement, elle réglemente les procédures en cas de violation éventuelle des réglementations sur la protection des données et le régime de sanctions, par conséquent, notre législation essaye de donner au citoyen le contrôle, la visibilité et les plus amples connaissances possibles de l'utilisation de ses données.
Sénégal	---
Bénin	A notre connaissance, l'Assemblée nationale n'est pas impliquée. Seules, les structures gouvernementales peuvent justifier. La question juridique de la propriété des données est abordée dans ladite loi.
Canada	La LPRPDE, qui s'applique aux organisations du secteur privé, ne discute pas spécifiquement de la propriété des données. Malgré tout, au Canada, l'autonomie des individus quant à leurs renseignements personnels est discutée sous plusieurs angles. Ces angles incluent, entre autres, le consentement, la réputation en ligne ainsi que le modèle de surveillance de la loi. a. *Consentement* Le consentement valable est un principe clé de la LPRPDE. Le principe général en ce qui concerne le consentement est le suivant : « Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire[22]. » Il est à noter que la LPRPDE comporte plusieurs exceptions où une organisation pourrait recueillir, utiliser ou communiquer les renseignements personnels d'un individu à son insu et sans son consentement. Par exemple, il pourrait être impossible ou peu réaliste d'obtenir le consentement d'une personne concernée dans certaines situations pour des raisons juridiques ou médicales[23]. Dans les dernières années, la notion de consentement a été remise en question. Effectivement, ce modèle a été « conçu à l'origine dans le contexte de transactions commerciales individuelles[24] ». Depuis la rédaction de la LPRPDE, la « technologie et les modèles d'affaires ont beaucoup évolué[25] ». Ainsi, certains remettent en doute « la faisabilité d'obtenir un consentement valable » au sein d'« un écosystème caractérisé par l'ampleur et la complexité de la circulation de l'information et l'omniprésence de l'informatique[26] ». Le commissaire à la protection de la vie privée explique la problématique de la manière suivante : Reconnu comme la pierre angulaire de la loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada, le consentement est l'outil qui permet aux individus d'affirmer leur autonomie et d'exercer un contrôle sur leurs

22 LPRPDE, annexe 1, « 4.3 Troisième principe – Consentement ».
23 ETHI, *Mémoire du Commissaire à la protection de la vie privée du Canada*, 2 décembre 2016.
24 *Ibid*.
25 *Ibid*.
26 Commissariat à la protection de la vie privée du Canada (CPVP), Groupe des politiques et de la recherche, *Consentement et protection de la vie privée : Document de discussion sur les améliorations possibles au consentement sous le régime de la* Loi sur la protection des renseignements personnels et les documents électroniques, mai 2016.

	renseignements personnels. La loi oblige les organisations qui souhaitent recueillir, utiliser ou communiquer des renseignements personnels à solliciter et à obtenir le consentement des intéressés. Toutefois, les avancées technologiques comme les mégadonnées, l'Internet des objets, l'intelligence artificielle et la robotique posent de sérieux défis pour les parties impliquées dans une transaction. Les organisations soutiennent qu'elles ne sont pas toujours en mesure de déterminer ou prévoir toutes les raisons pour lesquelles les renseignements personnels pourraient être utilisés ou communiqués dans le marché d'aujourd'hui en constante évolution et axé sur les données. Dans ce contexte, les efforts déployés pour expliquer les pratiques de protection de la vie privée prennent généralement la forme de politiques ou ententes sur les conditions d'utilisation formulées dans un jargon juridique, souvent incompréhensibles, qui ne cessent de changer. Il serait injuste de s'attendre à ce que les individus soient en mesure d'exercer un véritable contrôle sur leurs renseignements personnels ou de toujours prendre des décisions éclairées lorsqu'il s'agit de donner leur consentement. Voilà en quoi consiste le dilemme, qui ne peut que devenir plus complexe[27]. En mai 2016, le Commissariat à la protection de la vie privée a publié un document de discussion sur les améliorations possibles au consentement sous le régime de la LPRPDE[28]. Le Commissariat a mené des consultations sur ces enjeux et a publié ses résultats dans son rapport annuel 2016-2017. Dans son rapport, le commissaire indique que, selon lui, « le consentement continue de jouer un rôle important dans la protection du droit à la vie privée, dans les situations où la personne concernée dispose d'information suffisante pour donner un consentement valable[29] ». Il ajoute que : Le consentement demeure au cœur de l'autonomie personnelle, mais il faut ajouter d'autres mécanismes pour l'appuyer et ainsi protéger la vie privée plus efficacement. Notamment, des organismes de réglementation indépendants qui renseignent les citoyens, orientent l'industrie, lui demandent des comptes et sanctionnent les comportements inacceptables. On doit aussi envisager d'autres outils de protection de la vie privée dans des situations exceptionnelles et justifiables où cela est pratiquement impossible d'obtenir le consentement[30]. Dans son rapport de février 2018 sur la LPRPDE, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes de recommande au gouvernement du Canada « que le consentement demeure au cœur du régime de protection des renseignements personnels, mais qu'il soit renforcé et clarifié par des moyens additionnels lorsque possible ou requis[31] ». Il fait aussi les recommandations suivantes :

27 CPVP, *Rapport annuel au Parlement 2016-2017 concernant la* Loi sur la protection des renseignements personnels et les documents électroniques *et la* Loi sur la protection des renseignements personnels, septembre 2017.

28 CPVP, Groupe des politiques et de la recherche, *Consentement et protection de la vie privée : Document de discussion sur les améliorations possibles au consentement sous le régime de la* Loi sur la protection des renseignements personnels et les documents électroniques, mai 2016.

29 CPVP, *Rapport annuel au Parlement 2016-2017 concernant la* Loi sur la protection des renseignements personnels et les documents électroniques *et la* Loi sur la protection des renseignements personnels, septembre 2017.

30 *Ibid*.

31 ETHI, *Vers la protection de la vie privée dès la conception : Examen de la* Loi sur la protection des renseignements personnels et les documents électroniques, douzième rapport, 1re session, 42e législature, février 2018.

