Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Rapport d'évaluation

2021

Mathieu MICHEL
Secrétaire d'État à la Protection de la vie privée

PRÉFACE

Dès le début de mon mandat de Secrétaire d'État à la Protection de la vie privée, j'ai souligné l'importance de la confiance des citoyens dans le traitement de leurs données à caractère personnel dans le plein respect des réglementations européennes et nationales. Car, en effet, le développement et l'application des nouvelles technologies et la transformation digitale de notre société reposent largement sur le traitement des données.

Par ailleurs, les mesures que nous avons dû prendre dans le cadre de la lutte contre la pandémie et le traitement des données à caractère personnel impliquées ont une fois de plus démontré l'importance d'un cadre réglementaire solide et clair permettant des flux de données transparents et le développement d'applications numériques respectueuses de la vie privée.

La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel prescrit une évaluation de la loi qui doit être réalisée en 2021. Je ne peux, bien sûr, pas évaluer la Loi vie privée sans m'intéresser à la manière dont elle est appliquée par les acteurs de terrain, à savoir les responsables du traitement, les sous-traitants, les délégués à la protection des données, mais aussi les citoyens, la société civile, les syndicats, les organisations professionnelles et bien d'autres qui sont chargés, au quotidien, de traiter les données et d'appliquer les droits et obligations de la Loi vie privée.

Cependant, étant donné les défis auxquels nous sommes confrontés aujourd'hui pour renforcer la confiance des citoyens dans le traitement de leurs données, je ne me suis pas limité à évaluer la lettre de la Loi vie privée. La société numérique évolue rapidement. J'ai donc voulu nourrir l'examen d'une réflexion plus large sur la relation entre la vie privée, l'innovation et la transformation digitale.

L'évaluation a donné lieu à ce rapport contenant des recommandations que je présenterai à la Chambre des représentants. Avec ces recommandations en main, je dispose d'un large éventail d'orientations pour compléter et renforcer encore le cadre réglementaire de la protection des données, pour organiser les flux de données de manière plus transparente et pour adapter le paysage institutionnel des autorités de contrôle.

Je tiens à remercier toutes les personnes qui ont contribué à cette évaluation. La Loi vie privée est incontestablement un cadre réglementaire essentiel pour la transformation digitale à laquelle aspire ce gouvernement. La confiance dans le traitement de nos données à caractère personnel doit être au cœur de cette démarche.

Mathieu MICHEL

Secrétaire d'État à la Protection de la vie privée

1. INTRODUCTION

La Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (ci-après « Loi vie privée ») prescrit une évaluation de la loi qui doit donc être réalisée en 2021.

Cette évaluation a lieu trois ans après l'entrée en vigueur du Règlement général sur la protection des données[1] (ci-après « le RGPD ») et la transposition de la directive européenne relative au traitement des données à caractère personnel par les services chargés du contrôle de son application (ci-après « la Directive »).[2] Enfin, la Loi vie privée a également créé un cadre juridique pour le traitement des données à caractère personnel par les services publics qui ne relèvent pas de la compétence de l'Union européenne, à savoir les services de renseignement.

Au niveau belge, ce cadre juridique complet pour la protection des données à caractère personnel a donc été choisi à l'époque pour éviter que l'application et la transposition de la législation européenne ne soient fragmentées. Cela fait de l'examen de la Loi vie privée un exercice très complet touchant un large éventail de parties prenantes. Car, en effet, les données sont à la fois le moteur et l'huile de la modernisation numérique d'aujourd'hui. Qu'il s'agisse d'organiser des services efficients et accessibles par nos autorités administratives ou de développer les dernières applications technologiques dans toutes sortes de domaines de notre société, les données à caractère personnel des citoyens sont au cœur de tout cela.

Le bouleversement qui a eu lieu en 2018, notamment avec le RGPD, a provoqué une certaine agitation. Elle a soulevé de nombreuses questions sur l'application concrète de ces nouvelles normes de protection de la vie privée et sur les conséquences possibles en cas de non-respect. Après tout, l'Union européenne a placé la barre haut en matière de protection de nos données à caractère personnel, et chacun doit pouvoir s'élever au-dessus. Aujourd'hui, plus de trois ans après son entrée en vigueur, nous constatons que cela n'est toujours pas évident, tant pour ceux qui doivent se conformer aux obligations que pour les autorités de contrôle qui doivent les surveiller.

Avec l'évaluation de la Loi vie privée, le législateur a donné au niveau politique la possibilité de réagir rapidement. Tout d'abord, l'impact de la nouvelle législation peut être mesuré. L'adaptation aux nouvelles normes a exigé un effort sérieux de la part de toutes les parties concernées. Ce rapport d'évaluation peut servir de point de départ pour ajuster la politique. Par conséquent, lorsque cela est jugé nécessaire et dans la mesure où le droit européen applicable le permet, l'évaluation donnera lieu aux ajustements juridiques et aux mesures politiques nécessaires.

En outre, cette évaluation est également l'occasion d'une réflexion plus large et d'un débat de fond sur l'importance qu'il convient d'accorder à la vie privée dans notre société. Comment la protection de la vie privée s'articule-t-elle avec les autres droits fondamentaux et comment concilier l'innovation et la

[1] 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, PB L 119 du 4 mai 2016, p. 1-88.

[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119, 4 mai 2016, p. 89-131.

transformation digitale avec une protection robuste de nos données à caractère personnel ? La protection des données à caractère personnel est incontestablement au cœur de cette révision. Cependant, on oublie souvent que le RGPD cherche également à promouvoir la libre circulation des données, comme en témoignent, par exemple, le droit à la portabilité des données à caractère personnel ou les principes régissant le transfert des données à des fins de traitement compatible ou ultérieur.

Outre la Loi vie privée, cette évaluation aborde donc inévitablement la législation et les mesures connexes qui sont à la base d'une véritable politique de gestion des données. Les conclusions et recommandations de ce rapport constituent donc un plan possible pour faciliter la circulation des données à caractère personnel au sein du secteur public, entre ses différents niveaux et entre les secteurs public et privé.

Enfin, une évaluation du droit substantiel de la vie privée est inextricablement liée au paysage institutionnel de la vie privée. D'une part, plusieurs institutions jouent un rôle dans la facilitation du flux de données. D'autre part, en 2018, le législateur belge a également choisi de nommer quatre autorités de contrôle au niveau fédéral. En outre, il faut également tenir compte des autorités de contrôle liées aux différentes entités fédérées et des intégrateurs de services. Cela rend le paysage institutionnel de la protection de la vie privée très complexe, ce qui ne facilite pas nécessairement la circulation des données ou le contrôle du respect de la législation. Cette dimension fait donc également l'objet d'une attention particulière tout au long de cette évaluation et peut donner lieu à un ajustement du paysage institutionnel.

2. MÉTHODOLOGIE UTILISÉE POUR L'ÉVALUATION DE LA LOI VIE PRIVÉE

L'évaluation de la Loi vie privée s'est déroulée entre février et septembre 2021 et a été menée dans le cadre d'une vaste consultation et d'un dialogue avec les parties prenantes intéressées et concernées.

En termes d'organisation, un comité d'accompagnement composé de quatre experts universitaires en matière de protection de la vie privée a été mis en place pour orienter l'exercice dans la bonne direction:

- Paul DE HERT (VUB)
- Willem DEBEUCKELAERE (UGent)
- David RESTREPO AMARILES (ULB)
- Jean-Marc VAN GYSEGHEM (Unamur)

Ce comité d'accompagnement a été nommé avec pour mandat de conseiller sur le processus et la méthodologie d'évaluation, de participer aux auditions des parties prenantes et d'analyser les contributions des parties prenantes consultées. Il est important de souligner que le rapport d'évaluation n'est pas un rapport scientifique avalisé et adopté par les membres du comité d'accompagnement. Ceux-ci, ainsi que le Service Protection des données du SPF Justice et la Direction générale de la Transformation Digitale du SPF BOSA, ont endossé un rôle de soutien dans le cadre de la rédaction du rapport.

En termes de contenu, étant donné l'impact transversal d'un cadre réglementaire tel que celui sur la protection des données à caractère personnel, l'objectif a été de donner au plus grand nombre possible de parties prenantes l'opportunité de partager leurs opinions, expériences et points de vue. L'évaluation

a suscité un grand intérêt et a résulté en plus de quarante contributions d'autorités, d'entreprises, d'associations professionnelles, du monde académique, d'organisations et de citoyens.

Une **consultation à grande échelle** a été organisée autour de trois questions centrales :

- quelles sont les forces et les faiblesses de l'actuelle Loi vie privée ?
- comment accroître la confiance et la transparence dans l'utilisation des données à caractère personnel ?
- comment encourager l'innovation fondée sur la collecte de données tout en la conciliant avec la nécessité d'un cadre réglementaire solide, capable d'assurer la sécurité juridique » ?

Le 17 juin, un **webinaire** intitulé « La Loi vie privée répond-elle aux besoins de notre société ? », a eu lieu auquel ont participé 390 personnes. Parallèlement, le webinaire a également été l'occasion de lancer une vaste **consultation publique en ligne**. Dans le prolongement du webinaire et de la consultation publique, trois **sessions thématiques** ont également été organisées :

Session A : Les outils d'application de la Loi vie privée

- Codes de conduite/Certification/Bonnes pratiques/Sandboxes/Privacy ruling
- Analyses d'impact relatives à la protection des données (DPIA)
- Privacy by design/Privacy by default
- Partage des données/réutilisation de données à caractère personnel

Session B : Communication & sensibilisation

- Informations et accompagnement
- Transparence : registre de traitement des données, publication DPIA, publication des décisions des autorités de contrôle au Moniteur belge
- Droits des personnes concernées : droit à l'oubli, portabilité des données, identification des problèmes dans l'exercice des droits.
- Rôle du délégué à la protection des données

Session C : traitement des données à des fins de recherche scientifique ou historique, d'archivage ou de statistiques

- Anonymisation et pseudonymisation des données à caractère personnel
- Mesures de sécurité
- Traitement de données à caractère personnel sensibles
- La diffusion/réutilisation de données à caractère personnel ou de résultats de recherche
- Accès à des données à caractère personnel
- Exercice des droits des personnes concernées

Un examen de la Loi vie privée ne peut pas non plus se faire sans l'œil critique des **autorités de contrôle** mandatées par le législateur pour superviser et guider sa mise en œuvre et sanctionner son non-respect. L'application du RGPD et de la Loi vie privée depuis 2018 fournit des indications importantes sur ces autorités de contrôle et, en particulier, sur leur propre fonctionnement et leurs relations mutuelles. Un dialogue a donc eu lieu avec chacune des autorités de contrôle pour leur donner l'occasion de présenter

leurs observations et recommandations.

Enfin, le rapport d'évaluation fournit dans la section 3 un compte rendu factuel de toutes les contributions faites soit sur demande, soit spontanément. Le contenu de la partie 3 ne reflète donc en aucun cas une quelconque position du gouvernement. Cette dernière a été réservée à la quatrième partie qui résume un certain nombre de conclusions, de recommandations et de suggestions pour la suite des travaux sur la base des contributions des parties prenantes.

3. L'ÉVALUATION DE LA LOI VIE PRIVÉE PAR TOUTES LES PARTIES PRENANTES PARTICIPANTES

3.1. Le cadre juridique du traitement des données et la sécurité juridique

Le choix d'une loi-cadre sur la protection de la vie privée. Au niveau belge, un cadre juridique complet pour la protection des données à caractère personnel a été choisi en 2018. Cette approche est toujours applaudie, mais la Loi vie privée a également perdu en clarté et en lisibilité en raison des ponts qu'il a fallu construire entre différents régimes de protection. D'autre part, il existe également un grand nombre de législations sectorielles qui contiennent des dispositions spécifiques sur la protection des données à caractère personnel mais qui n'ont pas été mises à jour depuis l'entrée en vigueur du RGPD.

En outre, on observe une fragmentation du paysage institutionnel, tant par la multitude des autorités de contrôle et des entités intermédiaires qui donnent accès aux données à caractère personnel que par la dispersion du cadre juridique organique de ces autorités et entités. En d'autres termes, une rationalisation et une harmonisation de la législation, tant au niveau du droit matériel que des autorités et entités compétentes s'impose.

La transparence et la responsabilité sont des principes au cœur de la législation sur la protection des données, qui devraient également être reflétés dans la réglementation applicable. Une Loi vie privée doit être rédigée dans un langage accessible, compréhensible et clair afin que chacun, non seulement les spécialistes mais surtout les citoyens, puisse comprendre les possibilités et les limites de ce qui peut être fait avec leurs données à caractère personnel.

