Les Cahiers de droit

L'évaluation des facteurs relatifs à la vie privée : pour un équilibre entre l'objectif de protection des renseignements personnels et la responsabilité des entreprises

Serge Kablan, Arthur Oulaï and Patrick Mignault

Volume 64, Number 2, June 2023

URI: https://id.erudit.org/iderudit/1101118ar
DOI: https://doi.org/10.7202/1101118ar

See table of contents

Publisher(s)

Faculté de droit de l'Université Laval

ISSN

0007-974X (print)
1918-8218 (digital)

Explore this journal

Cite this article

Kablan, S., Oulaï, A. & Mignault, P. (2023). L'évaluation des facteurs relatifs à la vie privée : pour un équilibre entre l'objectif de protection des renseignements personnels et la responsabilité des entreprises. *Les Cahiers de droit*, *64*(2), 397–437. https://doi.org/10.7202/1101118ar

Article abstract

Québec recently passed Law 25, which modernizes the protection of personal information in various acts, including the Act respecting the protection of personal information in the private sector. Among the new obligations imposed upon businesses is the requirement to conduct a privacy impact assessment (PIA). This article explores the PIA by examining the situations in which such an assessment is required and by outlining some elements that will help us understand its method and implementation. The study of the contours of this new obligation, illustrated by the development and operation of financial technology, reveals an imposing burden for businesses. At the same time, the study shows that the widespread use of PIAs contrasts with the lack of legislative guidance. The authors argue for a more balanced and informed obligation.

L'évaluation des facteurs relatifs à la vie privée : pour un équilibre entre l'objectif de protection des renseignements personnels et la responsabilité des entreprises

Serge Kablan*, Arthur Oulaï** et Patrick Mignault***

Le Québec a récemment adopté la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels *qui, comme son titre l'indique, modernise la protection des renseignements personnels dans diverses lois, incluant la* Loi sur la protection des renseignements personnels dans le secteur privé. *Parmi les nouvelles obligations imposées aux entreprises figure l'obligation de réaliser une évaluation des facteurs relatifs à la vie privée (EFVP). Le présent texte explore l'EFVP en examinant, d'une part, les situations dans lesquelles une telle évaluation est requise et en esquissant, d'autre part, quelques éléments permettant d'en comprendre la méthode et la réalisation. L'étude des contours de cette nouvelle obligation, illustrée par le développement et l'exploitation d'une technologie financière, dévoile un fardeau imposant pour les entreprises. En même temps, l'étude permet de constater que la généralisation de l'EFVP contraste avec l'absence de balises législatives. Les auteurs plaident pour une obligation plus équilibrée et mieux éclairée.*

* Professeur de droit, Faculté des sciences de l'administration, Université Laval.
** Professeur, Faculté de droit, Université de Sherbrooke.
*** Professeur, Faculté de droit, Université de Sherbrooke.
Le présent article a bénéficié du soutien financier de la Chaire Fintech AMF – Finance Montréal. Article mis à jour le 18 mai 2023.
En vertu des règles linguistiques de la revue, l'utilisation de la seule forme masculine vise à alléger le texte et, selon les circonstances, elle désigne aussi bien les femmes que les hommes.

Québec recently passed Law 25, which modernizes the protection of personal information in various acts, including the Act respecting the protection of personal information in the private sector. Among the new obligations imposed upon businesses is the requirement to conduct a privacy impact assessment (PIA). This article explores the PIA by examining the situations in which such an assessment is required and by outlining some elements that will help us understand its method and implementation. The study of the contours of this new obligation, illustrated by the development and operation of financial technology, reveals an imposing burden for businesses. At the same time, the study shows that the widespread use of PIAs contrasts with the lack of legislative guidance. The authors argue for a more balanced and informed obligation.

La provincia de Québec ha adoptado recientemente la ley número 25, la cual moderniza la protección de datos personales, vigente en distintas leyes, incluyendo la Loi sur la protection des renseignements personnels dans le secteur privé (Ley de Protección de Datos Personales en el Sector Privado). Entre las nuevas obligaciones que se le imponen a las empresas está la de realizar una Evaluación de Impacto en la Privacidad (PIA), que este texto examina. Se analizan, por una parte, las situaciones en las cuales se requiere de dicha evaluación y, por otra parte, se realiza un bosquejo de algunos elementos que permiten comprender el método y la ejecución. El estudio de la amplitud de esta nueva obligación, ilustrada por el desarrollo y la explotación de una tecnología financiera, ha revelado una carga imponente para las empresas. Al mismo tiempo, el estudio ha permitido constatar que la generalización de una Evaluación de la Protección de Datos Personales contrasta con la ausencia de lineamientos legales. En el texto, los autores abogan por una obligación más equilibrada y más clara.

Pages

1 Le contexte de l'évaluation des facteurs relatifs à la vie privée 403

1.1 Les projets de système d'information ou de prestation électronique de services 403

1.2 La communication d'un renseignement personnel à l'extérieur du Québec.. 416

2 La méthode et la réalisation de l'évaluation des facteurs relatifs à la vie privée : quelques éléments utiles 422
2.1 De l'approche minimalise de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25) 422
2.2 Les modalités de l'évaluation des facteurs relatifs à la vie privée 426
2.2.1 La description des opérations de traitement envisagées et leurs finalités 426
2.2.2 L'évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités 428
2.2.3 L'évaluation et la gestion des risques pour les droits et libertés des personnes concernées 433
Conclusion 437

Les fuites de renseignements personnels se sont multipliées ces dernières années. Il s'agit, pour certains, d'une « série noire appelée à se poursuivre[1] ». L'affaire de la Fédération des caisses Desjardins du Québec impliquant quelque 4,2 millions de victimes a fait parler de « crise », d'abord au sein du Mouvement lui-même[2], et sans doute aussi dans une société civile médusée par la pénétrabilité du bouclier censé préserver le secret de ses données. Or, les États sont confrontés à un enjeu bien plus grand, celui des mégadonnées dont le volume a soudainement grossi avec l'accroissement des flux d'information générés par des populations que l'on a astreintes à des confinements répétés pour tenter de juguler la pandémie de la maladie à coronavirus (COVID-19)[3]. Les données qu'elles ont ainsi produites (qu'elles les aient sciemment téléversées dans le cyberespace, notamment par le biais des médias sociaux, ou qu'elles aient été

1. Voir l'article de Jean-Michel G. Gagnon, « Vol de renseignements personnels : une série noire appelée à se poursuivre », *Le Journal de Québec*, 8 août 2019, [En ligne], [www.journaldequebec.com/2019/08/08/une-serie-noire-appelee-a-se-poursuivre] (17 mai 2023).
2. Voir l'article de Tristan Péloquin et Hugo Pilon-Larose, « Vol de données chez Desjardins : 4,2 millions de victimes », *La Presse*, 2 novembre 2019, [En ligne], [www.lapresse.ca/actualites/justice-et-faits-divers/2019-11-02/vol-de-donnees-chez-desjardins-4-2-millions-de-victimes] (16 avril 2023).
3. Anja Feldmann et autres, *The Lockdown Effect : Implications of the COVID-19 Pandemic on Internet Traffic*, ACM Internet Measurement Conference (IMC '20), New York, 27-29 octobre 2020, [En ligne], [dl.acm.org/doi/pdf/10.1145/3419394.3423658] (16 avril 2023).

captées lors de leurs pérégrinations en ligne) cachent des habitudes, des comportements, des profils, des besoins, des tendances, des prédictions, des occasions d'affaires, etc., que les entreprises avisées ont rapidement détectés et valorisés, grâce à des outils de collecte et d'analyse dont Google Trends, d'autant plus puissant qu'il permet de « découvrir [de manière presque synchrone] ce que cherchent les internautes du monde entier[4] ».

Ceci met au premier plan à la fois le pouvoir des algorithmes et la question de leur gouvernance. Mais surtout, ce contexte rend la réforme du cadre législatif inéluctable, poussée par l'indispensabilité de règles plus adaptées aux enjeux de la société de l'information et capables de garantir au consommateur le contrôle de ses données. Au Québec, le projet de loi nº 64[5] poursuit cet objectif. Il a été adopté et sanctionné respectivement le 21 et le 22 septembre 2021 et vise à moderniser la protection des renseignements personnels dans diverses lois, incluant la *Loi sur la protection des renseignements personnels dans le secteur privé*[6]. Cette dernière fait l'objet de la présente analyse. L'entrée en vigueur des nouvelles dispositions est en cours et sera complétée en 2024.

La réforme québécoise est inspirée du *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (RGPD)[7]. Cela suppose, à terme, une protection au moins équivalente à l'égard « des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil[8] ». La Loi sur le secteur privé définit le renseignement personnel comme tout renseignement, c'est-à-dire tout élément d'information ou toute indication (statut social, origine ethnique,

4. Google, « Aide Google Tendance des recherches », [En ligne], [support.google.com/trends/answer/6248105 ?hl=fr] (16 avril 2023).
5. *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, projet de loi nº 64 (sanctionné – 22 septembre 2021), 1re sess., 42e légis. (Qc) ; L.Q. 2021, c. 25 (ci-après « Loi 25 »).
6. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c. P-39.1 (ci-après « Loi sur le secteur privé »).
7. *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, J.O.U.E. nº L 119/1, 4 mai 2016 (ci-après « RGPD »).
8. Loi sur le secteur privé, préc., note 6, art. 1 al. 1.

comportement disciplinaire, etc.)[9] qui peut, de façon directe ou indirecte, être relié à une personne physique et permettre de l'identifier, peu importe le support de ce renseignement et la forme sous laquelle il est accessible (forme écrite, graphique, sonore, visuelle, informatisée ou autre)[10]. De son côté, le législateur européen emploie les termes « donnée à caractère personnel » pour désigner toute information se rapportant à une personne physique identifiée ou qui peut l'être, directement ou indirectement, notamment par référence à un identifiant (nom, numéro d'identification, données de localisation, identifiant en ligne) ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[11].

Il y a plus que la similitude de ces définitions. Au Québec, la modernisation de la protection des renseignements personnels repose, notamment, sur une obligation accoutumée au droit européen, laquelle est en partie énoncée à l'entame de la Loi sur le secteur privé, à l'article 3.3 al. 1 (nouveau). Cet article impose la réalisation d'une évaluation des facteurs relatifs à la vie privée (EFVP) dans le cadre des projets de système d'information ou de prestation électronique de services. Deux autres situations sont envisagées dans la Loi sur le secteur privé : l'exigence d'une EFVP avant de pouvoir communiquer un renseignement personnel à l'extérieur du Québec (nouvel article 17) et la nécessité de cette évaluation afin de pouvoir communiquer un tel renseignement sans le consentement de la personne concernée, aux fins d'étude, de recherche ou de production de statistiques (nouvel article 21).