RECOMMANDATION 2 sur l'adhésion facultative par défaut :

Que le gouvernement du Canada propose des modifications à la *Loi sur la protection des renseignements personnels et les documents électroniques* afin de prévoir explicitement l'adhésion facultative par défaut en ce qui a trait à toute utilisation des renseignements personnels à des fins secondaires, et la mise en place d'un système d'adhésion facultative par défaut sans égard à l'objectif poursuivi.

RECOMMANDATION 3 sur la transparence algorithmique :

Que le gouvernement du Canada envisage la prise de mesures visant à améliorer la transparence algorithmique.

RECOMMANDATION 4 sur la révocation du consentement :

Que le gouvernement du Canada étudie la question de la révocation du consentement afin de clarifier la forme qu'elle doit prendre ainsi que ses effets juridiques et pratiques.

Bien que dans son rapport annuel 2016-2017, le commissaire donne certaines pistes de solution, le modèle de consentement prévu à la LPRPDE et les améliorations qui doivent y être apportées demeurent un enjeu complexe qui reste à explorer.

b. Réputation en ligne et droit à l'oubli

Au moment actuel, la LPRPDE comporte très peu de dispositions concernant la suppression des renseignements personnels, leur correction ou leur exactitude. Cela dit, avec l'avènement des nouvelles technologies, il devient de plus en plus difficile pour les individus d'exercer un contrôle sur leurs renseignements personnels en ligne. Selon le commissaire à la protection de la vie privée, « une atteinte à la réputation peut prendre de graves proportions lorsque les moteurs de recherche accordent de l'importance à des renseignements personnels qui autrement seraient restés dans l'ombre[32] ». Le commissaire a indiqué au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique que la réputation en ligne, dont le droit à l'oubli, constitue un enjeu à être étudié[33].

La notion du « droit à l'oubli » n'est pas bien définie, mais peut inclure deux notions :

- le « droit au déréférencement », soit le droit à ce que les renseignements répertoriés dans les résultats de recherche par les moteurs de recherche soient retirés. Ce droit correspond à la suppression de la référence à des renseignements personnels, mais non à la suppression totale des données.
- le « droit à l'effacement », soit le droit à la suppression des renseignements qui sont disponibles en ligne. Il s'agit d'un droit reconnu par l'UE en vertu duquel « le responsable du traitement des données serait tenu de supprimer des données[34] » dans certaines circonstances.

Aucune loi fédérale canadienne ne vise spécifiquement le droit à l'oubli. Par conséquent, le Commissariat à la protection de la vie privée du Canada, qui est responsable de surveiller la conformité à la LPRPDE, constitue l'autorité à laquelle les gens s'adressent lorsque leurs renseignements personnels sont disponibles en ligne sans leur consentement. Le Commissariat mène alors une enquête sur la plainte déposée. Néanmoins, il est important de noter que, lorsqu'une atteinte à la réputation ne survient pas dans le cadre

32 *Ibid*.
33 ETHI, *Mémoire du Commissaire à la protection de la vie privée du Canada*, 2 décembre 2016.
34 *Ibid*.

d'une transaction commerciale qui tombe sous le régime de la LPRPDE, les lois provinciales en matière de responsabilité civile et délictuelle entrent en ligne de compte.

En janvier 2016, le Commissariat a publié un document de travail sur la réputation en ligne « pour faire avancer la discussion sur la meilleure façon d'aider les personnes lorsque des renseignements personnels mis en ligne portent atteinte à leur réputation[35] ». Ce document traite notamment du droit à l'oubli. Le Commissariat à la protection de la vie privée a mené des consultations[36] à ce sujet et a publié ses résultats dans un Projet de position[37]. Voici un résumé de cette proposition de position :

> Pour ce qui est de l'effacement à la source, la LPRPDE accorde aux individus le droit de retirer leur consentement et exige que les renseignements personnels dont on n'a plus besoin soient détruits, effacés ou dépersonnalisés. Conjointement, ces deux principes supposent qu'une personne devrait pouvoir effacer les renseignements qu'elle a elle-même affichés en ligne.
>
> Lorsque les renseignements personnels en question ont été affichés par d'autres, l'intéressé n'a pas un droit absolu de les retirer. Néanmoins, tout comme dans le cas du déréférencement, il devrait pouvoir utiliser un mécanisme permettant de contester le caractère exact, à jour et complet des renseignements et, lorsqu'il est établi que la contestation est justifiée, on devrait pouvoir les faire corriger, effacer ou étoffer comme il se doit.
>
> Dans les deux cas de figure susmentionnés, s'il est impossible de régler un problème avec un site Web ou un moteur de recherche, les individus peuvent déposer une plainte officielle auprès du Commissariat.
>
> Dans l'ensemble, le pouvoir de demander le déréférencement de résultats de recherche ou l'effacement de renseignements à la source est, dans certaines situations, similaire au « droit à l'effacement ("droit à l'oubli") » prévu par le *Règlement général sur la protection des données* (RGPD) de l'Union européenne. Toutefois, le rapport ne constitue pas l'adoption au Canada d'un cadre européen. Il s'agit plutôt d'une interprétation des lois canadiennes actuelles et des recours qu'elles prévoient concernant la réputation en ligne.
>
> Il est important de prendre des mesures en ce qui a trait au déréférencement – étant donné qu'il y a un risque d'atteinte à la réputation et que les solutions proposées par le Commissariat sont, à son avis, équilibrées et réalisables. Toutefois, le rapport recommande aussi que le Parlement examine cet enjeu. Les élus devraient confirmer le juste équilibre entre la protection de la vie privée et la liberté d'expression dans notre société démocratique[38].

Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes s'est penché sur le projet de position du Commissariat à la protection de la vie privée et a fait deux recommandations au gouvernement du Canada à ce sujet dans son rapport de février 2018 sur la LPRPDE :

> **RECOMMANDATION 11 sur le droit à l'effacement :**
>
> > **Que le gouvernement du Canada envisage la mise en place, dans la *Loi sur la protection des renseignements personnels et les documents électroniques*, d'un encadrement du droit à l'effacement inspiré du modèle mis en**

35 CPVP, *Réputation en ligne : Que dit-on à mon sujet?*, janvier 2016.
36 CPVP, *Consultation sur la réputation en ligne*.
37 CPVP, *Projet de position du Commissariat sur la réputation en ligne*.
38 *Ibid*.

place dans l'Union européenne qui, au minimum, inclurait un droit des jeunes d'obtenir l'effacement de renseignements qu'ils ont mis en ligne, que ce soit par eux-mêmes ou par le biais d'une organisation.

RECOMMANDATION 12 sur le droit au déréférencement :

Que le gouvernement du Canada envisage la mise en place, dans la *Loi sur la protection des renseignements personnels et les documents électroniques*, d'un encadrement du droit au déréférencement et que ce droit soit explicitement reconnu à l'égard des renseignements personnels mis en ligne par un individu alors qu'il était mineur[39].

c. Modèle de surveillance et les pouvoirs du commissaire à la protection de la vie privée

L'efficacité du modèle de surveillance de l'application des lois en matière de protection des renseignements personnels et les pouvoirs actuels du commissaire à la protection de la vie privée sont des enjeux importants dans la mesure où ceux-ci contribuent à un exercice efficace des droits des citoyens.

Tel que mentionné ci-haut, le commissaire à la protection de la vie privée du Canada veille au respect de la LPRP et de la LPRPDE. Au moment actuel, les pouvoirs du commissaire sont basés sur un modèle d'ombudsman où des enquêtes administratives sont menées. Le commissaire reçoit des plaintes et procède à des enquêtes en vertu de la LPRP et la LPRPDE. Le commissaire tente de régler les plaintes en misant sur la persuasion et la conciliation. La LPRP et la LPRPDE prévoient principalement des pouvoirs d'enquêtes et de recommandations non contraignantes pour le commissaire à la protection de la vie privée. Ainsi, à l'issue des enquêtes, le commissaire peut uniquement formuler des recommandations.

La question du meilleur modèle de surveillance pour la protection des renseignements personnels en est une qui est discutée depuis longtemps. Certains sont d'avis que le modèle d'ombudsman actuellement en place pourrait être plus efficace et préconisent la mise en place d'un modèle exécutoire où le commissaire détiendrait des pouvoirs d'ordonnance[40]. De même, les discussions portent sur les sanctions administratives pécuniaires et l'opportunité de conférer au commissaire de la protection des renseignements personnels un tel pouvoir dans le cadre de l'application de la LPRPDE[41].

Contrairement aux recommandations du commissaire où les organismes visés sont libres de mettre en œuvre ou non les recommandations, en vertu d'un pouvoir d'ordonnance, les ordonnances rendues sont contraignantes. Notamment, le commissaire pourrait alors obliger une organisation à cesser une action ou à poser une action afin de prévenir une infraction à la LPRP ou à la LPRPDE. Si une organisation ne respectait pas l'ordonnance, l'ordonnance pourrait normalement être certifiée par la Cour fédérale. Elle deviendrait alors exécutoire comme le sont les ordonnances de la Cour fédérale et l'organisation visée pourrait potentiellement être trouvée coupable d'outrage à la Cour[42].

Puis, les sanctions administratives pécuniaires (SAP) :

---

39 ETHI, *Vers la protection de la vie privée dès la conception : Examen de la* Loi sur la protection des renseignements personnels et les documents électroniques, douzième rapport, 1re session, 42e législature, février 2018.

40 ETHI, *Protéger la vie privée des Canadiens : Examen de la* Loi sur la protection des renseignements personnels, quatrième rapport, 1re session, 42e législature, décembre 2016. ETHI, *Vers la protection de la vie privée dès la conception : Examen de la* Loi sur la protection des renseignements personnels et les documents électroniques, douzième rapport, 1re session, 42e législature, février 2018.

41 *Ibid*.

42 CPVP, Arguments en faveur de la réforme de la *Loi sur la protection des renseignements personnels et les documents électroniques*, mai 2013.

	sont des sanctions civiles ou des amendes qui peuvent être imposées dans les cas de non-conformité à la loi. Une SAP n'est pas de nature punitive. Elle a surtout pour but de favoriser la conformité ou, inversement, de prévenir la non-conformité, grâce à un incitatif monétaire. Plus qu'un simple « prix à payer pour faire des affaires », les SAP représentent un moyen rapide et efficace d'amener les organisations à se conformer à la loi. Les SAP sont imposées par l'organisme qui applique la loi, plutôt que par les tribunaux. Si elles ne sont pas payées, elles deviennent des créances de la Couronne qui peuvent être recouvrées au moyen d'une poursuite civile. La décision d'imposer une SAP, comme toute autre décision d'un organe administratif, pourrait faire l'objet d'un contrôle judiciaire[43]. Le commissaire a recommandé la mise en place d'un modèle exécutoire où il détiendrait des pouvoirs d'ordonnance pour l'application de la LPRP[44]. Dans son rapport de décembre 2016 intitulé *Protéger la vie privée des Canadiens : Examen de la* Loi sur la protection des renseignements personnels, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes a recommandé « que le gouvernement du Canada renforce la surveillance du droit d'accès en adoptant un modèle exécutoire dont les paramètres sont clairement et rigoureusement définis[45] ». En ce qui concerne la LPRPDE, l'ancienne commissaire à la protection de la vie privée, Jennifer Stoddart, a recommandé en 2013 de « renforcer l'application de la *Loi* et encourager une plus grande conformité à celle-ci[46] ». Dans son mémoire, la commissaire Stoddart avait exposé plusieurs options, dont celles des pouvoirs d'ordonnance et des SAP. Le commissaire actuel, Daniel Therrien, a poursuivi les discussions entourant le meilleur modèle de surveillance pour la LPRPDE. Il a mené des consultations sur le consentement valable pendant lesquelles son organisation a abordé le renforcement des pouvoirs du commissaire. Dans son rapport annuel 2016-2017 au Parlement, le commissaire Therrien recommande au gouvernement du Canada de « conférer au commissaire le pouvoir de rendre des ordonnances et la possibilité d'imposer des sanctions administratives pécuniaires[47] ». Dans son rapport de février 2018 intitulé *Vers la protection de la vie privée dès la conception : Examen de la* Loi sur la protection des renseignements personnels et les documents électroniques (rapport de février 2018 sur la LPRPDE), le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes a fait une recommandation similaire, soit « d'accorder au commissaire à la protection de la vie privée des pouvoirs d'exécution, incluant le pouvoir de rendre des ordonnances et le pouvoir d'imposer des amendes en cas de non-respect de ces ordonnances[48] ».
Québec	En 2015, la Commission d'accès à l'information du Québec a formulé les recommandations qui suivent (recommandations auxquelles le gouvernement a souscrit) :

43 *Ibid*.