Responsabilité et sensibilisation. La sensibilisation à la protection des données a considérablement augmenté depuis l'arrivée du RGPD et de la Loi vie privée. Les administrations traitent les données et les aspects de la vie privée qui y sont associés de manière plus réfléchie. La nouvelle législation a aussi encouragé les organisations privées à introduire des mesures de sécurité adéquates. Les sanctions imposées entre-temps par l'Autorité de protection des données pour diverses infractions à la loi ont également contribué à responsabiliser davantage les responsables du traitement. Par ailleurs, la prise de conscience des consommateurs qui optent de plus en plus pour des applications et des entreprises respectueuses de la vie privée fait que les organisations privées s'engagent de plus en plus dans la protection de la vie privée et y voient un avantage concurrentiel.

D'autre part, il est également souligné que les obligations ne concernent pas uniquement les responsables du traitement. Le citoyen joue également un rôle important dans la protection de ses

propres données à caractère personnel. Être informé et conscient de ses propres données contribue également à une société dans laquelle la vie privée de chacun et par chacun est respectée et promue de manière positive.

« La vie privée est devenue un enjeu sociétal. Elle relève de la responsabilité sociétale. Tout citoyen a le droit d'accéder à la digitalisation sans que les données qu'ils donnent en échange d'un service ou produit soient compromises. La pandémie nous a propulsé dans une nouvelle dimension en l'espace de quelques mois. La plupart des citoyens n'y sont tout simplement pas préparés et ne sont certes pas conscients des risques liés à la digitalisation. A mon niveau, j'essaie d'intégrer le respect de la vie privée dans la responsabilité sociétale, le rapport annuel et la stratégie de l'entreprise. » (un délégué à la protection des données)

Les lacunes de l'actuelle Loi vie privée. Plusieurs autorités ont indiqué qu'il était nécessaire de clarifier certains concepts ou terminologies tels que « une donnée à caractère personnel », « l'exercice de tâches judiciaires », « le transfert de données à caractère personnel », « les données relatives à la santé », « les services de la société de l'information », « la recherche scientifique », « l'anonymisation », le concept d'« autorité publique » ou la notion de « responsable du traitement ». Certaines de ces dispositions sont insuffisamment ou trop vaguement définies, tandis que d'autres ne le sont pas. Dans tous les cas, cela donne lieu à des interprétations et donc à des applications différentes ou divergentes. En particulier, la qualification des organisations sans but lucratif en tant qu'autorité parce que leurs activités sont principalement financées par des autorités ou des institutions publiques ou que leur gestion est soumise au contrôle de ces autorités ou institutions (cf. article 5, 3° de la Loi vie privée) est remise en question par le secteur sans but lucratif. En effet, cette qualification entraîne des obligations administratives et financières qui sont souvent difficiles à supporter pour les asbl. Par exemple, la nomination d'un délégué à la protection des données est une charge supplémentaire qui serait difficile à justifier pour les petites organisations aux ressources limitées. Par analogie avec la législation luxembourgeoise, on pourrait appliquer un critère selon lequel les associations qui n'effectuent qu'un traitement de données accessoire ne sont pas soumises à l'obligation de désigner un délégué à la protection des données.

Le champ d'application de certains articles de la Loi vie privée pourrait également être clarifié, par exemple les règles spécifiques prévues au chapitre IV du titre 1 pour le secteur public. Il est également nécessaire de clarifier l'interprétation de certaines obligations imposées par la Loi vie privée, par exemple les garanties dans le traitement des catégories spéciales de données en vertu des articles 9 et 10 de la Loi vie privée.

Elle souligne également la nécessité d'un cadre juridique plus clair pour les échanges internationaux de données, par exemple pour l'utilisation des services de cloud. La coopération tant réglementaire que pratique entre les régulateurs nationaux et internationaux devrait être renforcée, par exemple en élaborant un cadre juridique concret sur l'assistance mutuelle. La question se pose également de savoir si l'information et la compréhension des développements concernant les transferts internationaux de données sont suffisantes. Cet aspect est considéré comme l'un des principaux obstacles réglementaires à l'innovation. La jurisprudence Schrems II de la Cour de justice de l'Union européenne à Luxembourg a des répercussions considérables sur les transferts internationaux de données et sur la manière dont les entreprises doivent les traiter. Cela entraîne des retards et des difficultés dans la négociation des contrats. Les PME, plus particulièrement, ne disposent pas des ressources et des connaissances nécessaires pour répondre aux exigences strictes de la Cour de Justice européenne.

La Loi vie privée devrait également clarifier les ponts entre les différentes parties de la loi. Comme indiqué précédemment, il s'agit d'un cadre juridique complet qui définit les régimes de protection des données de multiples types d'autorités et d'opérations de traitement des données. Cela reflète, entre autres, l'existence d'une distinction au niveau européen entre le RGPD et la Directive, d'une part, et entre le droit de l'Union européenne et les régimes de protection des données qui ne trouvent pas leur origine dans le droit européen, d'autre part. Il est toutefois nécessaire de clarifier les limites entre les différents régimes de protection des données afin de pouvoir déterminer le responsable du traitement des données, les obligations y afférentes et le fondement juridique correcte pour le traitement des données.

À cet égard, la question se pose de savoir dans quelle mesure une révision de la liste des autorités qui tombent dans le champ d'application du titre 2 de la Loi vie privée, conformément à l'article 26, 7° est nécessaire. Faut-il ajouter certaines autorités telles que le système pénitentiaire ou suffit-il de clarifier la ligne de démarcation entre les régimes de protection des données ? Les services de police ou le casier judiciaire, par exemple, sont demandeurs à ce dernier niveau. En effet, ils sont confrontés à la possibilité d'une application ou d'une interprétation incorrecte de la réglementation, ce qui a des conséquences importantes pour l'exercice des droits des personnes concernées.

Il est également suggéré de prévoir une meilleure division selon un champ d'application général, d'une part, et les régimes spéciaux de protection des données, d'autre part. Certains services publics sont en charge d'opérations de traitement de données qui peuvent relever de plusieurs régimes de protection de la vie privée, notamment les autorités du secteur de la sécurité. En plus du RGPD, les titres 2 ou 3 de la Loi vie privée et des lois spéciales sont souvent applicables. Cela rend l'application correcte du cadre juridique complexe et difficile à expliquer aux citoyens. Il en va de même pour l'obligation de conclure des protocoles dans le cadre des échanges de données (cf. article 20 de la Loi vie privée). L'application de cette obligation manque de clarté lorsqu'il s'agit de traitements de données qui relèvent de plusieurs régimes de protection de la vie privée.

Il est également suggéré d'organiser un débat sur les obligations de conservation des données à caractère personnel, tant en ce qui concerne la définition territoriale de l'obligation de conservation (régionale, nationale, européenne) que les spécifications techniques et les normes de conservation (par exemple, centralisée ou décentralisée). En outre, il y a également un manque de clarté concernant les périodes de conservation à appliquer. Souvent, les délais sont vagues ou non définis ou ils sont dispersés dans différentes réglementations. En outre, certaines périodes de conservation imposées par la loi ne sont pas conformes à d'autres dispositions légales applicables. C'est le cas, par exemple, dans le secteur financier. Les responsables du traitement bénéficieraient d'un inventaire, d'une rationalisation et d'une centralisation des périodes de conservation. D'autre part, l'importance de conserver les données au-delà de la période de conservation est également soulignée, par exemple pour la recherche historique.

Enfin, les situations de crise telles que les pandémies ou les catastrophes naturelles peuvent mettre à l'épreuve la sauvegarde de nos droits et libertés fondamentaux, tels que le droit à la vie privée et la protection de nos données à caractère personnel. Il est donc préconisé de créer un cadre juridique clair pour le traitement des données à caractère personnel en situation de crise. Cela devrait non seulement apporter une plus grande sécurité juridique en ce qui concerne la sauvegarde de nos droits et libertés fondamentaux. Les services publics chargés de gérer les situations de crise doivent également être en mesure de mener à bien leurs missions juridiques de manière pragmatique. Un cadre juridique clair doit permettre de trouver un juste équilibre entre les différents intérêts. Par ailleurs, il est préconisé de ne

pas interpréter et appliquer la réglementation applicable de manière trop rigide. Elle met en évidence l'équilibre entre les droits fondamentaux, où le droit à la vie privée et à la protection des données doit être mis en balance avec d'autres droits fondamentaux. Par exemple, l'approche de l'Autorité de protection des données face à ces situations de crise n'est pas universellement appréciée.

Des motifs juridiques clairs pour le traitement des données. Il est nécessaire de disposer d'un fondement juridique clair et approprié pour le traitement des données au niveau local, régional ou sectoriel. On constate que les normes générales fournissent un fondement juridique, mais qu'elles ne sont pas suffisamment claires en ce qui concerne la protection de la vie privée, les flux de données et la sécurité de l'information (par exemple, dans le cadre de la coopération intercommunale, des partenariats public-privé, de l'échange de données avec la police locale, etc.).

Des précisions sont également demandées sur les traitements fondés sur l'intérêt général ou vital. Il s'agit de motifs juridiques légitimes, mais fondés sur des concepts qui laissent souvent place à une interprétation large ou vague. Il est donc difficile de délimiter les frontières de ces motifs juridiques, ce qui peut conduire à des situations contraires à d'autres principes de traitement des données, tels que la finalité du traitement. Après tout, un fondement juridique général ou vague peut conduire à une interprétation (trop) large de la finalité réelle du traitement. La ligne de démarcation entre ce qui est un traitement initial et un traitement ultérieur des données à caractère personnel peut donc être mise à mal.

C'est notamment étroitement lié, par exemple, à la problématique de la notion d'« autorité publique », qui peut avoir de nombreuses implications non seulement pour le fondement juridique du traitement des données à caractère personnel, mais aussi pour le régime applicable à ce traitement (comme l'exclusion des amendes administratives). Le monde académique demande également au législateur d'expliciter que l'intérêt public est une base légale sur laquelle les universités et les établissements d'enseignement supérieur peuvent mener des recherches scientifiques.

Un meilleur alignement avec et entre les dispositions légales sectorielles en matière de protection de la vie privée. La demande d'un cadre juridique plus clair en matière de protection des données dans la législation sectorielle (par exemple, la législation sur les caméras, les décrets de gouvernance, la législation sur les pandémies, etc.) et d'une clarification des bases juridiques sur lesquelles elle peut être invoquée est revenue à plusieurs reprises. En outre, l'impact de certaines législations sectorielles sur le traitement des données à caractère personnel par des organisations privées et, en particulier, l'obligation pour les responsables du traitement de fournir une assistance à des fins de sécurité ou de criminalité, crée des charges administratives supplémentaires et une insécurité juridique.

Par ailleurs, il est également souligné que l'existence d'une variété d'instruments réglementaires dans certains secteurs qui ne sont pas harmonisés entre eux et qui peuvent donc freiner le traitement des données à caractère personnel pour des applications innovantes. En outre, la Loi vie privée elle-même pourrait être mieux adaptée aux besoins de certains groupes professionnels, par exemple le secteur des assurances, les avocats ou les fiduciaires.

Il est nécessaire de renforcer la cohérence juridique entre des réglementations contradictoires, laissant les responsables du traitement dans l'incertitude quant aux données qui peuvent être traitées et à celles qui doivent l'être légalement, par exemple dans les secteurs de l'assurance et de la finance.

Une meilleure coordination avec d'autres types de législation. La relation avec les autres législations n'est pas toujours claire. Par exemple, il est difficile pour les services publics de trouver un équilibre entre les obligations de publicité administrative ou de réutilisation des données et les obligations de protection des données. Pour les professions juridiques également, la législation sur la protection de la vie privée est parfois en contradiction avec les obligations de secret professionnel. Par exemple, il convient de préciser que la présence d'un représentant du bâtonnier est requise lors d'une inspection sur place par une autorité de contrôle. Il en va de même dans le secteur de la santé, où une clarification de la Loi vie privée concernant la relation avec le secret médical est préconisée. L'évolution des autorités vers l'utilisation de canaux et de plateformes numériques pour partager de plus en plus de données de santé des prestataires et des institutions de soins de santé à des tiers qui doivent démontrer une relation thérapeutique avec le patient soulève des questions pour certains concernant la responsabilité du fournisseur de données. La numérisation de la société et en particulier des services (publics) pose de nouveaux défis au secret professionnel. La manière dont les règles de protection de la vie privée sont interprétées en relation avec et par les détenteurs de secret professionnel nécessite une analyse et un débat plus approfondis. Par exemple, la question se pose de savoir si nous sommes plutôt susceptibles d'évoluer vers un modèle de responsabilité partagée des données.