Si l'exigence de l'EFVP n'est pas inédite, étant notamment prévue dans le RGPD, l'antériorité de ce règlement européen offre un élément de comparaison irrésistible. En particulier, nous proposons de confronter l'approche de la nouvelle version de la Loi sur le secteur privé à celle du RGPD. L'implémentation d'une solution putative de technologie financière par une entreprise de compétence provinciale, dans le cadre d'un système

9. Dans le langage courant est un *renseignement* tout « élément d'information, indication destinée à faire connaître quelque chose ou quelqu'un » : *Dictionnaire de l'Académie française*, 9e éd., s.v. « Renseignement », [En ligne], [www.dictionnaire-academie.fr/] (16 avril 2023) (ci-après « DAC »).

10. Loi sur le secteur privé, préc., note 6, art. 1 al. 2 et art. 2 (nouveau). L'art. 2 (nouveau) ajoute les mots « directement ou indirectement » à la définition du renseignement personnel. Cette disposition entrera en vigueur le 22 septembre 2023. L'article 1 al. 5 de la Loi précise que les sections II (dispositions concernant la collecte des renseignements personnels) et III (dispositions concernant le caractère confidentiel des renseignements personnels) ne s'appliquent pas au renseignement qui a un caractère public en vertu de la Loi. Voir aussi l'article 100 de la Loi 25, préc., note 5.

11. RGPD, préc., note 7, art. 4 (1).

bancaire ouvert, servira à illustrer cette étude comparée. Par technologie financière, on entend l'« [e]nsemble des technologies numériques les plus évoluées et les plus récentes utilisées pour améliorer les services financiers et bancaires[12] », incluant des sous-secteurs aussi diversifiés et complexes que celui de la chaîne de blocs, des logiciels financiers, de l'ingénierie financière ou de la cryptomonnaie. Ces sous-secteurs ne sont pas en soi notre centre d'attention : nous nous concentrerons plutôt sur les données ou les renseignements personnels des consommateurs auxquels tous s'abreuvent et dont le traitement est rattrapé par la Loi 25. Notre ambition est binaire : elle est pragmatique, à savoir identifier et étayer des façons de résoudre les défis auxquels les entreprises assujetties à la Loi 25 pourraient être confrontées dans la réalisation de l'EFVP. Notre ambition a aussi son lot d'idéalisme, recherchant l'équilibre parfait entre l'objectif de protection des renseignements personnels et la responsabilité des entreprises. La thèse que nous défendons est certes favorable à l'EFVP, qui apparaît comme un exercice opportun dans le contexte. Mais, dans la réalisation de cette EFVP, le fardeau que la Loi impose aux entreprises nous semble dépasser la juste mesure, tantôt en raison d'imprécisions dans la Loi, tantôt sous l'effet de contraintes en excès de ce qui est nécessaire pour protéger les renseignements personnels. Dans la mesure où cette opinion est démontrée, le recalibrage de l'exigence de l'EFVP serait une recommandation logique, réalignement qui peut s'opérer soit par le truchement de lignes directrices inspirées d'initiatives étrangères, soit directement par action législative (entendue notamment de la révision de la Loi), à moins de privilégier la combinaison des deux.

Ce double objectif à l'esprit, il convient, dans un premier temps, de définir le contexte ou l'objet de l'EFVP (partie 1). Dans un second temps, il faut s'intéresser à la technique ou au procédé de sa réalisation (partie 2). Afin d'incarner notre propos, nous imaginerons le développement et l'exploitation d'une application mobile d'optimisation financière. Étant donné que nous nous appuyons sur la Loi 25 et le RGPD comme références pour l'analyse, nous ne nous concentrerons que sur le traitement des renseignements personnels que l'application pourrait effectuer et pour lequel une EFVP est requise. Il est important de noter que les nouvelles

12. Office québécois de la langue française, *Le grand dictionnaire terminologique*, s.v. « Technologie financière », [En ligne], [vitrinelinguistique.oqlf.gouv.qc.ca/] (16 avril 2023) (ci-après « GDT »). Pour illustration, voir Walo, *L'application & la Carte qui préparent vos enfants à l'indépendance financière*, [En ligne], [https://wealthica.com/fr/a-propos/] (17 mai 2023), qui « fournit des applications et des outils financiers novateurs pour permettre aux consommateurs de prendre de meilleures décisions financières et de mieux contrôler leur vie financière ».

obligations concernant l'EFVP ne sont pas exclusives aux solutions de technologie financière.

1 Le contexte de l'évaluation des facteurs relatifs à la vie privée

Le contexte de l'EFVP désigne les situations où cette évaluation est requise. L'examen que nous entreprenons concerne les contextes décrits aux articles 3.3 et 17 précités. L'exigence d'une EFVP dans le cadre de l'article 21, soit le cas concernant la communication de renseignements personnels aux fins d'études, de recherche ou de production de statistiques n'est pas abordée ici[13].

1.1 Les projets de système d'information ou de prestation électronique de services

Le nouvel article 3.3 al. 1 de la Loi sur le secteur privé énonce la règle suivante :

> Toute personne qui exploite une entreprise doit procéder à une évaluation des facteurs relatifs à la vie privée de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.

Un projet, selon le *Dictionnaire de l'Académie française*, est « [un] dessein, [une] intention qu'on a de réaliser quelque entreprise, et qui prend en compte les moyens utiles à sa mise en œuvre[14] » ; c'est « ce que l'on se propose d'accomplir[15] ». La définition que donne le *Dictionnaire de management de projet* met davantage en exergue les principales caractéristiques des projets, soit la satisfaction d'une demande ou d'un besoin, la détermination d'objectifs spécifiques, des paramètres temporels, le caractère d'unicité de l'initiative, la novation, la mobilisation de ressources et la nécessité de structures organisationnelles affectées à l'initiative. Le projet est ainsi décrit comme un « [p]rocessus unique qui consiste en un ensemble d'activités coordonnées et maîtrisées comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant les contraintes de délais, de coûts et de ressources (ISO 10006)[16] ». Selon l'article 3.3 précité, toute personne qui s'engage

13. Nous laissons l'article 21 hors du présent texte pour privilégier les contextes qui ont un lien plus immédiat avec l'exemple de l'application mobile d'optimisation financière.
14. DAC, préc., note 9, *s.v.* « Projet ».
15. *Id.*
16. Association francophone de management de projet (AFITEP), *Dictionnaire de management de projet*, Paris, Afnor, 2010, s.v. « Projet », p. 211.

dans un tel processus dans le cadre d'une entreprise qu'elle exploite[17] est tenue de réaliser une EFVP au départ de ce processus, c'est-à-dire aussi tôt qu'elle a l'idée d'un projet, voire à compter de l'avant-projet[18]. Cette évaluation, au sens de la Loi, porte sur le projet et elle est requise lorsque celui-ci concerne l'acquisition, le développement ou la refonte d'un *système d'information* ou la *prestation électronique de services* impliquant le traitement[19] de renseignements personnels.

Le *système d'information* et la *prestation électronique de services* ne sont pas définis dans la Loi sur le secteur privé. On est ainsi porté à considérer le sens commun des concepts. Selon *Le grand dictionnaire terminologique*, de l'Office québécois de la langue française, un *système d'information* (SI) est l'« [e]nsemble structuré de tous les éléments qui contribuent à la gestion de l'information dans une entreprise, dont les ressources matérielles, techniques, financières, humaines, intellectuelles ou autres, que cet ensemble soit informatisé ou non, en totalité ou en partie[20] ». Comme en administration publique, la *prestation électronique de services* (PES) consiste, en l'occurrence pour une entreprise, à prester des services aux consommateurs par l'intermédiaire d'Internet[21]. Au sens de la Loi (nouvel article 3.3), *tout* projet d'acquisition, de développement ou de refonte de SI ou de PES doit[22] subir une EFVP par cela même que tel projet implique la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels[23]. L'*acquisition* s'entend normalement de l'action d'acquérir une chose, c'est-à-dire de l'obtenir pour soi par transfert de propriété, licence d'utilisation, etc. ; le *développement* est un processus comprenant généralement l'analyse des besoins,

17. La notion d'*entreprise* a, en l'espèce, le sens de l'article 1525 al. 3 du *Code civil du Québec*, L.Q. 1991, c. 64 (voir l'article premier de la Loi sur le secteur privé, préc., note 6) : « Constitue l'exploitation d'une entreprise l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services. »
18. Le terme *projet* peut en effet désigner la « totalité du phasage (depuis l'idée de projet jusqu'à sa terminaison) » ou uniquement « la phase de réalisation du projet, la phase préalable étant alors qualifiée d'avant-projet ».
19. Dans notre texte, nous entendons par « traitement » la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
20. GDT, préc., note 12, s.v. « Système d'information d'entreprise ».
21. *Id.*, *s.v.* « Prestation électronique de services ».
22. L'indicatif présent du verbe « devoir » est employé dans la disposition : « Toute personne qui exploite une entreprise *doit procéder* à [ou est tenue, par obligation, de procéder à] une évaluation des facteurs relatifs à la vie privée » (Loi sur le secteur privé, préc., note 6, art. 3.3 (nouveau)).
23. *Id.*

la spécification, la conception du système, la programmation, le déploiement et la maintenance[24] ; quant à la *refonte*, elle appelle un remaniement complet, une réingénierie ou une révision qui affectent la conception du système. S'agissant d'un logiciel par exemple, la refonte pourrait inclure la mise à niveau, mais probablement pas la mise à jour ordinaire[25].

La pertinence de certaines de ces définitions générales est discutable, du moins dans le contexte d'un renforcement de la protection des renseignements personnels. D'abord, il faut se demander si, suivant la réforme de la Loi sur le secteur privé, le SI peut ou doit être interprété comme incluant les ensembles non informatisés. La question est inévitable une fois que le législateur affiche un objectif de modernisation de la Loi, lequel suppose la promotion de règles adaptées aux besoins de l'époque actuelle (on sous-entend que les ensembles non informatisés appartiennent à une autre époque). D'un autre côté, la définition de la PES est imprécise, comparée à celle du « service » ou du « service de la société de l'information » dans le RGPD. Pour définir ce type de services, l'article 4 (25) du RGPD renvoie à l'article 1 (1) (b) de la directive (UE) 2015/1535 du Parlement européen et du Conseil. En l'espèce, il est question de « tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services[26] ». Le mode « à distance » s'entend du service qui est fourni sans que les parties qui sont impliquées soient simultanément présentes[27]. La « voie électronique » suppose le recours à des équipements spécifiques, capables de traiter des données, de les stocker ou de les transmettre, les acheminer et les recevoir[28]. L'expression

24. GDT, préc., note 12, *s.v.* « Cycle de vie du développement logiciel » ; « Développement logiciel ».
25. *Id.*, *s.v.* « Refonte ». Selon le GDT, préc., note 12, la « mise à jour » est l'« [o]pération consistant à déployer une version d'un logiciel qui comporte des corrections ou des modifications mineures par rapport à la version précédente ». Quant à la « mise à niveau », elle est l'« [o]pération consistant à améliorer les fonctionnalités d'un logiciel, ou encore à en ajouter ou à en retirer, et à y apporter des modifications majeures ».
26. *Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société d'information (texte codifié)*, J.O.U.E. nº L 241/1, 17 septembre 2015, art. 1 (1) (b) (ci-après « Directive (UE) 2015/1535 »).
27. L'annexe I de la Directive (UE) 2015/1535, préc., note 26, donne une liste indicative de services qui ne sont pas considérés comme des services fournis à distance, par exemple les services qui sont prestés en présence physique du prestataire et du destinataire, mais qui impliquent l'utilisation de dispositifs électroniques.
28. Il est précisément question du « service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu

« à la demande individuelle d'un destinataire de services » signifie que le service est fourni par transmission de données sur demande individuelle[29]. Cette méticulosité du RGPD, qui a l'avantage de circonscrire la portée matérielle de la réglementation, a manqué à la nouvelle mouture de la Loi sur le secteur privé.