44 CPVP, Lettre présentée au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique au sujet d'une étude de la *Loi sur la protection des renseignements personnels*, « Étude de la *Loi sur la protection des renseignements personnels* », *Conseils au Parlement*, 13 septembre 2016.

45 ETHI, *Protéger la vie privée des Canadiens : Examen de la* Loi sur la protection des renseignements personnels, quatrième rapport, 1re session, 42e législature, décembre 2016.

46 CPVP, *Arguments en faveur de la réforme de la* Loi sur la protection des renseignements personnels et les documents électroniques, mai 2013; *Schrems c. Data Protection Commissioner*, C-362/14, 6 octobre 2015.

47 CPVP, *Rapport annuel au Parlement 2016-2017 concernant la* Loi sur la protection des renseignements personnels et les documents électroniques *et la* Loi sur la protection des renseignements personnels, septembre 2017.

48 ETHI, *Vers la protection de la vie privée dès la conception : Examen de la* Loi sur la protection des renseignements personnels et les documents électroniques, douzième rapport, 1re session, 42e législature, février 2018.

	- Obliger les organismes publics et les entreprises à adopter des politiques de confidentialité simplifiées qui présentent, en termes clairs et compréhensibles, une vue d'ensemble de leurs engagements sur la protection des renseignements personnels. - Imposer aux organismes publics et aux entreprises l'utilisation de pictogrammes de protection pour informer le public de leurs engagements. En 2016, la Commission a également recommandé au gouvernement de modifier l'article 8 de la *Loi sur le secteur privé* pour que des renseignements plus complets y figurent. - Le moment où l'information doit être donnée à la personne concernée (selon que l'information est recueillie auprès d'elle ou d'un tiers et à son insu ou non). - Une obligation d'informer la personne des renseignements personnels qui seront collectés et des moyens par lesquels ils seront colligés. - Une mention sur l'obligation de clarté, d'intelligibilité et d'accessibilité de l'information, quel que soit le support utilisé pour recueillir les renseignements personnels. Les lois mentionnées ici ne traitent pas de la notion de propriété des données personnelles.
6.1 Selon votre loi, qui est propriétaire des données personnelles?	
Suisse	La LPD permet aux individus d'exercer pleinement les droits inaliénables attachés à leurs données personnelles, en leur garantissant un haut niveau de maîtrise sur celles-ci. A ce titre, nous souhaitons attirer votre attention **sur la résolution de l'Association francophone des autorités de protection des données personnelles (AFAPDP) adoptée le 18 octobre 2018** (texte en annexe).
France	Il n'existe pas de loi relative à la propriété des données personnelles. Le texte du RGPD autorise la collecte de n'importe quelle donnée dès lors qu'elle est utile pour un système (hormis, comme le dispose l'article 8, les « *données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique*. »)
Hongrie	Article VI de la Loi Fondamentale 3) Toute personne a droit à la protection des données à caractère personnel et à la connaissance et à la diffusion des données d'intérêt public. (4) Le respect du droit à la protection des données à caractère personnel et à la connaissance des données d'intérêt public est soumis au contrôle d'une autorité indépendante établie par une loi pivot.

	La Cour constitutionnelle interprète le droit à la protection des données à caractère personnel comme un droit de la défense non traditionnel, mais aussi compte tenu de son côté actif, comme un droit à l'autodétermination de l'information. [15/1991. (IV. 13.) Décision de la Cour de justice] En conséquence, en règle générale, tout le monde a droit à ses propres données personnelles, conformément à l'ordre constitutionnel, ce droit peut être limité par la loi en Hongrie, en tenant compte du principe de l'objectif lié.
Catalogne	La Constitution espagnole et la doctrine constitutionnelle considèrent le droit au respect de la vie privée comme un droit personnel, tel que le reconnaît le RGPD. Cela signifie que la personne concernée doit avoir le contrôle de ses données. Selon le RGPD, les données à caractère personnel traitées par des entités, entreprises ou autres collectivités afin de mener à terme leurs fonctions ne leur appartiennent pas, elles appartiennent aux personnes avec lesquelles elles interagissent. Ce sont elles les vraies *propriétaires* de leurs informations personnelles. Par conséquent, les données personnelles n'appartiennent pas à celui qui les gère, mais bel et bien aux personnes titulaires des données.
Québec	Sans objet
7. La loi offre-t-elle aux citoyens les garanties légales à l'exercice effectif de leurs droits, notamment en leur permettant de contrôler l'usage qui est fait de leurs données personnelles?	
Suisse	Le projet de révision de la LPD prévoit : • Le devoir d'informer lors de la collecte : le devoir d'information couvre à présent toute collecte de données. • Le devoir d'informer en cas de décision automatisée • Un droit d'accès • Le droit de demander de faire valoir son point de vue lors de décision automatisée et d'exiger que la décision soit revue par une personne physique • Le droit de demander rectification, effacement ou destruction des données • Le droit d'opposition au traitement (opposition à communication dans secteur public) • Le droit d'ester en justice (gratuité de la procédure civile) • Le droit de dénoncer une violation de la loi au Préposé.
Monaco	La loi n° 1.165 précitée permet aux personnes physiques, dont les données personnelles ont été collectées, de contrôler l'usage qui en est fait, dans la mesure où elle prévoit qu'elles peuvent s'adresser au responsable du traitement afin d'accéder à leurs données et, le cas échéant, de s'opposer à leur collecte ou d'obtenir qu'elles soient rectifiées. Elle ne prévoit en revanche pas la portabilité des données à l'instar du Règlement européen n° 2016/679, dit Règlement Général sur la Protection des Données (RGPD).