Remplir les obligations légales du RGPD. On constate que le législateur belge a fait un usage assez limité des clauses ouvertes du RGPD, c'est-à-dire des dispositions du RGPD qui permettent aux États membres d'introduire des règles supplémentaires. Selon certains, la Belgique pourrait aller plus loin à cet égard, par exemple dans le domaine des ressources humaines ou du traitement des données sensibles (les « catégories spéciales de données à caractère personnel » au sens du RGPD). Il est souligné que les fondements juridiques du traitement de certaines catégories de données à caractère personnel spéciales sont inadéquats pour certains secteurs. En particulier, le traitement des données de santé et judiciaires par des entreprises privées (par exemple, le secteur des assurances) nécessite une extension du cadre légal. En outre, le non-respect des principes de protection de la vie privée dans un contexte de droit du travail entraînerait une insécurité juridique. Cela complique le dialogue social sur la vie privée. On plaide également pour un meilleur encadrement du rôle des syndicats en tant que responsables du traitement dans l'utilisation des listes électorales lors des élections sociales. De manière générale, avec l'adoption de la Loi vie privée, la Belgique a manqué l'occasion de disposer d'un cadre clair pour le traitement des données à caractère personnel dans le cadre de la relation de travail.

La Belgique n'a pas non plus fourni de cadre juridique spécifique pour le traitement des données biométriques. Néanmoins, on ne peut nier l'importance croissante de cette catégorie de données. La nécessité d'une réglementation supplémentaire est également pointée du doigt dans les domaines des relations de travail, de l'utilisation des cookies, du marketing direct et du traitement des big data et de l'intelligence artificielle.

Selon d'autres, l'harmonisation des normes européennes doit être assurée. L'application des clauses ouvertes réduit l'avantage d'un environnement réglementaire unifié et complique l'application de la législation sur la protection de la vie privée. C'est par exemple le cas du seuil de consentement des mineurs, qui est fixé en Belgique à 13 ans (cf. article 7 de la Loi vie privée). Les interprétations et les applications différentes du cadre réglementaire dans les États membres de l'UE entravent le travail des entreprises dans leur coopération internationale.

3.2. Cohérence dans le fonctionnement et l'application du cadre de protection des données

Une approche pragmatique. L'application de la législation sur la protection de la vie privée est perçue comme une lourde charge administrative, en particulier par les petites et moyennes entreprises. Certains secteurs soutiennent donc qu'une réforme de la Loi vie privée devrait garder à l'esprit les obligations administratives et éviter d'imposer des charges supplémentaires dans la mesure du possible. Dans le même ordre d'idées, la nécessité d'une plus grande souplesse et d'un plus grand pragmatisme dans l'application des règles de protection de la vie privée est également soulignée. Dans le contexte du traitement des données à caractère personnel par le monde universitaire, par exemple, il est suggéré que le régime d'exception qui s'applique aux publications universitaires en vertu de l'article 24 de la Loi vie privée devrait être étendu et séparé de la publication effective des résultats de la recherche.

L'un des facteurs contribuant à l'existence de charges administratives supplémentaires et à l'insécurité juridique est l'absence d'une approche nationale globale de la protection des données. L'exemple de devoir conclure plusieurs protocoles ou accords pour pouvoir échanger des données entre différents niveaux ou services est cité à titre d'exemple. Le manque d'harmonisation entre les différents niveaux politiques complique et retarde l'échange de données et affaiblit la protection des droits des citoyens. Une mesure concrète qui pourrait répondre à cette préoccupation est la conclusion d'un accord de coopération entre l'État fédéral, les Communautés et les Régions.

Responsable du traitement et sous-traitant Le RGPD et la Loi vie privée attribuent des capacités différentes à ceux qui traitent les données à caractère personnel. En premier lieu, une distinction est faite entre le responsable du traitement et le sous-traitant. Chaque qualité entraîne des obligations spécifiques. Toutefois, les critères d'identification du responsable du traitement, notamment dans le cas du traitement de données complexes et impliquant la fourniture, le traitement ou la transmission de données par plusieurs entités, sont considérés comme peu clairs. C'est particulièrement le cas pour le secteur public. Par exemple, il n'existe pas de lignes directrices centrales sur la désignation légale du responsable du traitement pour le traitement des données par les services publics. Dans certains cas, un ministre est désigné, dans d'autres cas, le chef d'un service public et dans d'autres encore, un département d'un service public. En général, cela conduit non seulement à une application incohérente des principes juridiques de la vie privée, notamment du principe de responsabilité. Il arrive aussi souvent que la désignation juridique du responsable du traitement ne corresponde pas à la situation réelle de l'entité qui détermine les finalités et les moyens du traitement des données, ce qui est le facteur décisif pour déterminer qui doit être désigné comme responsable du traitement.

En outre, le rôle du sous-traitant et la relation avec le responsable du traitement méritent également une plus grande attention. En effet, certains sous-traitants peuvent être qualifiés de responsables du traitement en raison de leur position dominante. Les autorités de contrôle nationales et européennes devraient fournir davantage de précisions et d'orientations sur ces interrelations.

Divergences entre les autorités de contrôle. L'existence de différents régimes de protection des données en fonction du type d'autorité et de traitement des données entraîne également la répartition

des pouvoirs de contrôle entre plusieurs autorités de contrôle. Cependant, l'ambiguïté susmentionnée qui existe parfois dans la démarcation entre les régimes de protection des données affecte également les actions de ces autorités de contrôle. En d'autres termes, l'absence d'un cadre juridique cohérent et clair signifie que leurs avis, recommandations et lignes directrices peuvent également être différents ou diverger les uns des autres. Cela place à la fois les sous-traitants de données à caractère personnel et les citoyens dans des situations parfois peu claires. Une application cohérente et correcte de la législation exige donc que les risques d'interprétations différentes de la législation sur la protection de la vie privée soient minimisés.

Disponibilité des autorités de contrôle. Même si les autorités de contrôle sont parfois dépeintes comme celles qui tiennent le bâton et imposent des mesures draconiennes, elles jouent également un rôle d'accompagnement des organisations qui traitent les données à caractère personnel. C'est particulièrement vrai pour l'Autorité de protection des données qui dispose en effet d'un solide arsenal de mesures correctives et de sanctions dans le cadre du RGPD. En 2017, en créant l'Autorité de protection des données, le législateur belge a également souligné l'importance d'un rôle de soutien et de conseil envers les sous-traitants de données. Cela suppose une accessibilité et une disponibilité facile de l'Autorité de contrôle d'une part, mais aussi une action d'accompagnement proactive d'autre part ce qui est une condition fondamentale pour une application cohérente et correcte de la Loi vie privée au nom de toutes les personnes concernées. La mesure dans laquelle les autorités de contrôle, et en particulier l'Autorité de protection des données, se conformeront à ces attentes dépendra de plusieurs facteurs qui seront examinés en détail dans le présent rapport.

3.3. Transparence et confiance dans l'utilisation des données à caractère personnel

La Loi vie privée : une histoire racoleuse. Bien que les données soient omniprésentes dans notre vie quotidienne et qu'il ne se passe pas un jour sans que les risques et les opportunités des processus d'automatisation et de numérisation soient soulignés, en premier lieu il a été signalé que la Loi vie privée pourrait manquer de clarté quant à sa propre raison d'être. Les données à caractère personnel sont au cœur de la transformation digitale de notre société et donc de notre existence individuelle et de notre interaction en tant que collectivité. Les nouvelles technologies à l'origine de ces évolutions fulgurantes sont alimentées par nos données à caractère personnel. Il est donc suggéré d'organiser un débat sur l'importance des données et de leur protection, ainsi que sur la direction que nous souhaitons donner à ces évolutions sociales. Une Loi vie privée devrait avant tout avoir pour principe que les nouvelles technologies axées sur les données doivent servir l'humanité et ne doivent en aucun cas nuire aux personnes et à une société harmonieuse.

Une meilleure compréhension de la loi applicable. Des déclarations de confidentialité facilement accessibles et compréhensibles reflètent le besoin de transparence, de prévisibilité et de clarté quant à la manière dont les données à caractère personnel sont collectées, traitées et transférées. Dans ce domaine aussi, de nombreuses améliorations peuvent être accomplies. La complexité de l'évolution technologique, qu'elle soit législative ou technique, nécessite une vulgarisation des services et outils qui nous accompagnent dans notre quotidien privé et professionnel.

Diverses mesures peuvent être élaborées à cette fin. Par exemple, il est proposé que la Loi vie privée mentionne explicitement l'obligation pour les services publics de mettre une déclaration de confidentialité à la disposition du citoyen. Dans une optique d'exemplarité des autorités, la Loi vie privée pourrait fournir un cadre minimal pour ces avis de confidentialité, avec une exception pour certains services spécifiques énumérés aux titres 2 et 3. Un rapport annuel sur la protection de la vie privée pourrait également faire partie de ce cadre juridique. Plus généralement, les autorités publiques devraient regrouper toutes les informations sur la législation sur la protection de la vie privée d'une manière simple et les rendre accessibles via un site web. Dans le secteur de la santé, il est recommandé que tous les sites web et portails consacrés à la santé comportent une déclaration de confidentialité claire, simple et complète. En dehors du secteur public, toutes les organisations tireraient également un bénéfice d'un meilleur accompagnement au niveau du contenu des déclarations de confidentialité.

« Il est à noter que la raison d'être de la protection des données n'est pas inscrit très clairement dans la loi-cadre et qu'il serait bon de rappeler que les nouvelles technologies doivent être au service de l'humanité et ne doit en aucun cas nuire. C'est donc au travers d'une transparence complète auprès des personnes concernées que la relation de confiance pourra être rétablie et ceux-ci seront plus enclins à partager leurs données. » (Une autorité régionale)

Au-delà même de la fourniture d'une déclaration de confidentialité claire, les autorités publiques devraient se concentrer davantage sur l'application de sa propre obligation de transparence en matière de traitement des données. Le citoyen ne sait pas suffisamment quelles données sont utilisées par quelle instance et dans quel but. Le lien entre les décisions politiques et les données sur lesquelles elles se fondent n'est pas non plus suffisamment transparent. C'est pourquoi il est préconisé de mettre en place une plateforme numérique centrale sur laquelle les citoyens peuvent accéder facilement à ces informations et, dans la mesure où c'est légalement possible, gérer l'accès à leurs données à caractère personnel et leur utilisation.

La création d'un registre des données à caractère personnel gérées par les services publics est citée comme un pas dans la bonne direction. Toutefois, cela ne doit pas se limiter au catalogage des bases de données. De même, le croisement de données à l'aide de procédés ou d'outils tels que datamining, datamatching et datawarehouses doit être inclus dans ce cadastre. Le même besoin de transparence s'applique aux analyses d'impact relatives à la protection des données effectuées par les instances publiques et aux avis de l'autorité de protection des données sur ces analyses. En particulier, en ce qui concerne le développement et l'utilisation d'applications innovantes, la publication de ces analyses et avis donnerait aux citoyens un aperçu du respect de la législation sur la protection de la vie privée.

Les éléments essentiels de la protection des données dans chaque législation pertinente. Les principes de base du traitement des données, également appelés éléments essentiels (finalité du traitement, catégories de données, destinataires, etc.), devraient être inclus dans toute législation qui implique un traitement des données ou des flux de données. Il est à noter qu'une grande partie de la législation existante et ancienne ne fournit toujours pas ces principes de base. Même dans les législations plus récentes, cela reste un point d'attention et les principes de base sont encore trop souvent énoncés en termes généraux. Cela laisse trop de latitude aux responsables du traitement et réduit la prévisibilité de la gestion des données. Par exemple, la possibilité pour les autorités publiques de traiter ou de

transmettre des données à caractère personnel sous « forme pseudonymisée ou anonymisée » ne donne aucune indication sur la manière dont le traitement ultérieur sera effectivement effectué.

Comme indiqué précédemment, ce problème concerne également l'existence d'un fondement juridique claire pour le traitement des données à caractère personnel, plus particulièrement par les services publics. Dans l'exercice de leurs fonctions statutaires, les services publics lancent parfois des opérations de traitement de données pour lesquelles aucun fondement juridique explicite ou distinct n'a été déterminé. Un fondement juridique général, tel qu'un mandat légal ou l'exécution d'une tâche dans l'intérêt public, est souvent invoqué. Cependant, la transparence et la confiance dans la bonne gestion des données à caractère personnel par les autorités publiques nécessitent une délimitation juridique spécifique, notamment pour les opérations de traitement de données complexes ou sensibles. De plus, la transparence pourrait être augmentée en créant une législation sectorielle sur la protection des données pour les services publics.

Enfin, l'importance du respect et de la mise en œuvre de l'obligation de prendre les mesures organisationnelles et techniques nécessaires et appropriées pour que le traitement des données à caractère personnel s'effectue dans un environnement sécurisé est également soulignée. Il s'agit notamment de garanties humaines et techniques concernant l'accès aux données à caractère personnel et leur utilisation, la réalisation d'audits de sécurité réguliers, la journalisation, etc.