Mais surtout, l'objet de ce que le législateur européen appelle « analyse d'impact relative à la protection des données » (AIPD) n'est pas systématiquement *tout* projet d'acquisition, de développement ou de refonte relatif à un service de la société de l'information ou à un SI et comportant le traitement de données à caractère personnel[30]. Seuls certains types d'opérations de traitement sont visés. Pour celles-ci, l'AIPD doit être « lancée le plus tôt possible dans le cycle de conception du traitement[31] ». Le législateur a dans sa mire les opérations de traitement qui, en raison de leur nature, de leur portée, de leur contexte et de leur finalité, sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques[32]. La définition du risque est précise : il s'agit d'un « scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité[33] ». Sont notamment concernés les types d'opérations de traitement qui reposent sur de « nouvelles technologies » ou ceux « qui sont

---

par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques » : Directive (UE) 2015/1535, préc., note 26, art. 1 (1) (b) (ii). Toutefois, la consultation d'un médecin ou d'un avocat par téléphone ou télécopieur, le marketing direct par téléphone ou télécopieur, les services prestés par téléphonie vocale ou télécopieur, la distribution automatique de billets, etc., ne sont pas considérés comme des services fournis par voie électronique (*id.*, annexe I).

29. *Id.*, point 3 : les services non fournis « *à la demande individuelle d'un destinataire de services* » incluent ceux administrés « par l'envoi de données sans appel individuel et destinés à la réception simultanée d'un nombre illimité de destinataires (transmission de « point à multipoint ») » comme les services de radiodiffusion télévisuelle ou les services de radiodiffusion sonore.

30. Nonobstant, toute activité de traitement doit faire l'objet d'une évaluation (générale) continue de façon à permettre au responsable du traitement d'identifier quel type de traitement est susceptible d'engendrer un risque élevé. Voir : RGPD, préc., note 7, art. 35 ; Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 – Adoptées le 4 avril 2017, telles que modifiées et adoptées en dernier lieu le 4 octobre 2017*, 17/FR WP 248 rév. 01, p. 7, [En ligne], [www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf] (ci-après « Lignes directrices concernant l'AIPD »).

31. *Id.*, p 17.

32. RGPD, préc., note 7, art. 35 (1) ; Lignes directrices concernant l'AIPD, préc., note 30, p. 17.

33. Lignes directrices concernant l'AIPD, préc., note 30, p. 7.

nouveaux et pour lesquels aucune analyse d'impact relative à la protection des données n'a été effectuée au préalable par le responsable du traitement, ou qui deviennent nécessaires compte tenu du temps écoulé depuis le traitement initial »[34]. La liste des types d'opérations de traitement pour lesquelles une AIPD est requise est établie et publiée par l'autorité de contrôle. Cette dernière peut indiquer, de la même façon, les types d'opérations pour lesquelles une AIPD n'est pas demandée[35].

En ciblant les types d'opérations de traitement en fonction des risques qu'ils présentent pour les droits et libertés des personnes physiques (principalement, les risques pour les droits à la protection des données et à la vie privée ; le cas échéant, les risques pour la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté et la liberté de conscience et de religion)[36], le règlement européen rompt avec l'ancienne approche de la directive 95/46/CE[37], jugée peu efficace, qui imposait une obligation générale sans distinction de notifier tous les traitements aux autorités de contrôle. L'on réprouve, en particulier, la charge administrative et financière que cette obligation a générée sans systématiquement améliorer la protection des données à caractère personnel[38].

Au Québec, la Loi 25 a précipité les entreprises sur ce sentier (généraliste) abandonné (car peu efficace) en soumettant à une EFVP « tous » les projets d'acquisition, de développement et de refonte de SI ou de PES impliquant le traitement de renseignements personnels. La mise en œuvre de cette obligation est en soi un défi, en l'occurrence pour les très petites entreprises (TPE) ainsi que les petites et moyennes entreprises (PME) ; l'approche généraliste de la Loi québécoise est d'autant plus contraignante qu'elle requiert une expertise pluridisciplinaire que les entreprises devront immanquablement développer ou s'adjoindre pour pouvoir évaluer chacun des projets visés et maintenir cette évaluation à jour (le fardeau financier est probablement à craindre). Le défi concerne d'ailleurs aussi les autorités de contrôle elles-mêmes, compte tenu de l'importance de la charge administrative et financière corrélative à l'obligation imposée aux entreprises.

34. RGPD, préc., note 7, considérant nº 89.
35. *Id.*, art. 35 (5) et (10).
36. Lignes directrices concernant l'AIPD, préc., note 30.
37. *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, J.O.U.E. nº 281/31, 23 novembre 1995 (ci-après « Directive 95/46/CE »).
38. RGPD, préc., note 7, considérant nº 89.

Au demeurant, que l'on considère l'approche généraliste de la nouvelle version de la Loi sur le secteur privé ou la démarche spécialisée du RGPD, certaines initiatives, comme l'implantation d'un système bancaire ouvert, rendent inévitable l'EFVP ou l'AIPD. Le bien-fondé d'un tel système, au Canada, a fait l'objet d'un rapport sénatorial en 2019[39] duquel il est ressorti que les États, en adoptant un système bancaire ouvert, établissent notamment un cadre qui permet au consommateur d'avoir accès à ses données financières personnelles et de les contrôler. Il s'agit, de toute évidence, de retirer aux institutions financières individuelles la mainmise sur le flot de données que génère le consommateur dans ses opérations bancaires quotidiennes[40].

Cela suppose, d'une part, la portabilité de ces données ; autrement dit, le droit du consommateur de décider celles dont il veut autoriser la transmission de sa banque vers un tiers fournisseur (soit une entreprise de technologie financière ou une autre). D'autre part, le système bancaire ouvert favorise l'accès transparent à des services d'initiation de paiement[41]. Pour des raisons liées notamment à la sécurité des données, les interfaces de programmation d'application (*application programming interface* ou API)[42] sont le canal de communication privilégié au sein d'un tel système bancaire[43]. L'interface API Google

39. Canada, Sénat, *Un système bancaire ouvert, qu'est-ce que cela signifie ?*, rapport du Comité permanent des banques et du commerce (BANC), juin 2019, [En ligne], [publications.gc.ca/collections/collection_2019/sen/yc11-0/YC11-0-421-32-fra.pdf], (16 avril 2023) (ci-après « rapport BANC »).

40. Canada, Ministère des Finances, *Examen des mérites d'un système bancaire ouvert*, document de consultation, janvier 2019, [En ligne], [publications.gc.ca/collections/collection_2019/fin/F2-266-1-2019-fra.pdf] (16 avril 2023).

41. L'initiation de paiement est « [la possibilité pour le consommateur] de faire des paiements directement à partir d'un compte bancaire à l'aide d'une application pour téléphone intelligent plutôt qu'au moyen d'une carte de débit ou de crédit » : rapport BANC, préc., note 39, p. 7.

42. *Id.* Une interface API est un logiciel intermédiaire permettant à deux applications de communiquer entre elles. Elle sert de point d'accès universel par lequel l'information est extraite d'une base de données. Les API constituent la principale solution technologique permettant l'échange sécurisé de données entre une banque et un fournisseur tiers dans le cadre d'un système bancaire ouvert.

43. *Id.*, p. 7 et 11. Cette solution logicielle est préférée à la capture de données d'écran (ou grattage d'écran) qui, bien qu'elle soit utilisée par près de 4 millions de Canadiens au moyen de services d'agrégation de données, présente des risques pour la sécurité des coordonnées de connexion bancaires et de données financières du consommateur. La capture de données d'écran est le « processus par lequel on accède aux données bancaires au moyen de certaines applications pour téléphones intelligents. Des entreprises de technologie financière utiliseront l'identifiant de connexion aux services bancaires en ligne d'un client pour accéder au compte bancaire de ce dernier afin de

Apigee[44], considérée comme une plateforme fédératrice, est une figure de proue de la gestion du cycle de vie des API[45]. Sa variante du secteur bancaire (Apigee Open Banking APIx) permet aux entreprises de créer des écosystèmes où elles peuvent regrouper et intégrer l'ensemble des interfaces API nécessaires au partage sécuritaire des données bancaires des consommateurs[46].

Imaginons un fournisseur de technologie financière participant à ce partage de données, par exemple le concepteur et l'opérateur d'une application mobile d'optimisation des finances personnelles. Ce fournisseur pourrait nourrir l'ambition d'offrir au consommateur des produits ou des services qui lui sont adaptés, incluant l'octroi de financement. Le raffinement des propositions, leur justesse, dépendra notamment de la puissance et de la sophistication des technologies sur lesquelles repose le traitement des données auxquelles ce fournisseur aura eu accès, surtout si ce traitement doit recouper des données provenant de sources secondaires (par exemple, d'infonuages privés ou publics, de l'Internet des objets, d'applications partenaires, etc.). À ce chapitre, les méthodes comme l'apprentissage automatique (supervisé, non supervisé, profond, etc.)[47]

---

recueillir et de stocker les informations relatives à son compte et à son historique de transactions ». Ce qu'il advient des coordonnées de connexion ainsi capturées n'est pas clair (le rapport sénatorial évoque un risque accru de vol d'identité et de fraude, des menaces à la cybersécurité, un processus requérant énormément de ressources et l'incapacité du client à contrôler l'étendue ou la durée de l'accès aux données). Les API utilisent un mécanisme d'authentification différent, qui n'implique pas la conservation de ces coordonnées de connexion. Voir aussi Canada, Sénat, *Témoignage*, Comité sénatorial permanent des banques et du commerce, 1re sess., 42e légis., fascicule no 51, 20 février 2019. Voir également Brett Stuckey et Adriane Yong, *Le système bancaire ouvert – Publication no 2019-42-F*, Ottawa, Bibliothèque du Parlement, 2020, p 2.