France	Oui, la loi offre aux citoyens des garanties légales pour contrôler l'usage qui est fait de leurs données personnelles. Ils ont aussi la possibilité de les modifier, les compléter ou les effacer (droit à l'oubli) comme le dispose l'article 40.
Belgique	**Dérogations aux droits de la personne concernée** Le RGPD confère de très nombreux droits à la personne dont les données à caractère personnel sont traitées (« *la personne concernée* »). Notamment, **le droit à l'information, le droit de consultation, le droit de rectification des données inexactes, le droit d'opposition, le droit à l'oubli, le droit à la limitation du traitement, le droit à la portabilité des données et le droit d'être informé des violations de la sécurité.** Le législateur belge énumère un certain nombre de cas strictement définis dans lesquels il peut être dérogé à ces droits. **Ces droits ne sont pas d'application**, notamment, lorsque le responsable du traitement dispose de données à caractère personnel qui proviennent directement ou indirectement des autorités judiciaires, des services de police, de l'inspection générale de la police fédérale ou de la police locale, de la Cellule de Traitement des Informations financières (CTIF), de l'Administration générale des douanes et accises et de l'Unité d'information des passagers (UIP). Ces droits ne s'appliquent pas davantage aux traitements de données à caractère personnel par l'UIP elle-même. Ils ne s'appliquent toujours pas lorsque le responsable du traitement dispose de données à caractère personnel émanant directement ou indirectement des services de renseignement et de sécurité, de l'OCAM ou de l'Autorité de sécurité nationale, entre autres.(art. 11 et ss). **Partage des données** Lorsque **la police fédérale** communique des données à d'autres autorités ou à des organismes privés, elle formalise cette transmission, pour chaque type de traitement, par **un protocole** entre le responsable du traitement initial et le responsable du traitement destinataire des données. Le protocole peut mentionner, notamment, les finalités pour lesquelles les données à caractère personnel sont transférées, les catégories de données à caractère personnel transférées, la base légale et la périodicité du transfert et les sanctions applicables en cas de non-respect du protocole. **Propriété des données** Le Règlement européen n'autoriserait pas le législateur national à prendre des dispositions spécifiques en la matière. Dès lors, la législation belge ne consacre pas le droit de la propriété des données. Ce concept n'a d'ailleurs pas de statut légal en Belgique. Par contre, il existe différents mécanismes de protection des données, dont le RGPD. Actuellement, la propriété relative aux données ne peut porter que sur la création intellectuelle (droit d'auteur, marque, brevet, …).
Roumanie	Comme déjà mentionné, le RGPD fait partie du cadre juridique roumain. En conséquence : Les personnes physiques/juridiques qui utilisent les données à caractère personnel sont tenues d'informer d'avance le propriétaire des données sur ce fait. Le propriétaire des données à caractère personnel peut donner son consentement pour le traitement des données; peut retraire son consentement; a le droit de s'opposer à l'utilisation des données; a accès à ses données et peut les rectifier/transférer/supprimer; a le droit de demander aux personnes physiques/ juridiques respectives de cesser leur utilisation ou, selon le cas, de les rendre anonymes.

	Si les données à caractère personnel sont volées, sont perdues ou font l'objet d'une **violation**, la personne/la structure traitant les données à caractère personnel doit informer **l'Autorité nationale de contrôle du traitement des données à caractère personnel** (l'ANCTDCP) et, également, le propriétaire des données à caractère personnel, si cette violation entraîne un risque grave en ce qui concerne les données personnelles ou la vie privée. Si une personne considère que ses droits en matière de protection des données n'ont pas été respectés, elle peut déposer une plainte directement auprès l'ANCTDCP qui examinera la plainte et répondra dans le délai prévu par la loi. La personne qui se considère lésée dans ses droits peut aussi choisir de poursuivre directement en justice l'entreprise ou organisation concernée sans passer préalablement par l'ANCTDCP. L'instance peut décider même d'accorder le droit à une compensation financière au cas de préjudice matériel ou moral (une souffrance psychologique).
Hongrie	Les articles 12-14 du GDPR exigent des informations sur la gestion des données des personnes concernées. L'article 15 du GDPR régit le droit d'accès de la personne concernée, c'est-à-dire à recevoir des informations sur demande au sujet de ses informations personnelles gérées, la source des données, le but du traitement des données, sa base juridique, sa durée, les circonstances d'un incident de protection des données qui peut avoir eu lieu, ses effets et les mesures prises pour le combattre, et, en cas de transfert de données, sa base légale et son destinataire.
Catalogne	Oui, notre loi reconnaît les mêmes droits reconnus par le RGPD (droit d'accès, de rectification, de suppression, de limitation de traitement, de portabilité et d'opposition) et ils peuvent être exercés directement ou par l'intermédiaire d'un représentant légal ou d'un bénévole. Le responsable du traitement est tenu d'informer la personne affectée des moyens dont il dispose pour exercer les droits qui lui correspondent. Les moyens doivent être facilement accessibles à la partie concernée. Il revient au responsable du traitement de prouver que l'obligation de répondre à la demande que la partie concernée fait au sujet de l'exercice de ses droits a été remplie. Les titulaires de l'autorité parentale peuvent exercer, au nom des mineurs, les droits d'accès, de rectification, d'annulation, d'opposition ou tout autre qui pourrait leur correspondre en termes de protection des données. Les actions effectuées par le responsable du traitement pour répondre aux demandes d'exercice de ces droits sont gratuites, sous réserve des dispositions des articles 12.5 et 15.3 du Règlement (UE) 2016/679 et des paragraphes 3 et 4 de l'article 13 de ladite loi organique.
Sénégal	Lors d'un séminaire d'actualisation du cadre institutionnel et normatif, tenu, en mai 2018, par la Commission de Protection des Données personnelles (CDP), il a été recommandé que la CDP s'adapte au contexte international, marqué une législation plus contraignante à l'international dont le dernier en date est l'entrée en vigueur le 25 Mai prochain du Règlement Général sur la Protection des Données Personnelles (RGPDP).
Bénin	Effectivement cette garantie est offerte par la loi.