Faciliter l'application de la législation. La transparence et la confiance vont également de pair avec la mesure dans laquelle est créé un climat dans lequel les différentes parties impliquées ont la possibilité de remplir leurs obligations, d'exprimer leurs préoccupations ou de remplir leurs obligations légales et statutaires. En d'autres termes, les ressources nécessaires doivent être consacrées à la mise en pratique d'un cadre législatif. Il est souligné que cet aspect est souvent considéré comme secondaire au sein des organisations ou parmi les décideurs politiques. Par conséquent, des investissements supplémentaires sont nécessaires (financiers, matériels, formations,...).

Vers un plus grand contrôle des citoyens sur l'utilisation des données à caractère personnel. Une façon d'accroître la confiance dans la gestion des données à caractère personnel est de donner aux citoyens un plus grand contrôle sur leurs propres données. L'évaluation montre que l'adhésion à ce niveau est importante. Les autorités fédérales pourraient stimuler le développement des coffres-forts numériques en ancrant ce concept dans la loi et en soutenant les partenaires privés dans son développement. Ces applications redonnent aux utilisateurs le contrôle de leurs données à caractère personnel et simplifient l'application des droits des personnes concernées, tels que la portabilité des données. Les autorités publiques, elles-mêmes, pourraient également utiliser cette technologie à leur propre niveau et ainsi contribuer à renforcer le droit à la vie privée du travailleur, d'une part, et à simplifier certains processus, d'autre part.

Par ailleurs, les éventuels obstacles à la fourniture appropriée et adéquate de services si le droit d'accès et de contrôle sur ses propres données à caractère personnel est étendu dans un sens absolu sont également soulignés. Dans le secteur de la santé, par exemple, la disponibilité numérique des données de santé au nom d'un patient peut faire en sorte que celui-ci soit informé de résultats médicaux avant que le prestataire de soins qui l'accompagne n'en ait connaissance. Il est également préconisé donc une application modulaire du droit d'accès dans l'intérêt du patient, par exemple en introduisant un délai

avant que les données de santé ne soient accessibles au patient. Cela devrait également permettre aux prestataires de soins de santé de s'acquitter d'obligations légales supplémentaires (par exemple, vérifier que les documents médicaux ne contiennent pas de données de tiers, ne contiennent pas d'informations préjudiciables au patient ou qu'un patient ne subit pas de pression de la part de tiers). Dans le contexte des mineurs, cette considération s'applique d'autant plus.

D'autres, en revanche, sont d'avis que ce ne sont pas les données personnelles qui doivent être au centre de la politique, mais plutôt leur utilisation par les organisations privées et publiques. Il devrait également y avoir plus de transparence autour de l'utilisation des algorithmes et des finalités du traitement des données à caractère personnel. Dans le secteur public en particulier, l'idée de développer un registre d'algorithmes pour les organismes publics a été évoquée.

Il convient également de mettre davantage l'accent sur les partenariats public-privé dans la gestion des données. Selon certains, cela devrait freiner la prolifération de pratiques innovantes non réglementées. Plus largement, il est également plaidé pour une réflexion sur une plus grande souveraineté numérique. Ce débat peut avoir lieu à plusieurs niveaux (régional, national, européen) et devrait s'inscrire dans une stratégie globale et cohérente de gestion des données (par exemple, en développant un système de cloud propre).

La limitation de l'imposition de sanctions administratives pécuniaires aux services publics. L'article 221 de la Loi vie privée prévoit que le régime des amendes administratives prévu à l'article 83 du RGPD ne s'applique pas aux autorités et à leurs préposés ou mandataires, sauf s'ils sont une personne morale de droit public offrant des biens ou des services sur un marché. Malgré la décision de la Cour constitutionnelle du 14 janvier 2021 selon laquelle cette disposition n'était pas inconstitutionnelle, l'exclusion d'une partie du secteur public est perçue comme discriminatoire par le secteur privé. Les investissements consentis par l'industrie et l'impact éventuel de sanctions suite à des audits de l'autorité de contrôle sont disproportionnés par rapport au respect du RGPD par le secteur public. Cela peut nuire à la confiance des citoyens dans la gestion des données à caractère personnel par les autorités publiques, car cela peut créer un sentiment d'impunité. L'exclusion des autorités publiques des amendes administratives est donc dénoncée par des délégués à la protection des données du secteur public lui-même.

En outre, ce régime d'exception pour le secteur public pose le problème de la responsabilité conjointe et solidaire en cas de responsabilité conjointe du traitement. En cas de violation de la législation sur la protection de la vie privée, les organisations privées devront supporter l'intégralité de l'amende administrative. Enfin, l'incohérence avec d'autres législations est également soulignée. Par exemple, la transposition de la directive NIS sur les mesures pour un niveau commun élevé de sécurité des réseaux et des systèmes d'information ne prévoit pas un tel régime d'exception pour les autorités publiques. Toutefois, le champ d'application de la directive NIS couvre également les données à caractère personnel.

D'autres estiment que cette exclusion doit être maintenue. Si une modification de la loi s'avérait nécessaire, il faudrait au moins préciser la qualification des autorités qui sont ou peuvent être exclues. Si la réglementation existante est utilisée, le législateur devrait au moins clarifier davantage le concept d'autorité publique. Autre point souligné : l'interprétation restrictive de la législation actuelle par l'Autorité de protection des données, qui fait que certaines entités (p. ex. des écoles ou des universités) tombent encore dans le champ d'application de l'article 83 du RGPD et peuvent donc être soumises à

une amende administrative. Ainsi, une plus grande sécurité juridique est nécessaire quant à l'intention et à la portée du législateur concernant ce régime d'exception.

Une politique d'application efficace. La confiance des citoyens dans la protection de leurs données à caractère personnel présuppose une politique efficace de mise en œuvre en cas de violation de la loi. L'utilisation abusive des données à caractère personnel doit être combattue de manière efficace et efficiente. Son importance doit être replacée dans un contexte plus large dans lequel des phénomènes tels que le piratage, les fake news, la désinformation, la diffamation et le harcèlement en ligne, etc. sont des excès de la croissance exponentielle de l'utilisation d'Internet dans notre vie quotidienne et nuisent à une utilisation sereine et constructive des services Internet et des nouvelles applications technologiques. Face à de tels phénomènes, les autorités de contrôle doivent être équipées de manière adéquate.

Plus précisément, la question se pose de l'efficacité du système de sanctions pénales instauré par le RGPD et le titre 6 de la Loi vie privée. À ce jour, ces sanctions pénales semblent ne pas avoir été utilisées, ou très peu. En outre, il est souligné que, dans certains cas, des sanctions pénales pèsent sur la tête du responsable du traitement pour les échanges internationaux de données pour lesquels il serait peu clair ou presque impossible de respecter les normes de confidentialité. Il est fait référence aux conséquences de l'arrêt Schrems II et à l'échec de la conclusion d'un nouvel accord bilatéral entre l'Union européenne et les États-Unis. Enfin, il est souligné que l'accent est trop mis sur les sanctions et pas assez sur la médiation.

Législation européenne contradictoire ou concurrente. Il a déjà été mentionné que la relation entre la législation sur la protection de la vie privée et les autres législations n'est pas toujours claire. Cela s'applique également à d'autres législations européennes qui regroupent parfois des instruments juridiques européens contradictoires ou concurrents, par exemple, la relation entre le RGPD et la directive PSD2 ou entre le RGPD et la directive anti-blanchiment. Dans d'autres cas, il s'agit d'une divergence entre la législation nationale et européenne.

Ainsi, la question se pose de savoir dans quelle mesure la loi du 11 avril 1994 relative à publicité de l'administration s'applique aux registres des traitements de données que tout responsable du traitement est tenu de tenir en vertu du RGPD. Ces registres sont souvent considérés comme des documents internes et peuvent également contenir des données sensibles pour l'entreprise, telles que des informations sur les mesures de sécurité techniques et organisationnelles appliquées par un responsable du traitement ou des informations contractuelles sur les sous-traitants. Par extension, la question se pose de savoir dans quelle mesure les obligations de transparence d'un service public s'appliquent et dans quelle mesure il est opportun d'aller vers une centralisation des registres des activités de traitement. Après tout, un registre des activités de traitement doit être conçu sur mesure et tenir compte des fonctionnalités du traitement des données qui a lieu.

3.4. Soutien et orientation dans l'application de la Loi vie privée

L'accent est mis sur la communication, la sensibilisation et l'autonomisation. Malgré les progrès réalisés en matière de sensibilisation et de traitement des aspects relatifs à la vie privée dans le cadre du traitement des données depuis l'existence du RGPD, il existe encore beaucoup d'incertitudes concernant la protection des données, en particulier chez les indépendants et les PME. Il est donc nécessaire de renforcer l'information, la communication et la sensibilisation, par exemple sur les flux de données et le stockage des données, mais aussi sur la protection de la vie privée en général ou sur les questions éthiques liées à la protection des données à caractère personnel et de la vie privée. Les citoyens, eux aussi, tireraient un bénéfice d'informations plus nombreuses et de meilleure qualité, mais de même, au sein du secteur public, la législation sur la protection de la vie privée est encore trop méconnue.

Dans certains cas, cela est dû à un manque de ressources ou de possibilités de formation, mais la raison sous-jacente est souvent l'absence d'une culture organisationnelle qui donne la priorité à cet aspect. Cela met tous les acteurs impliqués dans un flux de données dans une position difficile. Lorsque les règles ne sont pas claires, qu'elles ne sont pas appliquées ou qu'elles le sont de manière incohérente, ou que l'on n'investit pas suffisamment dans la sensibilisation de l'organisation, des défaillances se produisent inévitablement dans la chaîne des responsables du traitement, des sous-traitants, des délégués à la protection des données, des fournisseurs de données et des utilisateurs de données. Cela peut se traduire par l'absence de fondement juridique pour le traitement des données à caractère personnel ou l'existence d'un cadre juridique incomplet ou peu clair, la mise en place de systèmes de traitement de l'information qui ne sont pas conformes aux normes actuelles et présentent donc un risque pour la sécurité, l'impossibilité de répondre aux demandes des citoyens d'exercer leurs droits (accès, rectification, effacement,...) de manière appropriée et en temps utile,...

Un rôle particulier est joué par les autorités de contrôle, qui devraient investir davantage dans leur rôle d'orientation, d'information et de soutien. Communiquer avec le citoyen, le responsable du traitement ou le délégué à la protection des données pour suivre les différentes procédures ou mettre en œuvre les mesures de protection de la vie privée requises exige des efforts supplémentaires. Des canaux de communication directe avec les entreprises et les professionnels de la protection de la vie privée, éventuellement par le biais de fédérations sectorielles, seraient les bienvenus. Cela permettrait aux responsables du traitement et aux sous-traitants de prendre en compte les éventuelles préoccupations d'une autorité de contrôle dès l'élaboration d'un processus de traitement des données, afin de mieux évaluer les risques éventuels et d'éviter d'éventuelles sanctions à un stade ultérieur. Une meilleure compréhension des besoins d'un secteur spécifique permet de mieux aligner les objectifs stratégiques d'une autorité de contrôle.

Développer des outils de soutien. Il a déjà été souligné que l'application des obligations légales implique souvent une charge administrative qui est perçue comme bureaucratique, rigoureuse et inefficiente. D'autre part, les règles souvent encore peu claires entravent les processus innovants. Il y a donc un large plaidoyer pour passer à la vitesse supérieure dans l'utilisation des outils d'accompagnement et de soutien du RGPD. Des normes concrètes, des bonnes pratiques, des outils sectoriels et des modèles - validés par les autorités de contrôle - peuvent fournir le cadre nécessaire pour traiter les données de manière plus fluide et plus efficace, dans le plein respect des normes applicables en matière de

protection de la vie privée. Les autorités de contrôle pourraient également harmoniser et simplifier leurs recommandations et conseils, développer des FAQ et des modèles, et mettre en place une assistance de première ligne avec une section spécifique qui se concentrerait sur le soutien et le contrôle des services publics.

La prévisibilité de l'application des principes du RGPD et de la loi sur la vie privée pourrait également être améliorée, par exemple par le biais d'un mécanisme de « privacy rulings ». Ce mécanisme permettrait à l'autorité de contrôle d'interpréter l'application de la législation en fonction du cas individuel de traitement des données qui se présente. Cela permettrait de renforcer la sécurité juridique, la prévisibilité, la clarté et la conformité.

« *Le RGPD fournit une boîte à outils à la disposition de tous les types d'entreprises et d'organisations pour démontrer comment se conformer à la législation, comme des codes de conduite, des mécanismes de certification et des clauses contractuelles types. Ces instruments doivent être utilisés au maximum. Les petites et moyennes entreprises en particulier soulignent l'importance et l'utilité de codes de conduite adaptés à leur situation et n'entraînant pas de coûts ou de charges excessifs.* » (Une fédération professionnelle)

L'application de codes de conduite sectoriels et thématiques aiderait les responsables du traitement à obtenir un label conforme au respect de la vie privée. Il peut donc constituer un outil important pour les fédérations sectorielles, mais l'élaboration de ces codes de conduite nécessite une expertise et des ressources. Ici aussi, les responsables du traitement et les sous-traitants devraient pouvoir bénéficier d'une application simplifiée des codes de conduite. Une extension des codes de conduite peut également réduire la charge de travail des autorités de contrôle.