44. Google, « Gestion des API Apigee », [En ligne], [cloud.google.com/apigee] (16 avril 2023).

45. Paolo Malinverno et autres, *Gartner Magic Quadrant for Full Life Cycle API Management*, 22 septembre 2020, [En ligne], [www.gartner.com/en/documents/3990768] (16 avril 2023).

46. Ceci inclut des API relatives aux transferts de paiement, celles concernant les informations de compte, l'historique des transactions, les fonds disponibles, les produits financiers, etc.

47. Selon le GDT, préc., note 12, l'apprentissage automatique est un « mode d'apprentissage par lequel un agent [entité physique ou virtuelle] évalue et améliore ses performances et son efficacité sans que son programme soit modifié, en acquérant de nouvelles connaissances et aptitudes à partir de données et/ou en réorganisant celles qu'il possède déjà ». Le dictionnaire ajoute qu'« [u]ne application concrète de l'apprentissage automatique peut consister, pour un logiciel, à faire des prédictions et à rendre des décisions à partir de données, et ce, sans intervention humaine ».

ou, plus généralement, les solutions d'intelligence artificielle (IA)[48] s'imposent, car elles peuvent permettre de profiler le consommateur, de connaître de façon rigoureuse ses besoins et la manière de les satisfaire, d'anticiper ou de prédire ses actions[49]. L'IA serait ainsi une adjuvante redoutable, si ce n'est une pièce maîtresse de l'analyse du comportement. Le projet Covid Global Confinement Emotion aNalysis (COVGEN), qui explore l'ensemble des gazouillis échangés sur la planète entre mars 2020 et mars 2021 pour comprendre les émotions des millions de personnes en confinement[50], rappelle de manière emphatique que l'IA s'embarrasse peu du volume des données à traiter et de la vélocité anticipée dans ce traitement.

Si nous considérons le scénario du fournisseur de technologie financière selon une perspective québécoise, le développement de l'application mobile citée abstractivement subirait une EFVP dès le début du projet[51], dans la mesure où cette application mobile concerne une prestation électronique de services impliquant le traitement de renseignements personnels. Or, la finalité de cette évaluation n'apparaît pas de manière évidente dans la Loi sur le secteur privé. Qu'entend-on par « vie privée » dans le contexte ? Veut-on davantage définir ou connaître autant les impacts négatifs du projet sur les phénomènes personnels que les réponses aux risques dont le projet peut ou doit bénéficier ? S'agit-il d'apprécier la conformité du projet de SI ou de PES aux règles concernant la vie privée ? En l'espèce, l'unique indication au sujet de la finalité de l'EFVP se trouve à l'article 3.4 (nouveau), qui prévoit que le responsable de la protection des renseignements personnels peut, à toute étape d'un projet de SI ou de PES (ce qui inclut normalement l'EFVP), « suggérer des mesures de protection des renseignements personnels applicables à ce projet ». À la suite de l'EFVP,

48. Voir un exemple des produits d'intelligence artificielle et d'apprentissage automatique : Google, « Produits d'IA et de machine learning », [En ligne], [cloud.google.com/products/ai#tab1] (16 avril 2023).

49. Voir Institut canadien des actuaires, *Modélisation prédictive. Transformer les mégadonnées en grandes possibilités*, document 218081, [En ligne], [www.cia-ica.ca/docs/default-source/2018/218081f.pdf] (16 avril 2023).

50. Le projet est dirigé par Rita Orji (Persuasive Computing Lab) et Stan Matwin (Institute for Big Data Analytics), de la Faculty of Computer Science, à la Dalhousie University, à Halifax, au Canada : COVGEN, *Covid Global confinement Emotion aNalysis (COVGEN)*, [En ligne], [covgen.github.io/DalCOVGEN/] (16 avril 2023).

51. Ce moment de l'évaluation est déduit de l'article 3.3 al. 2 (nouveau) qui dispose que, « *[a]ux fins de cette évaluation, la personne doit consulter, dès le début du projet*, son responsable de la protection des renseignements personnels » (l'italique est de nous).

l'entreprise est appelée à identifier et à choisir des réponses aux risques mis en évidence lors de l'exercice, en tenant compte de la Loi.

Concrètement, les entreprises trouveront un cadre d'analyse plus précis dans une pluralité d'instruments dont deux retiennent notre attention : d'une part, elles peuvent se référer aux *Guidelines for Privacy Impact Assessment* publiées par l'Organisation internationale de normalisation (norme ISO/IEC 29134)[52]. D'autre part, et peut-être de manière plus spécifique, elles voudront considérer le *Guide d'accompagnement — Réaliser une évaluation des facteurs relatifs à la vie privée* dont une version de travail datée du 10 mars 2021 a été rendue publique par la Commission d'accès à l'information (CAI)[53]. Cette version du guide est antérieure aux amendements apportés au projet de loi nº 64 ; elle est conséquemment appelée à évoluer, et il n'est pas déraisonnable de souhaiter que cette évolution s'inscrive dans les standards internationaux.

Selon les lignes directrices ISO, l'impact à évaluer est relatif à tout ce qui a un effet sur la confidentialité des renseignements personnels, c'est-à-dire le secret des renseignements qui concernent une personne physique et qui permettent de l'identifier. Ainsi, la norme ISO/IEC 29134[54] définit l'évaluation d'impact comme un processus holistique, continuel, que le responsable du traitement des renseignements personnels amorce aux premières

52. ISO, *International Standard, Information Technology – Security Techniques – Guidelines for Privacy Impact Assessment*, ISO/IEC 29134 :2017, First Edition 2017-06, [En ligne], [www.iso.org/fr/standard/62289.html] (ci-après « norme ISO/IEC 29134 »). Cette norme est actuellement en réexamen, comme c'est le cas pour toute norme ISO qui doit être réexaminée tous les cinq ans.

53. Commission d'accès à l'information (CAI), *Guide d'accompagnement. Réaliser une évaluation des facteurs relatifs à la vie privée*, version de travail, 10 mars 2021, [En ligne], [www.cai.gouv.qc.ca/documents/CAI_Guide_EFVP_FR.pdf] (16 avril 2023) (ci-après « Guide d'accompagnement de l'EFVP »). La CAI est l'organisme qui veille à l'application de la Loi sur le secteur privé, préc., note 6. L'élaboration de lignes directrices est possible en vertu de l'article 123 (9º) (nouveau) de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1. Ce nouvel article est issu de la réforme initiée par la Loi 25. Il dispose que « [l]a Commission a également pour fonctions : […] d'élaborer des lignes directrices pour faciliter l'application de la présente loi et de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1), notamment en matière de consentement ». Au fédéral, voir notamment : Commissariat à la vie privée du Canada, *Guide du Commissariat au sujet du processus d'évaluation des facteurs relatifs à la vie privée*, mars 2020, [En ligne], [www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/evaluations-des-facteurs-relatifs-a-la-vie-privee/gd_exp_202003/] (16 avril 2023).

54. Norme ISO/IEC 29134, préc., note 52, introduction et section 3.7.

étapes du projet, plus exactement lorsqu'il est encore possible d'influencer l'issue du projet et de réaliser la « confidentialité programmée[55] ».

Quoique dans une forme préparatoire, le Guide d'accompagnement de l'EFVP éclaire également sur la nature et la finalité de l'EFVP en expliquant ceci : « L'EFVP est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées[56]. »

Cette interprétation de la Loi rejoint le RGPD. Qui plus est, par « facteurs relatifs à la vie privée », la CAI voit trois éléments, lesquels aussi définissent l'EFVP à la fois comme un outil de mise en conformité légale et un outil de gestion préventive des risques. Ces éléments sont les suivants : d'abord, l'EFVP permet de s'assurer que le projet de SI ou de PES respecte la législation sur la protection des renseignements personnels et les principes sous-jacents. L'approche ici est identique à celle du RGPD où la protection des données prend en compte, plus globalement, les droits et libertés des personnes physiques. Ensuite, l'EFVP sert à identifier les risques que le projet de SI ou de PES présente pour la vie privée, l'intimité, la vie personnelle, tout en proposant l'inventaire et une appréciation des impacts de ces risques, c'est-à-dire les conséquences, répercussions, incidences et implications du projet. Dans la version de travail du Guide d'accompagnement de l'EFVP, la notion de risque est décrite à la manière du RGPD[57]. Enfin, à travers l'EFVP, l'on doit pouvoir distinguer les stratégies et les mesures que les entreprises entendent déployer pour répondre aux risques identifiés.

Envisagé selon le RGPD, le scénario de l'application mobile d'optimisation des finances personnelles — ou plus exactement l'opération de traitement subjacente — serait également soumis à une AIPD dès sa conception. D'une part, en exigeant l'AIPD dès la conception, le législateur met l'accent sur le moment où il est encore possible de réaliser la *confidentialité*

55. De l'anglais *privacy by design*, l'expression désigne le « [p]rincipe selon lequel la protection des données personnelles doit être intégrée dans un système d'information dès sa conception » : GDT, préc., note 12, s.v. « Confidentialité programmée ».

56. Guide d'accompagnement de l'EFVP, préc., note 53, p. 6.

57. *Id.*, p. 15. Le risque est en effet présenté comme une menace potentielle, « une situation ou [un] évènement futur qui peut ou non se réaliser et qui causerait une perte ou un préjudice » ; lorsque ce risque est relatif à la vie privée, les rédacteurs du guide précisent que la perte ou le préjudice appréhendé concerne l'intimité ou la vie personnelle.

programmée[58] et la *protection des données par défaut*[59]. La *confidentialité programmée* permet au responsable du traitement de mettre en œuvre, depuis le moment de la détermination des moyens du traitement jusqu'au traitement lui-même, un ensemble de mesures techniques et organisationnelles pour garantir le respect des principes relatifs à la protection des données[60]. Au sens du règlement européen, la *protection des données par défaut* s'appuie aussi sur des mesures techniques et organisationnelles définies en amont du traitement. En l'occurrence, ces mesures visent à donner l'assurance que par défaut, c'est-à-dire sans l'intervention de la personne physique concernée, seules sont traitées les données qui sont nécessaires au regard de chaque finalité spécifique poursuivie[61]. L'analyse d'impact doit se poursuivre au fur et à mesure du développement de l'opération de traitement et même après son lancement[62].