Canada	a. *Loi sur la protection des renseignements personnels* La LPRP prévoit des obligations juridiques incombant aux institutions fédérales assujetties à la *Loi* relativement à la collecte, la protection, l'utilisation et la conservation des renseignements personnels. Tel que mentionné ci-haut, les individus peuvent déposer une plainte auprès du Commissariat à la protection de la vie privée du Canada lorsque certaines obligations prévues dans la *Loi* ont été violés (art. 29 de la LPRP), lequel fera une enquête. Par exemple, l'article 7a) de la LPRP indique qu'à « défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci : a) qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins ». En ce qui a trait à la portabilité des données, la LPRP ne prévoit pas ce principe. **b. *Loi sur la protection des renseignements personnels et les documents électroniques*** L'article 5 de la LPRPDE exige que les organismes assujettis à la *Loi* se conforme aux principes énoncés dans son annexe 1. L'annexe 1 inclut de nombreux principes liés à la collecte, la protection, l'utilisation et la conservation des renseignements personnels visant la protection du droit à la vie privée des individus. Tout individu peut déposer auprès du Commissariat à la protection de la vie privée du Canada une plainte visant le non-respect des principes énoncés à l'annexe. En ce qui concerne le contrôle de l'usage des données, deux principes semblent s'y rapprocher : - le cinquième principe de la LPRPDE énoncé à l'annexe 1 prévoit ce qui suit : Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées. - le deuxième principe exige ce qui suit : « Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci. » Veuillez noter que la portabilité des données n'est pas explicitement visée par la LPRPDE. Dans son rapport sur la LPRPDE, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique recommande « Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'y prévoir un droit à la portabilité des données ».
Québec	Le droit à la portabilité des données n'existe pas, tant au Québec qu'au Canada.
7.1 Le Règlement européen n° 2016/679, dit Règlement Général sur la Protection des Données (GDPR) par exemple prévoit la **portabilité des données**. Est-ce le cas chez vous?	
Suisse	L'instauration d'un droit à la portabilité des données n'est actuellement pas prévue.
France	La loi française prévoit aussi la portabilité des données, comme le veut le Règlement Général sur la Protection des Données.

Hongrie	La Hongrie étant membre de l'Union européenne, elle est donc tenue d'appliquer directement sa réglementation (sans la transposer dans le droit interne) (y compris le GDPR), en conséquence le droit à la portabilité des données [Article 20 du GDPR] est également applicable.
8. Des **pistes non explorées** à ce jour vous apparaissent-elles importantes à explorer ? Et si oui, lesquelles ?	
Suisse	---
Belgique	Vu la date à laquelle il a été négocié, le Règlement européen ne semble pas avoir exploré de nombreuses pistes telles « *l'intelligence artificielle* ». Au demeurant, il importe de souligner les mécanismes mis en œuvre par le Règlement et visant aux transferts de données hors UE (art. 44 et ss Du Règlement). Il est vraisemblable que des corrections devront avoir lieu. Toutefois, à ce jour, vu la date d'entrée en vigueur du Règlement européen et de la loi, il nous est difficile de les cibler.
Hongrie	--
Catalogne	Cela pourrait être intéressant d'essayer de s'attaquer aux transferts internationaux de données d'un point de vue plus souple et plus approprié à un contexte dans lequel les données circulent en permanence au-delà des frontières. Le système de protection actuel est lourd et confus, peu agile et mène à l'incertitude juridique. On pourrait y faire face, par exemple, avec une distinction entre les pays qui offrent des garanties adéquates et ceux qui ne le font pas. Au cas où des garanties suffisantes ne seraient pas offertes (avec une évaluation préalable de la Commission, en ce qui concerne l'Union européenne), il serait nécessaire de faire basculer la protection du droit sur les responsabilités que l'exportateur des données devrait assumer, puisqu'il devrait, en définitive, se faire responsable du traitement ultérieur des informations du destinataire ou des destinataires successifs de l'information.
Canada	La Bibliothèque du Parlement n'est pas en mesure de répondre à cette question en raison de son mandat d'objectivité et d'impartialité. Veuillez noter que les deux rapports du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes mentionnés ici-haut analysent des possibles réformes au régime canadien de protection de la vie privée. D'ailleurs, la partie 5 du rapport concernant la LPRPDE traite de l'incidence de l'adoption du RGDP. Le Comité fait d'ailleurs les recommandations suivantes : **RECOMMANDATION 17 sur les critères d'adéquation entre la *Loi sur la protection des renseignements personnels et les documents électroniques* et le Règlement général sur la protection des données :** **Que le gouvernement du Canada collabore avec les autorités de l'Union européenne afin de déterminer quels seraient les critères requis pour que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit considérée comme adéquate au regard du Règlement général sur la protection des données.**