L'élaboration de codes de conduite présuppose la mise en place de mécanismes de contrôle pour vérifier le respect du code de conduite. Ces mécanismes doivent être accrédités par les autorités de contrôle. Toutefois, le coût du contrôle et de l'application des codes de conduite doit être proportionnel aux capacités des fédérations sectorielles. Pour certaines fédérations professionnelles, il n'est pas non plus possible de prévoir un organe de contrôle indépendant. En outre, les codes de conduite doivent être conçus sur mesure. Si la barre était placée trop haut, certains secteurs pourraient ne pas être en mesure de respecter certaines normes, ce qui entraînerait un désavantage concurrentiel par l'exclusion de l'accès au marché.

Les systèmes de certification peuvent également aider les responsables du traitement, accompagner l'application des règles de confidentialité et renforcer la protection des données à caractère personnel, par exemple pour le traitement des données sensibles. Ainsi, la certification peut être utilisée par les responsables du traitement pour démontrer qu'ils mettent en œuvre des mesures de protection de la vie privée dès la conceptualisation des processus de traitement des données et en tant que norme. BELAC, en tant qu'autorité nationale de certification, peut jouer un rôle central dans ce domaine.

L'application des analyses d'impact relatives à la protection des données. Les responsables du traitement et les sous-traitants ont également besoin d'un meilleur accompagnement pour évaluer et traiter les risques. Les analyses d'impact constituent un outil important à cet égard, mais elles ne sont pas encore utilisées de manière suffisamment systématique. L'explication réside en partie dans l'absence de lignes directrices sur les conditions et les modalités d'application d'une analyse d'impact

relative à la protection des données. C'est le cas, par exemple, au cours du processus législatif. Les responsables du traitement ont besoin d'éclaircissements sur des questions fondamentales telles que le moment où une analyse doit être effectuée, le moment à partir duquel elle peut ou doit être effectuée dans la réalisation d'un processus de traitement des données, et si une analyse d'impact peut être rationalisée et centralisée dans le cas où plusieurs parties sont impliquées.

En outre, une méthodologie plus globale sur l'utilisation des analyses d'impact relatives à la protection des données devrait également être adoptée. Un responsable de traitement ne doit pas seulement estimer le risque sur la base des principes de nécessité et de proportionnalité. Le caractère intrusif d'un traitement de données doit être analysé dans un contexte plus large. Le terrain a donc besoin d'un accompagnement plus important au niveau de la manière de mener ces exercices souvent complexes, et si possible en coopération avec les autorités de contrôle.

Expertise sectorielle au sein des autorités de contrôle. La nécessité de désigner des points de contact au sein de l'Autorité de protection des données pour un secteur et/ou une expertise particuliers est mentionnée à plusieurs reprises. Les parties prenantes sur le terrain font souvent réclament des autorités de contrôle sensibles aux besoins et aux spécificités des opérations de traitement sectoriel. Une application éclairée, correcte et réalisable de la législation sur la protection de la vie privée nécessite une fertilisation croisée entre différents domaines d'expertise, la vie privée et la technologie. Aussi, tant le politique que le juridique et le technique jouent un rôle important dans le développement et mise en œuvre de normes législatives. L'instauration d'un dialogue, d'un débat à double sens où un feed-back est donné, permet aux autorités de contrôle de proposer des avis pragmatiques. En cas de fuite de données, par exemple, il est crucial de pouvoir réagir rapidement.

Il est également suggéré qu'un service d'assistance soit créé au sein de l'Autorité de protection des données afin de fournir des informations gratuites et rapides sur l'application de la Loi vie privée et des règlements sectoriels ou européens connexes.

Dans le même ordre d'idées, et plus particulièrement en ce qui concerne l'Autorité de protection des données, il est également fait référence à l'absence de création du Conseil de réflexion. Le Conseil de réflexion est un organe indépendant de l'Autorité de protection des données qui peut donner des avis non contraignants, par exemple sur le plan stratégique décrivant les priorités du comité de direction. La ratio legis de ce Conseil de réflexion est que, grâce à sa composition multidisciplinaire, il permet à l'Autorité de protection des données de rester en contact avec ce qui se passe sur le terrain et dans la pratique. Un tel organe est généralement considéré comme souhaitable et utile mais n'a pas encore été créé par la Chambre des représentants.

3.5. Un cadre pour l'innovation

Nécessité d'une politique globale de gestion des données. La législation belge sur la protection de la vie privée découle d'un cadre européen dont la protection des données à caractère personnel est la pierre angulaire. Toutefois, un système d'information ou un traitement de données est souvent plus complexe que le simple traitement de données à caractère personnel et se compose également de données non personnelles. Après tout, la numérisation et l'innovation ne reposent pas uniquement sur les données

à caractère personnel, mais sur les données au sens large du terme. En outre, la protection vise les personnes physiques et la question se pose de savoir dans quelle mesure les personnes morales devraient également bénéficier d'un certain niveau de protection. Dans l'ensemble, il est donc nécessaire de mettre en place une politique qui non seulement tienne compte de la dimension de protection de la vie privée du traitement des données, mais qui définisse également une vision globale de la gestion des données.

Le paysage juridique actuel, fragmenté et incomplet en matière de gestion des données freine les développements innovants. Pour faciliter les échanges de données de toutes sortes et stimuler l'innovation grâce aux nouvelles technologies, il faut un cadre politique et législatif approprié. Un tel objectif devrait également permettre à la Belgique de passer à la vitesse supérieure dans le développement d'une économie de la connaissance afin de se positionner plus fortement face aux plateformes numériques qui ont pris une position de quasi-monopole sur le marché. Le contrôle de la gestion des données est essentiel pour optimiser l'échange de données. De même, un tel objectif permettrait à la Belgique de se conformer à certaines obligations internationales. Par exemple, la Belgique est souvent pointée du doigt par les organismes internationaux pour son manque de données statistiques. Là aussi, la Belgique doit se montrer à la hauteur. En outre, d'autres dimensions doivent être prises en compte, au-delà de la perspective juridique et de la sécurité de l'information, par exemple les questions éthiques. Sur ce point également, la législation belge est insuffisante.

En outre, nous devons également tenir compte de l'impact de la numérisation sur l'environnement. Les matières premières qui permettent le développement de nouvelles technologies ne sont pas disponibles à l'infini. Il est donc proposé d'envisager une politique de mutualisation des services numériques afin d'en réduire la consommation. La normalisation, l'interopérabilité et la réutilisation des données peuvent constituer un principe directeur à cet égard.

Plus généralement, les autorités publiques devraient s'appuyer encore davantage sur l'utilisation des données dans le processus d'élaboration des politiques et le processus décisionnel. Parallèlement, il est également plaidé pour un débat sur les limites de l'innovation et des nouvelles technologies. Le RGPD fournit un cadre, par exemple, sur l'utilisation des données à caractère personnel pour le profilage, mais ce cadre doit être approfondi au niveau national ou européen. Le RGPD est également un instrument réglementaire neutre sur le plan technologique, qui est en outre complété par une législation sectorielle (par exemple, sur les communications électroniques avec la directive « vie privée et communications électroniques ») ou thématique (par exemple, le projet de règlement sur l'intelligence artificielle).

En d'autres termes, la Loi sur la vie privée est un maillon d'un ensemble plus vaste. Une loi sur la gestion transparente et efficace des données peut apporter une réponse concluante à toutes ces dimensions et à tous ces défis.

Une interprétation plus ouverte du mandat de contrôle. Les autorités de contrôle, elles aussi, pourraient adopter une approche plus diversifiée au lieu de se positionner simplement comme le chien de garde de la protection des données pour les citoyens. Il est noté que le mandat qui leur est confié dans le cadre du RGPD est plus large et qu'ils devraient également prendre en compte l'importance de l'innovation et de la numérisation. En particulier, les autorités de contrôle doivent être en mesure de guider les processus de conception des nouvelles technologies à un stade précoce, par exemple dans le cas du traitement des données biométriques ou de l'application de l'intelligence artificielle.

Les autorités de contrôle pourraient également adopter une position plus claire sur les questions de confidentialité. Pour cela, il est évidemment important que leur indépendance soit respectée. C'est une condition sine qua non si l'on veut qu'une autorité de contrôle puisse participer pleinement aux débats sociaux ou les initier.

Se concentrer sur les atouts de l'Europe. La domination américaine en matière de technologie Internet et de services connexes devrait être brisée. La vision européenne de la protection de la vie privée et des données peut être réalisée par une utilisation accrue de la technologie Internet européenne. Dans la mesure où les services publics doivent s'appuyer sur des services fournis par des entreprises de type GAFA, une gestion stratégique des fournisseurs similaire à celle en place aux Pays-Bas pourrait être envisagée. La contractualisation au niveau des services publics individuels nous place dans une position de négociation plus faible. L'élévation des négociations à un niveau centralisé et coordonné devrait permettre aux autorités belges d'imposer des conditions plus favorables. Cela a également son importance en ce qui concerne les clauses contractuelles en tant que sous-traitant de données à caractère personnel de citoyens et de résidents belges.

Le principe de minimisation des données doit être au cœur de toute initiative innovante en matière de traitement des données. Dans le secteur public, la question du traitement des données à caractère personnel et de l'utilisation des algorithmes devrait être au cœur des marchés publics. Des clauses types sur l'utilisation des données apporteraient une sécurité juridique et des conditions de concurrence équitables qui abaisseraient le seuil à partir duquel les petits acteurs du numérique peuvent soumissionner pour des marchés publics, en particulier pour des projets innovants.

Le concept de « regulatory sandboxes » revient sans cesse comme un point d'intérêt. La mise en place d'un cadre juridique explicite à cette fin répond au besoin de flexibilité dans l'application des réglementations existantes ou devrait compenser l'absence de réglementations sectorielles. Ce mécanisme permet de mettre en place des projets pilotes sous certaines conditions et en accord avec les autorités de contrôle compétentes. En d'autres termes, un cadre est mis en place dans lequel le seuil réglementaire est abaissé pour encourager et soutenir l'innovation. Les entreprises ont ainsi la possibilité d'effectuer des tests en direct et de se faire accepter par le marché.

La place du consentement comme fondement juridique du traitement des données. Le consentement en tant que fondement juridique se heurte souvent à l'évolution des technologies. Un cadre de protection des données trop strict peut également avoir l'effet inverse et créer une connotation négative chez les utilisateurs des nouvelles technologies. Il convient donc de débattre de l'importance du consentement en tant que fondement juridique du traitement des données à caractère personnel.

Il existe également des secteurs dans lesquels le consentement comme fondement juridique complique le traitement des données à caractère personnel, par exemple pour les assureurs ou les chercheurs scientifiques. Une personne a le droit de retirer son consentement à tout moment, ce qui compromet la fin de certains traitements avant la conclusion d'un contrat. La recherche scientifique, peut, elle aussi, être entravée par l'obligation de se fonder sur le consentement comme fondement juridique. Il est donc soutenu que, dans le cadre de l'article 9 § 4 du RGPD, il faut utiliser la possibilité de prévoir un cadre juridique supplémentaire, par exemple pour les données relatives à la santé, dans lequel la conclusion d'un contrat est considérée comme le fondement juridique plutôt que le consentement.

Toutefois, aucune ligne claire ne peut être tracée dans le débat sur l'interprétation du consentement comme fondement juridique. Dans le secteur de la santé, d'une part, on préconise la flexibilité nécessaire et la mention explicite dans la Loi vie privée que les prestataires de soins de santé peuvent gérer le dossier numérique sans le consentement préalable explicite du patient. La capacité de gérer conjointement un dossier patient numérique entre les réseaux hospitaliers au moyen d'une base de données commune est également considérée comme une évolution nécessaire. D'autre part, des voix s'élèvent pour demander une interprétation plus granulaire de l'obligation de consentement, par exemple pour donner aux patients plus de poids dans le transfert de leurs données à caractère personnel. La relation entre le consentement du patient en tant que fondement juridique et l'obligation légale de partager des données de santé via des canaux et des plateformes numériques pose aussi parfois des dilemmes éthiques, juridiques et opérationnels aux prestataires de soins et aux institutions.