D'autre part, si le déclencheur de l'AIPD est le risque élevé qu'un type d'opérations de traitement peut engendrer pour les droits et libertés des personnes physiques, dans le RGPD, ce niveau élevé du risque est perçu du premier coup dans certaines opérations. C'est le cas, comme dans le scénario de l'application mobile d'optimisation des finances personnelles, de l'opération de traitement qui comprend (selon la lettre

58. Voir *supra*, note 55.
59. RGPD, préc., note 7, art. 25 et considérant nº 78 ; Lignes directrices concernant l'AIPD, préc., note 30, p. 17. Voir aussi : Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices 4/2019 relatives à l'article 25. Protection des données dès la conception et protection des données par défaut*, version 2.0, adoptées le 20 octobre 2020, [En ligne], [edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf] (16 avril 2023).
60. *Id*.
61. *Id*. Cela suppose une limitation à quatre niveaux : concernant la quantité de données à caractère personnel collectées, l'étendue de leur traitement, leur durée de conservation et leur accessibilité (dans le dernier cas, les données ne doivent pas être ouvertes à un nombre indéterminé de personnes). Au Québec, le principe de la *protection des données par défaut* apparaît à l'article 9 al. 1 (nouveau) de la Loi sur le secteur privé, préc., note 6. La mise en œuvre de ce principe est requise dans le cadre précis de l'offre d'un produit ou d'un service technologique « disposant de paramètres de confidentialité ». Selon le texte, ces paramètres doivent assurer par défaut « le plus haut degré de confidentialité ». On se demande ce qu'il advient des autres produits ou services technologiques (ne disposant pas de paramètres de confidentialité). Par ailleurs, il n'y a aucune référence à des mesures organisationnelles de protection. De plus, le lien avec l'EFVP est absent. En pratique cependant, parce qu'il est impératif, le standard qu'introduit cette disposition constitue une référence que l'EFVP ne peut occulter, du moins pour les produits et services technologiques visés.
62. RGPD, préc., note 7, art. 35 (1) ; Lignes directrices concernant l'AIPD, préc., note 30, p. 17.

de l'article 35 (3) (a) du RGPD), « l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage[63], et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire[64] ». Pour illustration, le Groupe de travail « Article 29 » (G29) soumet l'exemple « d'une banque passant ses clients au crible d'une base de données de cote de crédit avant d'arrêter ses décisions d'octroi de prêt[65] ».

Plus généralement, le G29 a déterminé un ensemble de neuf critères à la lumière desquels le responsable du traitement peut décider si une AIPD doit être réalisée pour une opération de traitement du fait d'un risque élevé inhérent[66]. Dès qu'une opération de traitement satisfait à deux de ces

63. L'article 4 (4) du RGPD, préc., note 7, définit le profilage de façon suivante :

> Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

Dans la Loi sur le secteur privé, préc., note 6, art. 8.1 (nouveau) al. 2, « [l]e profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne ».

64. Hormis la discussion concernant le déclencheur de l'EFVP ou de l'AIPD, il faut noter que plusieurs opérations décrites à l'article 35 (3) (a) du RGPD, préc., note 7, et qui sont d'intérêt pour le système bancaire ouvert, nommément le profilage, la prise de décision fondée sur le traitement automatisé des renseignements personnels et la portabilité de ces renseignements, sont aussi réglementées dans la nouvelle version de la Loi sur le secteur privé, préc., note 6, art. 3.3, 8.1, 12.1 et 27. Néanmoins, si l'initiative du système bancaire ouvert devait se concrétiser, le cadre légal québécois et canadien nécessiterait l'addition d'un dispositif complémentaire comme l'Union européenne l'a fait en prévoyant notamment des règles sur les services de paiement dans la *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (DSP2)*, J.O.U.E. nº L 337/35, 23 décembre 2015. Ceci est vital pour organiser l'agrément des prestataires de services de paiement participants, spécifier l'obligation d'information qui leur incombe vis-à-vis du consommateur, cerner les droits et obligations liés à la prestation et à l'utilisation des services de paiement, identifier les normes techniques applicables, etc.

65. Lignes directrices concernant l'AIPD, préc., note 30, p. 12 et 13.

66. Ces critères sont au nombre de neuf : l'évaluation ou la notation ; la prise de décisions automatisée ; la surveillance systématique ; le traitement de données sensibles ou à caractère hautement personnel ; le traitement de données à grande échelle ; le croisement ou la combinaison d'ensembles de données ; le traitement de données concernant des

neuf critères, le G29 estime que le responsable du traitement peut considérer que cette opération est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques et qu'il importe de réaliser une AIPD[67]. L'AIPD permet alors, d'une part, de s'assurer que l'opération de traitement envisagée est conforme à la Loi. D'autre part, elle permet de prouver ou de démontrer cette conformité. Pour cela, il faut précisément évaluer l'origine, la nature, la particularité et la gravité du risque[68], tout en identifiant des mesures pour y faire face[69].

Ce premier contexte de l'EFVP a mis en exergue deux éléments de notre thèse. Premièrement, en énonçant une obligation indiscriminée, systématique, à l'égard de tous les projets de SI ou de PES impliquant le traitement de renseignements personnels, le législateur impose aux entreprises un fardeau qui rappelle l'ancienne approche généraliste européenne jugée peu efficace et abandonnée. Deuxièmement, l'imprécision de la Loi au sujet de l'EFVP, lorsque cette évaluation est entreprise dans le cadre d'un projet de SI ou de PES, est d'autant plus surprenante que ce flou concerne à la fois la nature et la finalité de l'EFVP. Ils ne sont pas définis dans la Loi, ces aspects pourtant essentiels, qui contribuent à circonscrire l'obligation imposée aux entreprises et à indiquer au consommateur ce à quoi il peut s'attendre en termes de protection. Reflet quasi parfait du RGPD, la proposition de la CAI (dans son projet de guide d'accompagnement de l'EFVP) tente de redresser le vague, toute intervention décisive pour le choix d'une méthode de réalisation de l'EFVP.

Avant de se pencher sur la réalisation de l'EFVP, il importe de développer l'autre contexte virtuellement pertinent en technologie financière, soit l'exigence d'une EFVP précédant la communication d'un renseignement personnel à l'extérieur du Québec.

---

personnes vulnérables ; l'utilisation innovante ou l'application de nouvelles solutions (technologiques ou organisationnelles) ; et le traitement qui empêche l'exercice d'un droit ou le bénéfice d'un service ou d'un contrat. Voir les Lignes directrices concernant l'AIPD, préc., note 30, p. 10-12.

67. *Id.*, p. 13. Le G29 précise qu'il peut arriver qu'une opération qui ne satisfait qu'à un seul des critères énoncés entraîne néanmoins une AIPD. Par ailleurs, le responsable du traitement qui considère qu'une opération de traitement n'est pas susceptible d'engendrer le risque élevé dont il est question doit motiver et documenter sa décision de ne pas procéder à une AIPD.
68. RGPD, considérant, nº 84.
69. RGPD, préc., note 7, art. 35 (7) (d). L'article 24 indique que les mesures prises pour s'assurer et prouver que le traitement est effectué conformément au règlement sont réexaminées et actualisées si nécessaire. Voir également les Lignes directrices concernant l'AIPD, préc., note 30, p. 4.

1.2 La communication d'un renseignement personnel à l'extérieur du Québec

La CAI situe la « communication » à la troisième étape du cycle de vie du renseignement personnel. Elle indique que « [l]a communication est la période où le renseignement personnel est communiqué [c'est-à-dire transféré, transmis, on le fait savoir ou connaître], par exemple dans un système de prestation électronique de services, par courriel, au service à la clientèle, par le biais de sites Web ou à un tiers[70] ». La communication du renseignement personnel peut être effectuée au Québec ou à l'extérieur du Québec. Lorsqu'elle est effectuée à l'extérieur du Québec, la communication doit être précédée d'une EFVP. C'est l'alinéa 1 de l'article 17 (nouveau) de la Loi sur le secteur privé qui établit cette exigence.

Cette disposition s'applique notamment à l'infonuagique, une forme d'impartition qui prend le pas sur le modèle classique de développement et de gestion *in situ* des SI ou des PES. Le modèle classique suppose l'acquisition d'infrastructures matérielles et logicielles, la création des conditions de leur pérennité, leur déploiement dans les espaces dédiés, l'arrimage à l'existant, l'initiation des ressources humaines aux nouveaux processus technologiques, etc. L'infonuagique permet d'éviter nombre de ces opérations et les investissements sous-jacents en proposant aux organisations (privées comme publiques) un « [m]odèle informatique dans lequel le stockage des données et leur traitement sont externalisés sur des serveurs distants accessibles à la demande à partir de tout appareil bénéficiant d'une connexion Internet[71] ». La filiale d'Amazon (Amazon Web Services ou AWS) et Microsoft dominent le marché mondial des services d'infrastructure et de plateforme infonuagiques : ensemble, ils détenaient en 2021 plus de 90 p. 100 de ce marché[72]. L'infrastructure d'AWS est maillée en régions, celles-ci étant des emplacements physiques disséminés sur le globe, avec des zones de disponibilité où sont installés des centres de données[73]. Le fournisseur de technologie financière de notre scénario ou toute entreprise

70. CAI, *Protection des renseignements personnels*, 5 mai 2021, [En ligne], [www.cai.gouv.qc.ca/entreprises/protection-des-renseignements-personnels-1/] (16 avril 2023). Le cycle de vie du renseignement comprend la collecte, l'utilisation, la communication, la conservation et la destruction du renseignement.

71. GDT, préc., note 12, s.v. « Infonuagique ».

72. Raj Bala et autres, *Magic Quadrant pour les services d'infrastructure et de plateforme cloud*, Étude Gartner publiée le 27 juillet 2021, ID G00736363. Voir aussi le texte d'Ulysse Bergeron, « Québec accorde un autre gros contrat à Amazon », *Le Devoir*, 28 juin 2021, [En ligne], [www.ledevoir.com/economie/614259/autre-gros-contrat-pour-amazon] (16 avril 2023).

73. Amazon, *Régions et zones de disponibilité*, [En ligne], [aws.amazon.com/fr/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2] (16 avril 2023).

ou tout organisme public[74] qui fait affaire avec ce prestataire, par exemple, a l'obligation de réaliser une EFVP avant de pouvoir dupliquer, sauvegarder, stocker, faire transiter, transférer, etc., un renseignement personnel dans l'un de ces centres de données, si celui-ci est physiquement situé à l'extérieur des frontières de la province du Québec. L'exigence a un objectif pratique : veiller à ce que le renseignement bénéficie d'une *protection adéquate* lors même que, par leur situation géographique, les centres de données destinataires peuvent échapper à l'emprise des lois du Québec.

L'EFVP jugée favorable à la communication du renseignement est celle dont les résultats attestent ou confirment l'*adéquation* de la protection qui sera accordée à ce renseignement à l'extérieur du Québec. L'*adéquation* est envisagée « notamment au regard des principes de protection des renseignements personnels généralement reconnus[75] ». De plus, la communication doit être encadrée par des clauses contractuelles écrites, définies par les parties en tenant compte des résultats de l'EFVP. Ces clauses incluent, le cas échéant, des mesures d'atténuation des risques identifiés dans le cadre de l'évaluation[76]. Précisons que l'entreprise qui a recours à une personne ou à un organisme situé à l'extérieur du Québec pour recueillir, utiliser, communiquer ou conserver, pour son compte, un renseignement personnel est aussi soumise à l'ensemble de ces formalités[77].