	RECOMMANDATION 18 sur les modifications législatives requises pour conserver le caractère adéquat : **Que le gouvernement du Canada identifie quelles seraient les modifications à apporter à la *Loi sur la protection des renseignements personnels et les documents électroniques*, s'il y a lieu, afin qu'elle conserve son caractère adéquat au regard du Règlement général sur la protection des données;** **Que, dans l'éventualité où il serait déterminé que les modifications requises pour conserver le caractère adéquat ne sont pas dans l'intérêt du Canada, le gouvernement du Canada crée des mécanismes permettant un échange de données sans heurts entre le Canada et l'Union européenne[49].**
Québec	Le Directeur général des élections du Québec (DGE) a recommandé que l'utilisation de données personnelles par les partis politiques au Québec soit encadrée par la loi. Récemment, le DGE a reçu l'appui de la présidente de la Commission d'accès à l'information à ce sujet. Un document interne de la Commission indique que la masse de données sur les électeurs détenues par les partis politiques met en cause le caractère confidentiel et le secret du vote[50]. En juin 2018, un projet de loi (nº 188) a été déposé à l'Assemblée nationale à ce propos. Toutefois, ce projet de loi est devenu caduc en raison de la dissolution de la Chambre et de la tenue d'élections.
8.1 *Pour les pays non-européens :* **Le GDPR est-il un modèle de référence?** Une source d'inspiration?	
Suisse	La Suisse est actuellement au bénéficie d'une décision d'adéquation de la Commission européenne qui établit que la Suisse, par l'intermédiaire de sa législation interne ou de ses engagements internationaux, offre un niveau de protection des données à caractère personnel comparable à celui garanti dans l'Union européenne. Cette dernière a été rendu sous la directive 95/46/CE[51]. Les décisions d'adéquations sont à présent prévues par le RGPD et la Commission européenne prévoit de publier une nouvelle décision concernant la Suisse fin mai 2020. L'adéquation n'exige pas que le système de protection des données du pays soit identique à celui de l'UE mais repose sur la norme de l'équivalence essentielle. L'un des objectifs de la LPD révisée est donc de se rapprocher du règlement (UE) 2016/679[52]. Ces travaux sont indispensables pour que l'UE continue de reconnaître la Suisse comme un Etat tiers ayant un niveau de protection des données suffisant pour que la possibilité d'échanger des données avec elle soit préservée.
Monaco	Compte tenu de la situation géographique de la Principauté, les transferts transfrontaliers de données personnelles depuis ou destination de l'Union européenne sont très fréquents. Aussi, bien que Monaco ne soit pas un Etat membre de l'Union européenne, elle devrait s'inspirer des dispositions du RGPD dans le cadre de la prochaine réforme de la loi relative à la protection des informations nominatives. En effet, pour que les échanges de données personnelles à destination ou en provenance de l'Union européenne puissent avoir lieu selon une procédure simplifiée, il convient que la législation monégasque offre aux données

[49] ETHI, *Vers la protection de la vie privée dès la conception : Examen de la* Loi sur la protection des renseignements personnels et les documents électroniques, douzième rapport, 1re session, 42e législature, février 2018.
[50] Martin Croteau, « La confidentialité du vote est menacée », *La Presse+*, 27 février 2019, p. A15.
[51] Lien vers la directive 95/46 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR
[52] Lien vers le règlement 2016/679 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

	personnelles un niveau de protection adéquat, c'est-à-dire, concrètement équivalent à celui offert par le droit de l'Union européenne. C'est la raison pour laquelle le Gouvernement a informé le Conseil National qu'un projet de loi inspiré des dispositions du Règlement Général sur la Protection des Données et de celles de Protocole d'amendement à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 révisée) serait prochainement déposé sur le bureau de l'Assemblée. Le Conseil National a anticipé l'intégration prochaine de dispositions équivalentes à celles du RGPD, notamment en s'assurant que les personnes dont les données personnelles sont recueillies, à savoir les fonctionnaires de l'Assemblée, ainsi que les élus et leurs assistants, ont effectivement consenti à ce qu'elles le soient et en renforçant la sécurité et la confidentialité des traitements de données personnelles qu'il met en œuvre.
Sénégal	LE RGDP peut être une source d'inspiration. Pour la mise en œuvre du traitement des données personnelles, l'Assemblée nationale collabore avec la Commission de Protection des Données personnelles - Autorité administrative indépendante – en s'y faisant représenter par un député.
Bénin	Rien à signaler. Car ledit règlement est inconnu dans le droit positif béninois.
Québec	Le Règlement est une source d'inspiration pour la réforme de nos lois.
8.2 *Pour les pays européens :* **Le GDPR donne-t-il satisfaction?** Des corrections sont-elles envisagées?	
France	La CNIL a publié le 23 novembre 2018 un bilan six mois après l'entrée en application du RGPD. Le constat est positif. Elle estime que 66% des Français (selon un sondage IFOP) se disent plus sensibles qu'avant à la protection des données et la Commission reçoit toujours plus de plaintes. Les débats autour du RGPD et son application en France ont renforcé la sensibilisation des Français sur les questions de sécurité informatique et de protection de données. La CNIL note une forte augmentation des visites sur son site (4,4 millions en 2017 et 7 millions en 2018) ainsi qu'une appropriation du Règlement par les professionnels : actuellement 15 000 délégués à la protection des données contre 5 000 correspondants informatique et libertés avant la mise en application du Règlement. Concernant les particuliers, la CNIL a reçu, en 2018, 34% de plaintes en plus qu'en 2017 et les autorités de protection européennes traitent en coopération 345 plaintes transfrontalières. A ce titre, entre mai et novembre 2018, quatre plénières du Comité européen à la protection des données (CEPD) ont eu lieu. Le RGPD a donc sensibilisé les populations européennes et permis une coopération de traitement des plaintes entre les Etats membres. Des corrections sont cependant envisagées puisqu'une ordonnance devrait améliorer la lisibilité du cadre juridique national. A propos de la lisibilité du RGPD, la CNIL prévoit aussi de mettre en place un plan d'accompagnement des collectivités locales en 2019 (sous forme de guide pratique, fiches thématiques) ainsi que la conception d'un MOOC (*Massive Open Online Course*) en ce début d'année, pour se familiariser avec les principes fondamentaux du RGPD.