Établir le cadre juridique du traitement des données dans le contexte de la recherche scientifique. La Belgique a transposé l'article 89, §§ 2 et 3 du RGPD par le biais du titre 4 de la Loi vie privée. Les avis sont partagés sur l'existence d'un titre distinct dans la Loi vie privée qui s'applique au traitement des données à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique ou de statistiques. D'une part, il est fait référence à la flexibilité que le RGPD a voulu introduire pour les traitements de données de cette nature. Imposer des réglementations supplémentaires est considéré comme l'ajout d'une couche complexe d'obligations en plus de celles qui existent déjà. Par exemple, il est fait référence à la nécessité d'ajouter les analyses d'impact relatives à la protection des données (article 191 de la Loi vie privée) et les accords de traitement (article 196 de la loi sur la Loi vie privée) au registre de traitement des données ou à l'obligation de réaliser une analyse d'impact relative à la protection des données à caractère personnel sensibles. Des réglementations supplémentaires ou différentes du cadre européen peuvent également être perçues comme un obstacle à la mise en place de projets de recherche dans un contexte européen. D'autre part, le besoin de clarification - et éventuellement d'un cadre réglementaire supplémentaire - en ce qui concerne l'implication des étudiants dans la recherche universitaire et le fait que l'anonymisation ou la suppression des données à caractère personnel sur des logiciels privés n'est pas toujours possible est mentionné.

D'autres se félicitent de l'introduction du titre 4 de la Loi vie privée mais soulignent les difficultés qu'ils rencontrent en pratique pour l'appliquer. Cela est dû, par exemple, à une terminologie peu claire, au manque de précisions sur les exigences procédurales, à l'applicabilité de certaines obligations et au chevauchement ou à la relation avec d'autres législations applicables (par exemple, sur les essais cliniques). Le mécanisme par lequel il faut travailler avec des tiers de confiance pose également des problèmes particuliers aux universités et aux écoles supérieures, car il y a peu d'acteurs sur le marché qui remplissent les conditions de la Loi vie privée. Cela a pour effet d'augmenter le coût des investissements. On pourrait aussi envisager de confier le rôle de tiers de confiance à des experts en recherche ou à des départements au sein même d'une université.

Compte tenu de ces obstacles, il arrive que certaines fédérations conseillent à leurs membres de ne pas faire usage du régime d'exception du titre 4, car il exige également plus d'obligations de conformité que la simple application du RGPD. En outre, il est également fait référence au champ d'application limité du titre 4. Ce n'est que lorsque l'exercice des droits des personnes concernées menace de rendre l'enquête impossible ou peut l'entraver et que des dérogations sont donc nécessaires pour atteindre les objectifs du traitement que le régime d'exception s'applique. Si aucune restriction n'est requise, le titre

4 ne s'applique pas. Dans la pratique, cela conduit à un manque de clarté. Par ailleurs, la possibilité de ne pas appliquer une partie du titre 4 dans la mesure où un code de conduite est établi (cf. article 187 de la Loi vie privée) est considérée comme inapplicable en l'état actuel des choses, car il n'y a pas de clarté quant à l'organe qui devrait être chargé de contrôler l'application du code de conduite.

Dans le secteur de la santé en particulier, des appels sont lancés en faveur d'un débat interfédéral sur l'établissement d'un cadre pour la mise à disposition de données de santé anonymisées ou pseudonymisées à des fins thérapeutiques et statistiques. Un tel débat suppose que des réponses soient apportées à différents problèmes : les questions éthiques, le verrouillage juridique de l'utilisation possible de ces données, la définition de normes à respecter par les tiers de confiance, la création d'un cadre pour le développement de cas d'utilisation, etc.

Compte tenu de l'importance de l'échange de données et de la recherche scientifique pour l'innovation, il convient d'actualiser le titre 4. Une simplification et un assouplissement du régime d'exception devraient donner à la Belgique un avantage concurrentiel par rapport au cadre général du RGPD et atténuer autant que possible les restrictions liées à la recherche scientifique. C'est notamment le cas de la recherche scientifique dans le secteur de la santé. Il est également nécessaire de mieux communiquer sur l'application du titre 4 et ses implications concrètes.

3.6. Améliorer l'échange des données

Simplification du système des protocoles administratifs et de l'accès aux données administratives. L'obligation faite par l'article 20 de la Loi vie privée aux services publics de conclure des protocoles d'échanges de données ne répond pas suffisamment à l'attente du législateur. Ce système a été introduit en réponse à la suppression du système précédent de comités sectoriels de l'ancienne Commission de la protection de la vie privée. Afin de dissiper les craintes que la suppression du filet de sécurité des comités sectoriels freine l'échange de données entre et parmi les services publics, la loi a introduit la possibilité de conclure des protocoles. En effet, ce système est conforme à la lettre et à l'esprit du RGPD, notamment à l'obligation de responsabilité qui rend les responsables du traitement responsables de l'organisation des échanges de données et de la détermination des modalités selon lesquelles ils ont lieu. Parallèlement, le comité de sécurité de l'information a aussi été créé, qui peut intervenir dans la détermination des modalités d'échanges de données par délibération.

Cet ensemble est considéré comme trop complexe, opaque et lourd. L'exigence de protocoles ou d'accords individuels pour l'échange de données constitue une lourde charge administrative et devrait être simplifiée (par exemple par un formulaire standard simplifié ou par la publication des protocoles de manière centralisée plutôt que sur les sites web de chaque responsable du traitement individuel). La possibilité de conclure des protocoles plus généraux est également préconisée, par exemple dans le cas d'échanges de données entre plusieurs parties. Il est également proposé d'étudier dans quelle mesure la facilitation de l'accès aux données administratives pourrait être améliorée et accélérée par l'intervention d'un mécanisme qui pourrait agir comme un tiers indépendant. Il est également préconisé que l'accès aux données détenues par les autorités publiques, et en particulier l'accès aux sources authentiques, reste gratuit.

Dans la foulée, une référence plus générale est faite à la complexité et à la lourdeur de l'accès aux données des autorités publiques (fédérales). Selon le type de données administratives, une procédure différente doit être suivie : une décision du ministre de l'Intérieur pour l'accès au Registre national, une délibération du Comité de sécurité de l'information pour les données sociales et sanitaires, un protocole conformément à l'article 20 de la Loi vie privée ou une délibération du Comité de sécurité de l'information pour les autres données administratives fédérales. En outre, il existe un patchwork législatif qui impose des règles spéciales par décret royal pour l'accès à certaines bases de données.

« Cette loi-cadre représente une avancée significative en ce qu'elle pose un réel accent sur une plus grande transparence mais également un meilleur contrôle des données. De plus, elle oblige aux institutions publiques de réaliser un inventaire de leurs traitements et de regarder leur légitimité ainsi que licéité. Dans beaucoup de cas, cela a permis à ceux qui voulaient assurer une certaine niveau de conformité de remettre en question leurs traitements mais aussi leur façon de travailler et de modifier leur procédure d'accès, d'extraction et de partage des données. Cependant, cela aurait dû être les résultats attendus pour la majorité des administrations publiques mais des faiblesses ont freiné l'aboutissement des objectifs de la loi-cadre. » (Une autorité régionale)

L'accès aux données administratives devrait donc être organisé de manière plus uniforme et simplifiée, éventuellement en faisant évaluer toutes les demandes d'accès par un organisme indépendant.

Par ailleurs, des efforts plus importants devraient être faits pour rendre les données administratives disponibles et pour maximiser l'utilisation des données disponibles. La qualité des données constitue un point d'attention particulier à ce niveau.

Revoir le rôle du Comité de sécurité de l'information. Le respect de l'obligation de fournir un fondement juridique clair et transparent pour le traitement des données à caractère personnel représente une préoccupation générale. Dans ce contexte, le rôle et le fonctionnement du comité de sécurité de l'information sont remis en question. L'influence éventuelle du Comité de sécurité de l'information dans la détermination ou l'élaboration plus poussée des éléments essentiels d'un traitement de données peut être en contradiction avec l'obligation de faire fixer ces éléments par le législateur. En outre, il existe un manque de clarté concernant la nature juridique des décisions du comité de sécurité de l'information et la possibilité de faire appel.

La ligne de démarcation avec les pouvoirs des autorités de contrôle, en particulier l'Autorité de protection des données, devrait également être clarifiée. La mesure dans laquelle le Comité de sécurité de l'information serait en mesure d'interpréter les dispositions du RGPD par le biais de délibérations ou de recommandations soulève la question de savoir si le Comité de sécurité de l'information n'entre pas ainsi dans le champ de compétence d'une autorité de contrôle indépendante.

La relation avec les responsables des traitements des données, en particulier les administrations publiques, est également considérée comme problématique. Par exemple, le Comité de sécurité de l'information peut agir à la demande d'une seule administration publique et ainsi émettre des recommandations contraignantes sans la participation de toutes les administrations publiques. Il est également mentionné que l'action du Comité de sécurité de l'information peut affecter l'autonomie d'une administration en tant que responsable du traitement des données.

Par ailleurs, fonctionnement efficient du Comité de sécurité de l'information par rapport aux autres modalités d'accès existantes est souligné et il est préconisé de maintenir un tel organe.

Le contenu de la qualité de responsable du traitement et sous-traitant. Au sein d'une même entité (université, service public, etc.), il est possible que des responsables du traitement aient été désignés à différents niveaux. Cette question a été soulevée précédemment. Toutefois, l'existence de plusieurs responsables du traitement des données au sein d'une même entité soulève également des questions pratiques quant à l'application des différentes obligations prévues par le RGPD et la Loi vie privée. Par exemple, peut-on tenir un seul registre des activités de traitement ou faut-il établir plusieurs registres, un pour chaque responsable du traitement ? Des accords doivent-ils être conclus entre les différents responsables de traitement sous la forme de protocoles conformément à l'article 20 de la Loi vie privée, d'accords de traitement de données ou d'un accord entre responsables du traitement conjoints ? La clarification de ces questions a un impact immédiat et pratique sur la facilitation des échanges de données.

Renforcer le fonctionnement des intégrateurs de services. Le système des intégrateurs de services est considéré comme un facteur clé de la réussite de la gestion des données administratives. Le rôle des intégrateurs de services doit être renforcé à tous les niveaux. La réalisation des objectifs en matière d'e-gouvernement, de simplification administrative et de réutilisation des données en dépend. L'accès aux sources authentiques devrait donc être encore élargi. Le rôle des intégrateurs de services dans la mise en place des échanges de données du secteur public doit également être clarifié. En effet, les intégrateurs de services ne sont pas toujours impliqués.

L'utilisation d'intégrateurs de services pour l'échange de données devrait être davantage encouragée. Leur rôle pourrait également être étendu, non seulement à l'échange de données à caractère personnel entre les services publics, mais aussi à l'égard des citoyens. En outre, le développement à part entière des intégrateurs de services renforcerait également la transparence du traitement des données à caractère personnel par les autorités publiques, car l'intégrateur de services enregistrerait automatiquement les flux de données.

Élargir l'accès aux données du registre national. L'utilisation de certaines données à caractère personnel telles que le numéro de registre national ou les données du registre de la population qui sont régies par une législation spéciale ou sectorielle pourrait contribuer à des processus de simplification administrative. L'identification correcte d'une personne joue un rôle crucial dans de nombreux processus administratifs et est également requise par diverses réglementations. L'élargissement de l'accès au registre national et de l'utilisation du numéro de registre national pourrait donc contribuer de manière significative à la transformation digitale et à la simplification des procédures administratives.

Le développement d'un portefeuille d'identification numérique est également présenté comme un outil permettant de faciliter l'interaction entre les citoyens et les organisations privées ou publiques.

Nécessité d'une interprétation et d'une application pragmatiques de la Loi vie privée. L'interprétation stricte de l'article 22 de la Constitution par l'Autorité de protection des données est perçue comme une entrave à l'organisation par les instances publiques de leur gestion des données. La décision de l'Autorité de protection des données selon laquelle le traitement des données à caractère personnel dans son ensemble doit être fixé par une loi ou un décret freine l'innovation, n'est pas très pragmatique

et ne tient pas compte de la possibilité pour le pouvoir exécutif de pouvoir ou d'être obligé d'organiser le traitement des données dans le cadre de tâches d'intérêt général.

L'approche de l'Autorité de protection des données dans des situations de crise telles que la pandémie du COVID-19 a également été critiquée comme étant trop lourde et trop stricte. En outre, elle ne serait pas en mesure de réagir assez rapidement, avec pour conséquence que des entreprises ont déjà développé des mesures ou des solutions sur le marché qui s'avèrent par la suite ne pas être conformes à l'avis de l'Autorité de protection des données. Il est donc difficile de trouver des solutions viables dans un contexte économiquement et sanitairement extrêmement exigeant.

3.7. La protection des personnes concernées

Renforcer l'accès aux droits des personnes concernées et leur exercice. Le RGPD et la Loi vie privée fournissent un cadre solide de droits sur lesquels les citoyens peuvent s'appuyer, non seulement pour contester l'utilisation abusive de leurs données à caractère personnel, mais aussi pour prendre le contrôle et gérer leurs données à caractère personnel. Le citoyen doit donc être mieux informé de cet éventail de possibilités. Il faut donc faire davantage d'efforts pour informer les citoyens de leurs droits et notamment de la possibilité de déposer une plainte, par exemple en cas de fuite de données. L'exercice du droit d'accès aux données à caractère personnel gérées par les services publics est également encore souvent insuffisant.