Si le législateur européen renvoie au même concept d'*adéquation* (de la protection), il le traite différemment et non au chapitre de l'AIDP. Les dispositions pertinentes, c'est-à-dire les articles 45 et suivants du RGPD, sont énoncées au chapitre V intitulé « Transferts fondés sur une décision d'adéquation — Transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ». L'article 45 prévoit que le transfert vers ce pays tiers, en l'occurrence un pays non membre de l'Espace économique européen (EEE), ou vers une organisation internationale, peut avoir lieu dans trois cas : premièrement, lorsque ce transfert a fait l'objet d'une *décision d'adéquation*, c'est-à-dire que la « Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat ». La décision de la Commission est prise sur la base d'éléments comme l'accès aux données par les autorités publiques du pays, la jurisprudence, les recours administratifs et judiciaires ouverts dans ce pays, l'existence et le fonctionnement effectif

74. Voir l'article 70.1 (nouveau) de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, préc., note 53.
75. Voir la Loi sur le secteur privé, préc., note 6, art. 17 al. 2 (nouveau).
76. *Id*.
77. *Id*., art. 17 al. 3 (nouveau).

d'autorités de contrôle indépendantes ou encore les engagements internationaux pris par le pays tiers ou l'organisation. Le Canada, par exemple, bénéficie d'une *décision d'adéquation*, plus exactement les destinataires au Canada dont les activités relèvent de la *Loi canadienne sur la protection des renseignements personnels et les documents électroniques*[78].

Deuxièmement, à défaut d'une *décision d'adéquation* rendue par la Commission, le transfert des données peut avoir lieu moyennant des *garanties appropriées* fournies par le responsable du traitement ou par le sous-traitant, conformément à l'article 46 du RGPD[79]. Ces garanties sont normalement contenues dans des instruments de transfert, comme des règles d'entreprise contraignantes[80] ou des clauses contractuelles types (CCT)[81]. Troisièmement, le responsable du traitement ou le sous-traitant établi dans l'EEE peut se prévaloir de l'une des dérogations de l'article 49, s'il en remplit les conditions[82].

Dans l'interprétation de ces dispositions, il faut s'intéresser au récent arrêt de la Cour de justice de l'Union européenne (CJUE) dans l'affaire C-311/18 (Schrems II)[83] et les mesures qui en ont découlé, en particulier les *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection*

78. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5. Voir la *Décision de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques*, J.O.U.E. nº L 2/13, 4 janvier 2002.

79. Suivant cette disposition, il importe aussi que « les personnes concernées disposent de droits opposables et de voies de droit effectives ».

80. RGPD, préc., note 7, art. 47.

81. *Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil*, J.O.U.E. nº L 199/31, 7 juin 2021.

82. Par exemple, le responsable du traitement ou le sous-traitant peut devoir obtenir le consentement explicite et informé de la personne concernée. Voir European Data Protection Board (EDPB), *Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679*, adoptées le 25 mai 2018, [En ligne], [edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf] (16 avril 2013).

83. *Data Protection Commissioner* c. *Facebook Ireland Ltd. et Maximillian Schrems*, Affaire C-311/18, 16 juillet 2020, [En ligne], [curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=12014297] (16 avril 2023).

des données à caractère personnel de l'UE[84] et les *Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance*[85]. L'élément suivant en ressort : l'existence d'une *décision d'adéquation* dans un contexte donné procède d'une évaluation du niveau de protection ; cette évaluation est réalisée par la Commission elle-même. Cela permet au responsable du traitement ou au sous-traitant (identifiés dans les Recommandations comme l'exportateur) de procéder immédiatement au transfert. L'absence de *décision d'adéquation* ou de dérogation suivant l'article 49 du RGPD remet le fardeau de l'évaluation sur les épaules de l'exportateur. En pareille situation, l'évaluation est typique et elle bénéficie d'un encadrement contrasté par rapport à l'AIPD : elle a pour objet de juger de l'*efficacité* de l'instrument de transfert que l'exportateur a sélectionné (par exemple les CCT) en confrontant cet instrument (et les garanties inhérentes) au droit et aux usages du pays tiers[86]. Selon les Recommandations 01/2020, « [o]n entend par "efficace" le fait que les données à caractère personnel transférées bénéficient dans le pays tiers d'un *niveau de protection substantiellement équivalent* à celui qui est garanti dans l'EEE[87] ». À moins de renoncer au transfert, des mesures supplémentaires (contractuelles, techniques ou organisationnelles) sont requises quand l'évaluation révèle que l'instrument de transfert et les garanties qu'il contient ne seraient pas efficaces si le transfert avait lieu[88].

Au Québec, une mouture initiale du projet de loi nº 64 exigeait que l'EFVP démontre une « *protection équivalant* à celle prévue à la [Loi

84. EDPB, *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE*, adoptées le 10 novembre 2020, [En ligne], [edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_fr.pdf] (16 avril 2023) (ci-après « Recommandations 01/2020 »).

85. EDPB, *Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance*, adoptées le 10 novembre 2020, [En ligne], [edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_fr.pdf] (16 avril 2023) (ci-après « Recommandations 02/2020 »).

86. Précisons que la définition du transfert est large : « l'accès à distance depuis un pays tiers (par exemple, dans des situations de soutien) et/ou le stockage dans un nuage situé hors de l'EEE, doit également être considéré comme un transfert » (Recommandations 01/2020, préc., note 84, par. 13).

87. *Id.*, par. 29 (l'italique est de nous). Les Recommandations 01/2020 citent Schrems II, préc., note 83 § 105 et deuxième conclusion.

88. Cette recommandation se fonde sur les points 134 et 135 de Schrems II (préc., note 83) : Recommandations 01/2020, préc., note 84, par. 44 et 47.

québécoise][89] » avant que l'on puisse communiquer un renseignement personnel à l'extérieur du Québec. Une autre disposition du projet de loi (l'article 103) prévoyait ceci : « Le ministre publie à la Gazette officielle du Québec une liste d'États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec[90]. » Lors des travaux parlementaires, la disposition a été amendée : on a retiré « *équivalant* à celle prévue à la [Loi québécoise] » au profit de « *adéquate*, notamment au regard des principes de protection des renseignements personnels généralement reconnus »[91]. Les parlementaires ont subséquemment éliminé l'obligation imposée au ministre de publier une liste des États dont le régime juridique est jugé *équivalent* à celui du Québec. L'amendement a ainsi été motivé :

> Plusieurs intervenants ont exprimé des inquiétudes par rapport aux exigences énoncées dans le projet de loi concernant la communication de renseignements personnels à l'extérieur du Québec, en particulier en ce qui a trait à l'évaluation du degré d'équivalence du régime juridique applicable dans l'État où le renseignement serait communiqué. Ces intervenants ont mentionné que cette exigence entraînerait d'importants coûts de mise en conformité et limiterait l'accès, par les entreprises québécoises, à certains services en ligne. Qui plus est, ce processus aurait nécessité la réalisation d'une *analyse comparative* entre la loi québécoise et le régime juridique applicable dans l'État où le renseignement personnel serait communiqué, une démarche s'avérant d'une certaine complexité.
>
> Il y a donc lieu d'amender le projet de loi afin de retirer la notion *d'équivalence* entre les lois québécoises et celles de l'État où la communication de renseignements est envisagée. La modification proposée aurait donc pour effet de permettre la communication hors Québec, dans la mesure où l'organisme public ou l'entreprise estime que le renseignement bénéficiera d'une protection *adéquate* à la suite d'une *évaluation* qui devra tenir compte de l'ensemble des mesures de protection applicables aux renseignements personnels, ce qui peut inclure le régime législatif certes, mais également des mesures contractuelles[92].

89. Québec, Assemblée nationale, *Projet de loi nº 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, présenté par Madame Sonia LeBel, ministre responsable des Institutions démocratiques, de la Réforme électorale et de l'Accès à l'information, Éditeur officiel du Québec, 2020, p. 19 (l'italique est de nous).
90. *Id.*
91. Loi sur le secteur privé, préc., note 6, art. 17.
92. Gouvernement du Québec, *Amendements apportés au projet de loi nº 64 – Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, mémoire au Conseil des ministres, 8 février 2021, p. 2, [En ligne], [cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/amendements_pl64_memoire.pdf ?1632421739] (16 avril 2023) (ci-après « Mémoire au Conseil des ministres ») (l'italique est de nous).

Cette explication est présumée rassurer les parties prenantes. Mais, selon notre thèse, elle convainc à grand-peine : c'est que, entre *protection équivalente* et *protection adéquate*, il nous semble demeurer un trait commun, soit l'évaluation qui doit confirmer ou infirmer l'*équivalence* ou l'*adéquation*. Dans un cas comme dans l'autre, il faut procéder à une analyse qui a la particularité d'être comparative, c'est-à-dire qu'elle doit établir ou exprimer des comparaisons. Relativement à l'*équivalence*, les comparaisons étaient envisagées par rapport à la Loi québécoise. Concernant l'*adéquation*, les comparaisons doivent être entreprises au regard « des principes de protection des renseignements personnels généralement reconnus ». Dans les deux cas, il s'agit de comparaisons multiformes, du droit, des usages, des processus administratifs, etc., toute chose semblant davantage du ressort de l'État (étant donné l'importance des ressources à mobiliser pour l'évaluation) que de celui de la très petite entreprise (TPE), de la PME ou encore de l'entreprise de taille intermédiaire (ETI). Les modalités et les critères du RGPD à propos des *décisions d'adéquation* sont une indication frappante que l'exercice n'est pas plus aisé lorsque l'évaluation vise à établir le caractère *adéquat* de la protection offerte dans un État tiers. Le fardeau des entreprises est d'autant plus astreignant qu'elles ont, seules, la responsabilité de cette évaluation, contrairement au contexte européen où les *décisions d'adéquation* autorisant le transfert des données vers un pays tiers ou à une organisation internationale sont rendues par la Commission à la suite d'une analyse qu'elle-même effectue. Et, comble de complexité, le législateur québécois définit l'évaluation à réaliser comme une EFVP (et non comme la seule appréciation de l'efficacité des instruments de transfert qui seront utilisés). Ce qui, aussi, positionne cette évaluation à la fois comme un outil de mise en conformité légale et un outil de gestion préventive de risques. Cette double qualification, on va le voir à partir de l'exemple européen, influence directement la réalisation de l'évaluation et, incidemment, le faix des entreprises.

Au total, à la lumière de ses caractéristiques, notre application fictive d'optimisation financière est de façon incontournable candidate à l'EFVP soit à titre de projet de SI ou de PES, soit parce qu'elle implique la communication de renseignements personnels à l'extérieur du Québec. La nature des renseignements collectés dans le cadre de ces applications et l'ampleur des opérations auxquelles ces renseignements sont soumis mettent en évidence l'intérêt de l'EFVP. Pour éviter la banalisation de l'EFVP, peut-être aurait-il fallu confiner celle-ci dans les situations qu'illustre notre application mobile (voire dans des opérations de traitement d'une certaine ampleur) ou, comme en Europe, dans des situations précises impliquant notamment des risques élevés pour la vie privée. Par ailleurs, la lettre du RGPD a offert des indications qui ont tracé les sillons dans lesquels les

guides d'accompagnement et autres outils ont cheminé pour éclairer les acteurs. Au Québec, la quasi-généralisation du recours à l'EFVP contraste avec l'absence de telles indications dans la Loi, du moins concernant les projets de SI et de PES. Il faudra, pour les acteurs, espérer que la CAI fasse preuve de générosité à cet égard.