Roumanie	Nous n'envisageons pas, à court terme, à procéder à des corrections du cadre législatif nationale sur les données personnelles.
Hongrie	Le GDPR est à appliquer directement et obligatoirement en Hongrie, le droit interne exige actuellement une correction, dans le sens qu'ils ne doivent pas entrer en conflit avec le GDPR, cela a été servi par la récente modification de la loi sur l'information, ainsi que par le projet de loi actuel T/4479.
Catalogne	Il donne satisfaction puisqu'avec son application l'on prétend que le niveau de protection des droits et des libertés des personnes physiques, à l'égard du traitement des données personnelles, soit équivalent dans tous les États membres. Par conséquent, il garantit que l'application des règles relatives au traitement des données à caractère personnel soit cohérente et homogène. Étant donné que seul neuf mois se sont écoulés depuis la pleine applicabilité du Règlement général sur la protection des données (RGPD), il est peut-être un peu tôt pour en faire un bilan, mais il est nécessaire d'expliquer de manière plus claire et plus compréhensible les droits des personnes afin de permettre aux personnes de les exercer efficacement; il faut réussir à ce que les responsables du traitement agissent en vertu du principe d'*accountability* (responsabilité proactive) et qu'ils assument l'analyse des risques et la gestion des risques comme une partie essentielle du traitement .
8.3 Comment votre Parlement l'a-t-il mis en œuvre le GDPR pour le traitement des données des parlementaires, des fonctionnaires et collaborateurs parlementaires ? *(responsables de traitement, relations avec les autorités nationales de protection des données personnelles, etc.)*	
France	**<u>A l'Assemblée nationale :</u>** <u>Moyens humains</u> Un délégué à la protection des données (DPO) interne a été nommé à l'Assemblée nationale en avril 2018. Il s'agit de l'ancien « correspondant informatique et libertés », fonction proche du DPO créée par la modification de 2004 de loi française du 6 janvier 1978. Cette fonction est cumulée avec celle de responsable de la sécurité du système d'information. De plus, une juriste spécialisée dans le droit des systèmes d'information a été recrutée comme adjointe au DPO. <u>Principales actions effectuées</u> Sur les dix-huit derniers mois, voici les grandes actions réalisées pour mettre les traitements de l'Assemblée en conformité : - cartographie des traitements de données à caractère personnel ; - élaboration d'un registre détaillé des traitements (fondement légal du traitement, données collectées, durée de conservation, éventuels destinataires, etc.) ; - analyse des écarts avec la règlementation ; - élaboration de plans d'actions pour la mise en conformité ; - intégration des principes fondamentaux (minimisation des données, transparence vis-à-vis des personnes concernées, maîtrise des données, etc.) le plus en amont possible dans les nouveaux projets.

	Droits des personnes concernées Les demandes d'exercices de droits des personnes concernées sont pour le moment peu nombreuses. Une seule demande de droit d'accès a été adressée à l'Assemblée (demande adressée directement au DPO). Le processus interne pour la gestion du droit d'accès n'est actuellement pas formalisé. Mesures de sécurité Les mesures de sécurité nécessaires à la maîtrise et à la protection des données à caractère personnel sont intégrées avec les autres mesures de sécurité. Elles sont identifiées dans une démarche commune (analyse de risques et analyse d'impact sur la vie privée). Cas des députés Le périmètre du DPO de l'Assemblée nationale ne comprend pas les traitements directement opérés par les députés (blogs, sites Internet, newsletters, etc.). Pour autant, les parlementaires ont eu de nombreuses questions concernant le RGPD et ses conséquences lors de son entrée en application en mai 2018. Des fiches de synthèse ont été élaborées à leur intention. De plus, des formations à destination des groupes politiques ont été organisées afin qu'ils puissent servir de relais et de soutien aux députés sur ces sujets. Informations publiées sur les sites web interne et externe de l'Assemblée : Les dispositifs techniques qui sont mis en place par le service des systèmes d'information (à savoir les annuaires, la messagerie électronique, l'agenda, l'accès au WIFI, etc.) font l'objet d'un traitement automatisé à des fins de diagnostic et de sécurité. Elles sont conservées pendant un an et peuvent être destinées à des prestataires techniques, éventuellement situés hors UE. Les données qui sont relatives à l'identité sont gardées un an après le départ de l'Assemblée : les fonctionnaires et collaborateurs parlementaires y ont un droit d'accès, d'opposition, de rectification et d'effacement des données inexactes. Pour toute question, vous pouvez contacter le DPO à l'adresse suivante : dpo@assemblee-nationale.fr **Au Sénat :** Un Correspondant informatique et libertés (CIL), préfigurant l'actuel délégué à la protection des données (DPD) a été désigné dès 2007. Le CIL était chargé de veiller à la conformité des traitements de données à caractère personnel (DCP) mis en œuvre par le Sénat au regard de la Loi « Informatique et Libertés », en particulier en tenant un registre des traitements, mais aussi en s'assurant de la bonne prise en compte des droits des personnes concernées par ces traitements, en cas de demande d'accès, de rectification ou de suppression. Le DPD, désigné à la mise en application du RGPD, a le même objectif vis à vis du règlement européen tout en prenant en compte les nouvelles prérogatives offertes par celui-ci aux personnes concernées (notamment le droit à la portabilité). La division déléguée à l'Association pour la gestion des assistants de Sénateurs (A.G.A.S.) qui gère pour les sénateurs les traitements concernant leurs collaborateurs a également désigné un DPD dans le même but.
Roumanie	Le Sénat/La Chambre de députes appliquent la législation en domaine en ce qui concerne le traitement des données personnelles - désignation d'une personne responsable avec le traitement des données, sollicitation de l'accord explicite du propriétaire - parlementaire ou fonctionnaire -, pour le traitement de ses données personnelles etc.

	Les deux Chambres ont fait des investissements en l'optimisation de la sécurité des leurs réseaux d'ordinateurs et de l'accès aux systèmes Intranet et l'Internet du Sénat/de la Chambre des députes etc.
Hongrie	Le projet de loi T/4479 est en cours d'élaboration, qui contient des amendements à un certain nombre de lois sectorielles, y compris les règles régissant le traitement des données à caractère personnel des membres du Parlement. [Projet de loi T/4479, Chapitre 54, Article 104]
Catalogne	Le Parlement est soumis aux obligations découlant du RGPD et de la LOPDGDD et, à cet égard, il a nommé un Délégué à la Protection des Données Personnelles et a créé un Comité de Sécurité de l'Information et de Protection des Données Personnelles afin de veiller à son application. Ce Comité est formé par le Secrétaire général du Parlement, qui en détient la présidence, et par plusieurs chefs de département de l'administration parlementaire.
Suisse	---

8.1.