Les conditions dans lesquelles le droit d'effacement et de rectification des données à caractère personnel peut ou peut être exercé devraient être clarifiées. Après tout, il n'est pas toujours évident pour les responsables du traitement de savoir dans quelle mesure l'exercice des droits des personnes concernées peut être refusé.

Il est suggéré de dresser et de publier une liste des exceptions aux droits des personnes concernées. Il convient également de clarifier les délais dans lesquels les citoyens sont en droit de recevoir une réponse ou une demande d'exercice de leurs droits. Les organisations syndicales demandent également à être autorisées à déposer une plainte au nom d'un de leurs membres et à exercer un recours administratif ou judiciaire en leur nom.

La relation tendue entre le droit de la vie privée et le droit pénal. L'exercice des droits des personnes concernées dans le paysage judiciaire devrait être clarifié. Le système actuel dans lequel la Loi vie privée renvoie au Code judiciaire, au Code de procédure pénale et à la législation pénale particulière ne fournit pas suffisamment de clarté sur l'existence et l'applicabilité des droits individuels des personnes concernées.

Un problème particulier qui est abordé est l'exception en droit belge à l'exercice du droit d'accès du citoyen aux données à caractère personnel traitées par les autorités de justice pénale. Le régime d'exception consistant à n'autoriser qu'un accès indirect au traitement des données à caractère personnel par les services de police, par le biais d'un système de vérification par l'organe de contrôle de l'information policière, est source de frustration pour les citoyens et n'est pas conforme à l'obligation de transparence attendue des autorités publiques.

Une attention particulière aux groupes vulnérables. Plus généralement, il est préconisé de mettre en place une protection supplémentaire pour les personnes vulnérables telles que les mineurs ou les personnes âgées par le biais d'actions d'information, de sensibilisation et de formation. Le monde numérique doit être accessible à tous, mais de manière informée et sécurisée. Cette question est donc liée à celle, plus large, de la fracture numérique et de l'aide à apporter aux groupes vulnérables pour qu'ils trouvent leur place dans le monde numérique.

En ce qui concerne spécifiquement les mineurs, il est fait référence au manque de clarté quant à la manière dont le RGPD et l'article 7 de la Loi vie privée doivent être appliqués. L'article 7 de la Loi vie privée stipule que le traitement des données à caractère personnel d'un enfant dans le cadre d'une offre directe de services de la société de l'information à un enfant est légal si le consentement est donné par des enfants âgés de 13 ans ou plus. La ligne de démarcation entre le consentement dans le contexte des services de la société de l'information et le fondement juridique du traitement des données à caractère personnel des mineurs en dehors de ce contexte n'est pas claire. Concrètement, l'exemple donné est celui du secteur de la santé. Là, se pose la question de l'accès des mineurs à leurs données de santé, par exemple par le biais d'applications de santé qui se répandent de plus en plus et proposent toutes sortes de services.

3.8. Rôle du délégué à la protection des données

Nécessité d'une plus grande maturité en matière de protection de la vie privée au sein de l'organisation. Le rôle central des délégués à la protection des données devrait bénéficier d'une plus grande visibilité. Ils font partie de la chaîne de responsabilité d'un responsable du traitement ou d'un sous-traitant. Ce faisant, ils contribuent aux processus internes de traitement des données sous la forme d'avis et de missions de surveillance. En même temps, ils sont le lien avec les autorités de contrôle compétentes.

L'importance accordée au poste de délégué à la protection des données au sein d'une organisation reflète le niveau de maturité avec lequel le traitement et la protection des données sont gérés. On constate toutefois que les responsables du traitement des données sont encore sous-utilisés par les responsables du traitement et les sous-traitants. Le rôle du responsable du traitement des données est encore trop souvent considéré au sein d'une organisation comme un facteur qui freine le traitement des données ou les processus innovants. Cela est dû en partie à l'existence de cultures organisationnelles archaïques qui investissent peu dans la gestion du changement. D'autre part, le rôle et le statut du délégué à la protection des données sont encore très mal connus, ce qui signifie que l'on ne sait pas toujours quand et comment on peut ou doit faire appel à ses services.

Plus de souplesse dans l'obligation légale de désigner un délégué à la protection des données. Le cadre juridique concernant le délégué à la protection des données pourrait être complété pour permettre la mise en commun des délégués à la protection des données. On note, en effet, une certaine inquiétude quant à la capacité des petites organisations et entreprises à respecter les obligations légales. La mise en commun leur permettrait d'avoir accès à un délégué à la protection des données commun.

Cela leur permettrait également de se conformer à l'exigence de l'article 20 § 2 de La Loi vie privée qui oblige les organismes privés à désigner un délégué à la protection des données s'ils échangent des

données avec les autorités fédérales. Les petites organisations et entreprises ont du mal à se conformer à cette obligation et peuvent donc être involontairement exclues des marchés publics.

D'autres, en revanche, préconisent d'étendre l'obligation de désigner un délégué à la protection des données au-delà des cas imposés par le RGPD. Si l'activité principale d'une organisation ou d'une entreprise consiste à traiter des données à caractère personnel - qu'il s'agisse ou non de catégories particulières de données à caractère personnel - ou si des technologies intrusives telles que des drones, des caméras ANPR ou des applications de réalité augmentée sont développées, un délégué à la protection des données doit être nommé. Le droit social ne prévoit pas non plus de rôle explicite pour le délégué à la protection des données.

Réduction des obligations supplémentaires par rapport au RGPD. Les articles 20, § 2 et 21 de la Loi vie privée sont remis en cause car le législateur belge va ici plus loin que le RGPD en ce qui concerne les obligations de désignation d'un délégué à la protection des données. Il est préconisé de supprimer l'obligation supplémentaire, prévue à l'article 21 de la Loi vie privée, pour les organisations privées de désigner un délégué à la protection des données pour le traitement des données provenant des autorités fédérales et susceptibles de présenter un risque élevé. Cela parce que la charge administrative par rapport aux avantages en termes de protection des données est jugée disproportionnée. Les autorités publiques disposent déjà d'un délégué à la protection des données et, si une analyse d'impact est effectuée correctement, les risques liés au traitement sont atténués à l'avance.

Si cette obligation est maintenue, il faudrait au moins aligner les conditions de son application sur l'article 35 du RGPD, qui est moins strict. Il convient également de revoir l'obligation prévue à l'article 20, § 2 de la Loi vie privée de désigner un délégué à la protection des données lorsqu'une organisation privée obtient des données à caractère personnel d'une autorité fédérale. Cette obligation n'est pas conforme aux dispositions de l'article 21 de la Loi vie privée. L'avis des deux délégués à la protection des données (autorité fédérale et organisation privée) avant un échange de données ne devrait être obligatoire que dans le cas où une organisation privée a désigné un délégué à la protection des données.

La faisabilité de certaines obligations ou attentes de la part des délégués à la protection des données est également mise en avant. Ils ne sont pas toujours les mieux placés ou dotés des ressources ou de l'expertise nécessaires pour accomplir certaines tâches - parfois supplémentaires. Un exemple cité est celui de la désignation d'un délégué à la protection des données agissant dans le cadre du titre 4 de la Loi vie privée pour émettre un avis sur l'utilisation des différentes méthodes de pseudonymisation et d'anonymisation.

Nécessité de coopération. En premier lieu, il convient de soutenir la coopération entre les délégués à la protection des données, par exemple en centralisant l'accès à l'expertise, aux informations, aux réglementations applicables, etc. La coopération entre l'Autorité de protection des données et les délégués à la protection des données mérite également une attention et un soutien accrus. Les délégués à la protection des données devraient bénéficier d'un meilleur contact et d'un contact direct avec les experts sectoriels au sein de l'Autorité de protection des données. L'importance de la coopération entre les délégués à la protection des données et les spécialistes de la gestion de l'information, y compris les archivistes, est également soulignée.

L'existence d'une ou plusieurs organisations faîtières en Belgique pourrait apporter un soutien supplémentaire au travail des délégués à la protection des données. Il pourrait s'agir d'une plateforme permettant d'échanger des bonnes pratiques, de développer des normes et, surtout, de discuter d'un cas avec discrétion. Après tout, les délégués à la protection des données sont soumis au secret professionnel, qui n'autorise l'échange d'informations que sous certaines conditions, afin que l'employeur du délégué à la protection des données ne soit pas exposé.

Renforcer le statut du délégué à la protection des données. Un débat est en cours sur la nécessité d'une protection supplémentaire et d'un renforcement du statut du délégué à la protection des données. Certains estiment que le délégué à la protection des données devrait bénéficier d'un statut équivalent à celui d'un représentant syndical afin de pouvoir exercer son rôle en toute indépendance au sein de l'organisation.

D'autres estiment que cela n'est pas souhaitable car cela pourrait placer le délégué à la protection des données dans une position de conflit d'intérêts. En tout état de cause, il est suggéré de développer un cadre déontologique sur le modèle de l'organisation française de coordination AFCDP.

3.9. Des autorités de contrôle indépendantes et efficientes

Une simplification du paysage institutionnel de la vie privée. L'importance de l'indépendance des autorités de contrôle et en particulier de l'Autorité de protection des données est fortement soulignée. La gestion des données à caractère personnel par les secteurs public et privé ne peut jouir de la confiance des citoyens que s'il existe également une autorité de contrôle forte, efficiente, impartiale et indépendante. À cet égard, il est souligné que le paysage institutionnel complexe et fragmenté de la protection de la vie privée doit être abordé à la fois dans la loi et dans la pratique. Le fonctionnement de l'Autorité de protection des données doit également être ajusté. Le rapport d'audit de la Cour des comptes du 31 mai 2021 met en évidence des lacunes importantes dans la structure et le fonctionnement actuels de l'Autorité de protection des données. Une modification de la loi organique du 3 décembre 2017 instituant l'Autorité de protection des données est donc nécessaire.

Cette question semble être au cœur des préoccupations de beaucoup. Les responsables du traitement et, en particulier, les services publics, doivent tenir compte d'une multitude d'instances. C'est le cas pour accéder aux données (par exemple, le Registre national), pour transmettre des données (par exemple, le Comité de sécurité de l'information ou la Vlaamse Toezichtscommissie) ou pour se conformer à certaines obligations procédurales (par exemple, l'Autorité de protection des données).

Un point d'achoppement particulier semble être le manque de clarté concernant la répartition des pouvoirs entre les différentes autorités de contrôle, tant interfédérales que nationales. Cela ne crée pas seulement une insécurité juridique, mais entraîne également des charges administratives inutiles (par exemple, la notification des coordonnées du délégué à la protection des données à plusieurs autorités de contrôle) ou un manque de clarté sur les procédures à suivre (par exemple, à quelle autorité de contrôle une fuite de données doit être notifiée).

Plus de synergies et de coopération entre les autorités de contrôle. Une coordination et une coopération accrues sont nécessaires entre les différentes autorités de contrôle. En effet, l'existence de plusieurs autorités de contrôle indépendantes a déjà suscité un certain nombre de préoccupations, telles que l'émergence d'interprétations divergentes de la législation sur la protection de la vie privée ou des difficultés pratiques dans les modalités de réalisation des inspections et des contrôles.

Il existe un protocole de coopération entre les quatre autorités de contrôle fédérales, mais il n'y a pas de tel protocole de coopération avec les entités fédérées et, plus particulièrement avec la Vlaamse Toezichtscommissie. Les différences entre les autorités de contrôle peuvent également entraîner un désavantage concurrentiel dans le secteur des services par rapport à d'autres pays européens (par exemple, dans le marketing direct ou les politiques au niveau des cookies). Il est fait référence au déséquilibre entre les différents niveaux politiques en ce qui concerne l'existence des autorités de contrôle.

D'autre part, le paysage institutionnel de la vie privée est également incomplet en l'absence d'un mécanisme indépendant de contrôle du traitement des données à caractère personnel par les autorités judiciaires. En ne remplissant pas cette obligation, la Belgique ne se conforme pas au RGPD. Toutefois, la spécificité de l'introduction d'un contrôle du fonctionnement des autorités judiciaires exige, tout d'abord, une clarté sur les modalités et la portée de cette obligation, notamment en ce qui concerne la notion de « dans l'exercice des fonctions judiciaires ».

Plus de ressources pour les autorités de contrôle. Il est également préconisé d'allouer des ressources suffisantes aux autorités de contrôle, notamment pour les aider à développer leur rôle de soutien aux responsables du traitement, aux sous-traitants mais aussi aux délégués à la protection des données. Par exemple, il est nécessaire que l'autorité de protection des données élabore des directives pratiques pour répondre aux questions et aux difficultés sur le terrain. Cela devrait également favoriser l'harmonisation de l'interprétation et de l'application des règlements.