Au-delà du contexte de l'EFVP, sa réalisation met en évidence l'ampleur de cette nouvelle exigence de la Loi 25.

2 La méthode et la réalisation de l'évaluation des facteurs relatifs à la vie privée : quelques éléments utiles

Le législateur québécois a adopté une approche minimaliste concernant la méthode et la réalisation de l'EFVP, naviguant entre le silence pour les SI et les PES et l'amorce de quelques indications pour la communication de renseignements à l'extérieur du Québec. Le regard posé sur le texte européen et les normes ISO a permis de dégager quelques éléments qui pourraient être utiles dans la mise en place des technologies financières et au-delà de ces dernières.

2.1 De l'approche minimalise de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Loi 25)

La réforme de la Loi sur le secteur privé est taciturne à propos des fondamentaux de la méthode de l'EFVP, du moins quand l'évaluation concerne un projet d'acquisition, de développement ou de refonte de SI ou de PES impliquant le traitement de renseignements personnels. La définition de la méthode de l'EFVP est un défi que le législateur semble avoir sciemment écarté, peut-être en regard de la variété des projets de SI et de PES soumis à l'EFVP. Le législateur s'en tient à des prescriptions ou à des orientations minimalistes, la plupart du temps à la périphérie de l'évaluation. Celles-ci sont énoncées aux articles 3.3 et 3.4 (nouveaux) de la Loi. Dans ces dispositions, la prescription de nature procédurale, c'est-à-dire l'obligation de consulter le responsable de la protection des renseignements personnels, et la recommandation concernant les mesures organisationnelles de protection des renseignements personnels n'appellent pas de commentaires particuliers[93]. En revanche, il importe de s'interroger

93. *Consulter* signifie « solliciter quelqu'un pour lui demander conseil » : DAC, préc., note 9, s.v. « Consulter ». Les conseils attendus sont présumément liés aux attributions, à l'expertise ou aux connaissances spécialisées du responsable de la protection des renseignements personnels.

sur la pertinence, à l'étape de l'EFVP, de l'obligation faite à la personne qui procède à l'évaluation de s'assurer que le projet de SI ou de PES permet qu'un renseignement personnel recueilli auprès de la personne concernée et soumis à un traitement informatique soit communiqué à cette dernière « dans un format technologique structuré et couramment utilisé[94] ». Dans l'exemple de l'application putative d'optimisation des finances personnelles, cela signifie que, en réalisant l'EFVP (dès le début du projet), le fournisseur de la technologie financière veille à ce que l'application qui sera distribuée permette au consommateur de jouir de la *portabilité* de ses renseignements à caractère personnel[95]. Le droit lié à la *portabilité* des données permet de réaffirmer et de garantir à la personne concernée le contrôle de ses données ou, comme l'explique mieux le G29, de « responsabiliser les personnes concernées au sujet de leurs données à caractère personnel, car [cela] facilite leur capacité à déplacer, à copier ou à transmettre facilement des données à caractère personnel d'un environnement informatique vers un autre[96] ». La matérialisation de ce droit influence la conception même des projets, et c'est peut-être pour cette raison que le législateur québécois l'introduit dans l'EFVP : ainsi, il force, à l'orée des projets, un certain paramétrage et des correctifs, le cas échéant, de façon à enchâsser ce droit dans lesdits projets. Mais alors, pourquoi ne pas aussi avoir expressément intégré à l'EFVP les autres droits, voire le principe de la *protection des*

94. Loi sur le secteur privé, préc., note 6, art. 3.3 al. 3. L'article 20 (1) du RGPD, préc., note 7, emploie l'expression « dans un format structuré, couramment utilisé et lisible par machine ». Le Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices relatives à la portabilité des données*, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, p. 20 et 21, [En ligne], [www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf], précise que « [l]es qualificatifs "structuré", "couramment utilisé" et "lisible par machine" constituent une série d'exigences minimales qui devraient faciliter l'interopérabilité du format de données fourni par le responsable du traitement. En ce sens, les termes "structuré, couramment utilisé et lisible par machine" donnent des précisions sur les moyens, tandis que l'interopérabilité est le résultat escompté ». Le Groupe de travail ajoute que « la portabilité vise à produire des systèmes interopérables, et non des systèmes compatibles » (p. 21).

95. Notons qu'à cette étape la Loi ne requiert qu'une prise en compte partielle du droit à la portabilité des données. La portée de ce droit est beaucoup plus étendue en vertu de l'article 27 (nouveau). En dehors de l'EFVP, les renseignements de la personne concernée doivent normalement aussi pouvoir être communiqués, à sa demande, à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement. Il en va ainsi « à moins que cela ne soulève des difficultés pratiques sérieuses ». Dans le RGPD, préc., note 7, le droit à la portabilité des données est traité à l'article 20. Voir aussi l'article 15 du RGPD.

96. G29, préc., note 94, p. 4.

données par défaut[97] et celui de la *confidentialité programmée* dont la mise en œuvre, comme en matière de portabilité, est liée à la conception des projets ou dépend de cette dernière ?

Le dernier alinéa de l'article 3.3 (nouveau) n'éclaire pas plus la méthode de l'EFVP. Il indique essentiellement que la réalisation de cette évaluation, quel que soit le contexte, doit être proportionnée, c'est-à-dire dosée, mesurée. L'EFVP peut ainsi être sommaire ou détaillée, compte tenu des cinq critères énoncés dans la Loi, à savoir « la sensibilité des renseignements concernés, […] la finalité de leur utilisation, […] leur quantité, […] leur répartition et […] leur support ». Or, malgré ces indications, il nous semble que le contexte précis de l'EFVP qui serait qualifiée de sommaire demeure incertain, tout comme le seuil de basculement vers une EFVP détaillée. Un mémoire du ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels a fait valoir que « l'évaluation pourra être très sommaire si ces différents critères conduisent l'entreprise ou l'organisme public à conclure que *le risque est faible de prime abord*[98] ». Mais la disposition précitée n'indique nulle part que le *risque* constitue l'élément ou le critère qui doit orienter le choix entre une EFVP sommaire (ou « très sommaire ») et une EFVP détaillée. Même si elle l'avait indiqué, sommaire ou non, l'évaluation n'en demeurerait pas moins une analyse de risque, c'est-à-dire un « [p]rocessus d'identification, d'estimation et d'évaluation des risques d'un projet afin de décider du traitement des risques retenus[99] ». Un tel processus, pour être digne de confiance, ne peut être envisagé sans méthode, et il n'est pas indiqué d'en omettre des maillons, d'autant plus que des renseignements à caractère personnel sont en jeu. On se demande alors à quel point il peut être sommaire ou « très sommaire » ou être effectué *prima facie*. Par-dessus tout, l'EFVP n'étant pas qu'un outil de gestion de risques, il est attendu que ses autres aspects seront également pris en considération dans sa réalisation (sommaire, très sommaire ou détaillée).

Outre la question de la proportionnalité de l'évaluation, le constat est que la réforme de la Loi sur le secteur privé est peu bavarde quant à la façon dont les entreprises doivent réaliser l'EFVP, du moins pour leurs projets de SI ou de PES. L'approche minimaliste de la Loi procure une certaine flexibilité aux entreprises, mais tend aussi à alimenter l'incerti-

97. Comme nous l'avons expliqué précédemment, la Loi sur le secteur privé, préc., note 6, énonce ce principe à l'égard de l'offre de produits ou de services technologiques pourvus de paramètre de confidentialité. Le lien avec l'EFVP n'est pas direct.

98. Mémoire au Conseil des ministres, préc., note 92, p. 3 (l'italique est de nous).

99. *Dictionnaire de management de projet*, préc., note 16, *s.v.* « Analyse des risques d'un projet », p. 14.

tude en n'accordant pas assez d'attention à la méthode et aux critères de l'évaluation (concernant les conditions de conformité ou d'acceptabilité de l'EFVP, le contenu commun du rapport d'évaluation, sa durée de validité ou ses conditions de caducité, etc.). Une fois mis au point, le Guide d'accompagnement de l'EFVP ne devrait pas fondamentalement diverger des instruments européens[100] ni de la norme ISO/IEC 29134 qui, déjà, donnent un portrait détaillé des balises manquantes et documentent attentivement la manière dont il est possible de réaliser l'EFVP. Nos observations terminales insistent particulièrement sur ces instruments européens et sur la norme ISO/IEC 29134. À l'occasion, des décisions des autorités de contrôle viendront nourrir l'analyse.

En vertu du RGPD, les modalités de l'AIPD tiennent compte de sa triple vocation : d'une part, il s'agit de garantir la conformité des opérations de traitement aux exigences de la Loi ; d'autre part, l'analyse d'impact peut servir de preuve de cette conformité ; enfin, l'analyse d'impact doit être utilisée comme un moyen de gérer préventivement les risques que les opérations de traitement présentent pour les droits et libertés des personnes physiques. Il est convenu que l'AIPD pourra reposer sur diverses méthodes dont le choix sera laissé au responsable du traitement[101]. Néanmoins, le paragraphe 7 de l'article 35 du RGPD énonce trois critères impératifs, c'est-à-dire des étapes auxquels doit satisfaire toute méthode ou toute façon de procéder à l'analyse (ce sont les critères d'acceptabilité de l'AIPD) : 1) la description des opérations de traitement envisagées et leurs finalités ; 2) l'évaluation de la nécessité et de la proportionnalité de ces opérations de traitement ; 3) l'évaluation et la gestion des risques pour les droits et libertés des personnes concernées[102]. Il est aisé de remarquer que, malgré la disponibilité de lignes directrices et de guides d'accompagnement, le texte européen prend soin d'énoncer des éléments fondamentaux à la réalisation de l'AIPD, chose dont le texte québécois aurait pu s'inspirer en ce qui concerne les projets de SI et de PES. Les sections qui suivent

100. La réforme québécoise est inspirée du RGPD.

101. Lignes directrices concernant l'AIPD, préc., note 30, p. 20.

102. Notons avant tout ceci : au même degré que la loi québécoise, le responsable du traitement qui effectue une AIPD doit demander conseil au délégué à la protection des données, si un tel délégué a été désigné. De plus, le paragraphe 9 de l'article 35 spécifie que le responsable du traitement doit recueillir, le cas échéant, l'avis des personnes concernées, c'est-à-dire les personnes physiques identifiées ou identifiables dont les données sont en jeu (RGPD, préc., note 7, art. 35 (2) et 1 (1)). Cet avis porte sur l'opération de traitement prévu : les Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD) présentent cette obligation de consultation comme le quatrième critère d'acceptabilité de l'AIPD. Voir aussi l'article 37 (5) du RGPD, préc., note 7.

visent à démontrer que ces précisions ne sont pas inutiles. En particulier, parce que ces éléments fondamentaux sont précieux dans la détermination de la méthode de réalisation de l'EFVP.