Plus généralement, un écart important en termes de ressources entre les différentes autorités de contrôle ou par rapport aux autorités intermédiaires chargées de la protection de la vie privée, telles que le Comité de sécurité de l'information, peut avoir un effet de « distorsion du marché » et donner lieu à une extension de facto des pouvoirs.

Plus de cohérence et de coopération avec les partenaires européens. Il est également préconisé également une coopération plus étroite entre les autorités de contrôle belges et leurs homologues européens et non européens. Les différences d'interprétation des normes européennes créent une incertitude juridique et réduisent l'impact d'une réglementation unifiée.

Un ajustement des compétences procédurales de l'Autorité de protection des données. Il semble également nécessaire d'adapter les procédures applicables à l'exécution de divers pouvoirs par l'Autorité de protection des données, par exemple en termes de droits de la défense (obligation d'être entendu et informé, délais de procédure, etc.).

4. CONCLUSIONS ET RECOMMANDATIONS

Comme le montre le chapitre précédent, un très large éventail de commentaires, de suggestions et de demandes ont été formulés au cours de l'évaluation de la Loi vie privée. En général, il semble y avoir un consensus sur l'importance de la Loi vie privée en tant qu'instrument réglementaire central. Toutefois, l'évaluation a montré que dans certains domaines, des ajustements ou des ajouts sont nécessaires.

Certaines de ces constatations dépassent d'ailleurs le cadre de la Loi vie privée et doivent être analysée sous l'angle de la nécessité d'une véritable politique de gestion des données.

Cette tâche n'incombe pas à une seule autorité. Ce rapport d'évaluation envoie un message à tous ceux qui peuvent jouer un rôle dans le renforcement de la protection des données à caractère personnel de nos citoyens et dans la mise en œuvre d'une politique de gestion des données cohérente et adéquate.

Les recommandations énumérées ci-dessous constituent des lignes directrices pour des mesures politiques dans lesquelles le gouvernement fédéral prendra ses responsabilités en premier lieu. Il s'agit d'une liste non exhaustive de mesures politiques qui devraient être considérées comme prioritaires.

Le cadre européen dans lequel s'inscrit la Loi vie privée doit également être pris en compte. Les possibilités et les limites de l'application de certaines de ces recommandations devront être évaluées au regard du RGPD et, dans une moindre mesure, de la Directive et de la Convention 108(+) du Conseil de l'Europe. Plus encore, la mise en œuvre de certaines recommandations peut s'inscrire dans le cadre d'initiatives européennes, de partenariats avec d'autres États membres de l'Union européenne et peut être l'occasion pour la Belgique de continuer à jouer son rôle de leader au niveau européen comme à l'époque de la mise en place du RGPD. D'autre part, en ce qui concerne les services publics, la mise en œuvre de ces recommandations doit également tenir compte de la spécificité des différentes institutions et, en particulier, des autorités policières et judiciaires, les forces armées pour certaines de leurs missions ainsi que des services de renseignement. Ces derniers sont en effet soumis à des régimes de protection des données distincts.

Dans son ensemble, ces lignes directrices doivent permettre un renforcement significatif de la protection de la vie privée des citoyens.

TRANSPARENCE
1. Apporter les clarifications nécessaires à la Loi vie privée ou mieux encadrer : ✓ certains concepts et terminologies tels que "l'exercice de fonctions juridictionnelles", "le transfert de données à caractère personnel", "les données relatives à la santé", "les services de la société de l'information", "la recherche scientifique", "l'anonymisation", le concept d'"autorité publique" ou la notion de "responsable du traitement". ✓ la possibilité de faire une distinction selon qu'un responsable du traitement relève du secteur privé ou du secteur public et selon les régimes de protection (RGPD, directive ou autre) dont relève un responsable du traitement (selon la nature de l'autorité ou selon le type de traitement des données)

- ✓ certaines obligations supplémentaires par rapport au RGPD, par exemple, dans l'application des dispositions relatives au traitement des données personnelles des mineurs ou en ce qui concerne l'intervention du délégué à la protection des données
- ✓ les passerelles entre les différents régimes de protection des données en fonction de la nature du responsable du traitement
- ✓ la relation avec les concepts ou obligations potentiellement conflictuels entre la Loi vie privée et d'autres lois et droits fondamentaux (par exemple, en ce qui concerne le secret professionnel, la divulgation administrative ou la relation avec le droit pénal)
- ✓ l'application des principes de base de la législation sur la protection des données afin de fournir un cadre plus clair pour les obligations des responsables du traitement et des sous-traitants, notamment en ce qui concerne les mesures techniques et organisationnelles, la minimalisation des données et les périodes de conservation.

Il doit être tenu compte des directives européennes existantes ainsi que la Convention 108(+) du Conseil de l'Europe.

2. Mobiliser des moyens pour promouvoir le débat public sur la vie privée. Une attention particulière doit être accordée à la relation avec les autres droits fondamentaux et au développement et l'impact des nouvelles technologies, big data, de l'intelligence artificielle,...

3. Renforcer les obligations de transparence et de responsabilité des responsables de traitement. En particulier, en ce qui concerne les administrations publiques, un cadastre central devrait fournir une vue d'ensemble des données personnelles traitées, au minimum en ce qui concerne les traitements soumis au RGPD. Les citoyens devraient aussi pouvoir accéder à leurs données à caractère personnel via une plateforme numérique. Les administrations publiques devraient également faire preuve de transparence et de proportionnalité dans leur utilisation des algorithmes. Un registre de transparence sera mis en place à cet effet.

4. Mieux utiliser les outils de soutien et d'orientation fournis par le RGPD et la Loi vie privée. Les responsables du traitement des données et les sous-traitants doivent être mis dans une meilleure position pour se conformer aux règles de confidentialité applicables. L'élaboration de codes de conduite et de mécanismes de certification plus nombreux et axés sur un secteur spécifique (par exemple le monde académique ou la recherche) devrait être au cœur de cette démarche. L'importance du rôle d'orientation, d'information et de soutien des autorités de contrôle peut être soulignée à cet égard. Des lignes directrices spécifiques sur l'utilisation des analyses d'impact sur la vie privée seront développées, si possible en coopération avec les autorités de contrôle.

5. Développer un portefeuille d'identification numérique grâce auquel l'interaction du citoyen avec les organismes privés et publics est organisée de manière simple, accessible et sécurisée.

6. Renforcer l'exercice des droits des personnes concernées en encadrant mieux, entre autres, le droit d'accès et la portabilité des données personnelles. Par ailleurs, le système d'accès indirect aux données à caractère personnel actuellement en vigueur en Belgique devrait être revu.

GOUVERNANCE DES DONNÉES
7. Renforcer dans la Loi vie privée les principes fondamentaux relatives à la protection des personnes physiques à l'égard des traitements de données à caractère personnel , notamment en rendant explicite que les éléments essentiels d'un traitement de données doivent être inclus dans toute réglementation organisant un traitement. Des éclaircissements et des conseils doivent être apportés sur le choix et l'application de la base juridique du traitement des données personnelles. Cela devrait permettre de mieux définir les possibilités et les limites de chaque base juridique et de la finalité du traitement des données.
8. Compléter la Loi vie privée par un cadre pour l'application des règles de protection de la vie privée dans des situations spéciales telles qu'une pandémie, une intervention en cas de crise et une catastrophe humanitaire ou autre et ceci dans le respect de la sauvegarde des droits fondamentaux et des intérêts du citoyen. La Loi vie privée devrait également être dotée d'un cadre juridique spécifique pour le traitement des catégories spéciales de données personnelles, par exemple les données biométriques.
9. Fournir plus de sécurité juridique et de clarté concernant les obligations et les conséquences lors de la mise en place d'échanges internationaux de données avec des acteurs situés en dehors de l'Union européenne. D'une part, dans les limites du cadre européen et entre autres en collaboration avec les autres Etats-Membres de l'Union européenne, le cadre juridique devrait être complété ou au moins clarifié, et d'autre part, davantage de mesures de soutien devraient être développées entre autres pour les petites et moyennes entreprises, qui ne disposent pas toujours des ressources et de l'expertise nécessaires pour faire face à cette complexité.
10. Fournir un cadre juridique explicite sur l'utilisation de "bacs à sable réglementaires" afin de permettre aux responsables du traitement des données de procéder à des essais de traitement des données dans un environnement sécurisé et contrôlé.
11. L'élaboration d'une politique globale de gestion des données qui non seulement prend en compte les données à caractère personnel mais élabore également des mesures concernant les entités juridiques et les données non personnelles. En particulier, l'élaboration d'une politique et d'instruments associés visant à offrir aux citoyens la possibilité d'exercer un contrôle accru et plus efficace sur leurs données personnelles, par exemple au moyen de coffres-forts numériques.

12. Veiller à l'élimination des obstacles à l'application efficace des règles relatives au traitement des données dans le cadre de la recherche scientifique. La facilitation de l'utilisation de données pseudonymisées et anonymisées devrait être au cœur de cette démarche. En particulier, le système des tiers de confiance doit être renforcé.

13. Simplifier les mécanismes administratifs d'échange de données entre organismes publics et entre organismes privés et publics. L'accès aux données publiques doit être organisé de manière plus uniforme, accessible et pragmatique.

ACTEURS INSTITUTIONNELS

14. Clarifier les relations entre la Loi vie privée, la législation sectorielle et la législation fédérée ayant un impact sur le traitement des données à caractère personnel, d'une part, et les relations entre les autorités de contrôle, d'autre part, notamment par le biais d'un accord de coopération entre l'État fédéral, les Communautés et les Régions. Un cadre explicite sur la répartition des compétences doit favoriser une meilleure coordination des mesures politiques et une meilleure coopération entre les autorités dont les autorités de contrôle.

15. Adapter la législation organique des autorités de contrôle fédérales. En particulier et prioritairement, l'indépendance et la bonne gouvernance de l'Autorité de protection des données devrait être renforcée. Le rapport d'audit de la Cour des comptes devrait servir de ligne directrice à cet égard. L'Autorité de protection des données doit pouvoir pleinement exercer ses compétences afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel. Il convient également d'adapter le fonctionnement et les procédures des autorités de contrôle afin qu'elles puissent remplir leurs missions légales de la manière la plus efficace et la plus adéquate possible et qu'elles aient le poids nécessaire pour agir contre les infractions. Les principes de simplification, de rationalisation et de création de synergies devraient être au cœur de cette démarche. Les autorités de contrôle pourraient aussi bénéficier d'une expertise sectorielle en leur sein. Il sera également répondu à l'obligation de mettre en place un mécanisme de contrôle indépendant pour le traitement des données personnelles par l'ordre judiciaire.

16. Mettre davantage l'accent sur une politique d'application efficace et appropriée en cas de non-respect de la législation sur la protection de la vie privée. En particulier, l'application des sanctions pénales devrait être reconsidérée et complétée.

17. Promouvoir une vision large de la protection des données, de l'innovation et du partage des données, fondée sur la fertilisation croisée entre différents domaines d'expertise (sectoriels), la vie privée et la technologie. Cette vision doit également être intégrée dans les structures et le fonctionnement de toutes les parties prenantes. Une culture organisationnelle doit être promue qui accorde l'attention nécessaire à la mise en œuvre d'une politique respectueuse de la vie privée. Les ressources nécessaires doivent être mises à disposition, tant au niveau organisationnel (avec une attention particulière pour l'anonymisation par exemple) qu'en

termes de possibilités de formation. En externe, la communication et la sensibilisation à la politique de confidentialité doivent être renforcées.
18. Afin de pouvoir simplifier les mécanismes administratifs d'échange de données, le paysage institutionnel devra être adapté avec des missions légales claires exercées de manière transparente. En particulier, le rôle et le fonctionnement du Comité de sécurité de l'information devraient être adaptés pour soutenir davantage les politiques gouvernementales de gestion des données, sans préjudice du rôle et du compétences des autorités de contrôle à l'égard des décisions du Comité de sécurité de l'information.
19. Améliorer encore le fonctionnement des intégrateurs de services afin qu'ils puissent renforcer leur rôle de facilitateur en matière d'échanges de données. À cette fin, l'accès aux sources authentiques devrait également être mieux encadré, simplifié et élargi. L'intensification des échanges de données ne peut également être pleinement réalisée que si l'accès aux sources authentiques est gratuit.
20. Élaborer des lignes directrices spécifiques sur le rôle, le statut et les tâches des délégués à la protection des données. En outre, une politique de soutien devrait être mise en œuvre pour permettre aux petites organisations de remplir leurs obligations légales, par exemple en promouvant la possibilité de "mutualiser" les délégués à la protection des données.