2.2 Les modalités de l'évaluation des facteurs relatifs à la vie privée

Les modalités de l'EFVP peuvent s'inspirer des trois critères d'acceptabilité de l'AIPD.

2.2.1 La description des opérations de traitement envisagées et leurs finalités

Le RGPD se démarque du texte québécois en énonçant, comme premier critère, que toute méthode d'analyse doit satisfaire la « description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement[103] ». Comme ce sont ces opérations de traitement qui font l'objet de l'analyse d'impact, il est logique qu'elles soient connues d'emblée[104]. Pour y voir, il est attendu du responsable du traitement cinq actions méthodiquement circonscrites dans les Lignes directrices concernant l'AIPD et par ailleurs étayées par la norme ISO/IEC 29134. Premièrement, il faut déterminer l'ensemble de ce qui constituera les opérations de traitement. La description concerne le processus d'affaires qui sera pris en charge, de même que la portée du traitement, le contexte dans lequel il s'inscrit et ses finalités. En quelque sorte, dans l'exemple de notre application mobile, il s'agit de brosser un tableau de la manière dont les données des utilisateurs seront collectées, auprès de qui elles le seront et dans quel but, qui y aura accès et dans quel but[105].

Deuxièmement, il importe de préciser les données à caractère personnel qui sont concernées par ce traitement, notamment s'il s'agit de données sensibles ou de données à caractère hautement personnel, lesquelles doivent bénéficier de mesures de protection adaptées. Il faut également indiquer la période pendant laquelle les données recueillies seront conservées et l'identité du destinataire de ces données[106].

---

103. RGPD, préc., note 7, art. 35 (7) (a).
104. Norme ISO/IEC 29134, préc., note 52, introduction et section 6.3.3.
105. Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD) ; norme ISO/IEC 29134, préc., note 52, section 6.3.3.
106. RGPD, préc., note 7, art. 4 (9) : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ». La disposition précise que, lorsqu'elles

Troisièmement, il faut proposer une description fonctionnelle ou logique des opérations de traitement. Suivant la norme ISO/IEC 29134, cela conduit à définir un ensemble de diagrammes : un diagramme du flux de données par entités et par interfaces ; un diagramme du flux de données tout au long du cycle de vie des données ; un diagramme du flux de travail qui décrit le moment où il convient de notifier et d'obtenir le consentement du responsable du traitement ou du délégué à la protection des données. De plus, le responsable de l'AIPD doit prévoir une liste des interfaces identifiant les parties connectées et les champs de données transférés ; le détail des ports, protocoles, API, chiffrement, etc.[107].

Quatrièmement, une autre exigence consiste à identifier les actifs sur lesquels reposent les données. Les Lignes directrices concernant l'AIPD et la norme ISO/IEC 29134 ont en vue l'actif humain (dans l'ensemble, les parties prenantes ou les personnes susceptibles de traiter les données à caractère personnel et les personnes qui peuvent être affectées par ce traitement) ; l'actif matériel et logiciel nécessaire à la gestion des données est tout autant concerné (par exemple, les terminaux de communication, logiciels ou applications mobiles des usagers, les réseaux, les bases de données, les documents papier ou les canaux de transmission papier)[108].

Cinquièmement, enfin, il faut prendre en compte les codes de conduite approuvés qui contribuent à la bonne application de la Loi[109]. Cette obligation s'impose au responsable du traitement comme à ses sous-traitants[110].

Ces cinq actions ci-dessus énumérées pourraient aider, dans un premier temps, les entreprises québécoises à prendre la mesure de leurs obligations à l'étape de la description du projet de SI et de PES faisant l'objet de l'EFVP.

Dans un second temps, le responsable du traitement doit évaluer la nécessité et la proportionnalité des opérations de traitement, telles qu'elles ont été décrites. Cette évaluation doit se faire en tenant compte des finalités de ces opérations.

---

sont susceptibles de recevoir des données à caractère personnel dans le cadre d'une mission d'enquête particulière, les autorités publiques ne sont pas considérées comme des destinataires au sens du RGPD.

107. Norme ISO/IEC 29134, préc., note 52, section 7.3.1.3.
108. *Id*.
109. Voir l'article 40 du RGPD, préc., note 7.
110. *Id*., art. 35 (8).

2.2.2 L'évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités

L'enquête des autorités canadiennes de protection des renseignements personnels concernant l'application mobile de la chaîne Tim Hortons illustre de fort belle manière la pertinence de l'évaluation de la nécessité et de la proportionnalité des opérations de traitement. Selon les conclusions de cette enquête[111], il y a eu près de 10 millions de téléchargements de l'application de Tim Hortons depuis son lancement en 2017 jusqu'à l'ouverture de l'enquête en 2020. Cette application devait permettre à l'entreprise de collecter les données de localisation détaillées de l'utilisateur « afin de mieux promouvoir son café et ses produits connexes[112] ». Or, une fois traitées, les grandes quantités de données collectées ont davantage permis de « [d]éduire le lieu du domicile et le lieu de travail d'un utilisateur, et les situations dans lesquelles un utilisateur était en déplacement […] de [g]énérer un "événement" d'entrée ou de sortie chaque fois que l'utilisateur visitait l'un des neuf concurrents identifiés par Tim Hortons, visitait les principaux sites et stades où se tenaient des événements à caractère sportif, ou retournait à son lieu présumé de résidence ou de travail[113] ». Tim Hortons a ainsi suivi les utilisateurs de l'application sans leur consentement, « aussi souvent que toutes les quelques minutes », même lorsque l'application n'était pas ouverte[114]. Cette pratique a été jugée illégale[115]. Elle a naturellement cessé. Fait notable, les enquêteurs ont recommandé à l'entreprise de procéder à une EFVP lors du développement de toute nouvelle application pouvant affecter la vie privée. Les enquêteurs ont été encore plus précis en indiquant que leur prescription comprend « sans s'y limiter : a) un processus permettant de s'assurer que les renseignements à recueillir sont *nécessaires* et *proportionnels* aux répercussions potentielles sur la vie privée relevées ; b) des mécanismes pour veiller à ce que les *communications* relatives à la protection de la vie privée *cadrent avec les pratiques liées à l'application* et les *expliquent de manière adéquate*[116]. » Il faut en comprendre qu'un projet de SI ou de PES se rapportant à une

111. L'enquête a été réalisée par la Commission d'accès à l'information du Québec, le Commissariat à l'information et à la protection de la vie privée de l'Alberta, le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique et le Commissariat à la protection de la vie privée du Canada, *Rapport de conclusions*, CPVP LPRPDE-040088 / CAI QC-1023953-S / OIPC-AB 016271 / OIPC-BC P20-83148, 1er juin 2022, [En ligne], [www.cai.gouv.qc.ca/documents/CAI_TDL_RF_FR.pdf] (16 avril 2023).
112. *Id*., p. 17.
113. *Id*., p. 13.
114. *Id*., p. 3.
115. *Id*., p. 4.
116. *Id*., p. 28 et 29.

application d'optimisation financière (comme dans notre exemple) ne saurait faire l'économie d'une évaluation de la nécessité et de la proportionnalité des opérations de traitement dans la réalisation de l'EFVP[117].

Dans le RGPD, l'exigence concernant l'évaluation de la nécessité et de la proportionnalité des opérations de traitement émane de l'article 35 (7) (b). En l'espèce, le responsable du traitement doit évaluer et documenter les mesures qu'il entend déployer pour assurer la conformité au RGPD, c'est-à-dire, d'une part, les mesures contribuant au respect des principes fondamentaux du traitement des données à caractère personnel et, d'autre part, les mesures concourant aux droits des personnes concernées.

Relativement aux premières mesures, le principe de finalité (bien connu de la Directive 95/46/CE[118]) est un prérequis qui sert à établir les limites dans lesquelles les données peuvent être collectées et peuvent être traitées ultérieurement[119]. Selon ce principe, les données à caractère personnel doivent être collectées pour des finalités *déterminées*, *explicites* et *légitimes*[120]. Suivant l'interprétation du G29[121] est *déterminée* la finalité qui est connue avec précision, celle qui est suffisamment définie pour permettre une application effective de toutes les garanties nécessaires à la protection des données et pour délimiter la portée du traitement (à savoir quel type de traitement est inclus ou est exclu)[122]. L'on écarte conséquemment les finalités énoncées vaguement ou en des termes généraux, comme le fait d'indiquer que la collecte des données à caractère personnel vise à « améliorer l'expérience des utilisateurs », ou est entreprise à des fins mercatiques, de sécurité informatique, de recherche, etc.[123]. Lorsque la

117. Dans une publication, certes consacrée à la biométrie, la Commission d'accès à l'information du Québec, *Biométrie : principes à respecter et obligations légales des organisations – Guide d'accompagnement pour les organismes publics et les entreprises*, 21 septembre 2022, p. 1-5, relève l'importance de ce critère de nécessité et de proportionnalité dans l'évaluation faite dans le cadre d'une EFVP.
118. Directive 95/46/CE, préc., note 37, abrogée par le RGPD, préc., note 7.
119. Groupe de travail « Article 29 » sur la protection des données, *Opinion 03/2013 on Purpose Limitation*, 00569/13/EN WP 203, adoptée le 2 avril 2013, p. 4, [En ligne], [ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf] (16 avril 2023) (ci-après « Opinion concernant le principe de finalité »).
120. RGPD, préc., note 7, art. 5 (1) (b).
121. Cette interprétation a été soumise dans le contexte de la Directive 95/46/CE, préc., note 37. L'abrogation de cette directive par le RGPD ne remet pas en cause l'interprétation du G29, dans la mesure où le RGPD reconduit le principe de finalité.
122. Opinion concernant le principe de finalité, préc., note 119, p. 12, 15 et 16.
123. *Id*. Le G29 reconnaît la nécessité de prendre en considération le contexte de la collecte des données quant au niveau de détails à fournir à propos de la finalité de la collecte (voir l'annexe 3, exemples 1, 3 et 13). Dans tous les cas, l'on devrait se limiter aux informations clés, lesquelles sont fournies aux personnes concernées de manière

finalité de la collecte est *explicite*, elle est clairement révélée, elle est expliquée ou exprimée sous une forme intelligible. Au nom de la transparence, l'intention poursuivie est signifiée sans ambiguïté et elle est comprise de la même façon par l'ensemble des parties prenantes, c'est-à-dire autant par le responsable du traitement, ses sous-traitants et les autorités de contrôle que par les personnes concernées elles-mêmes[124].

Au demeurant, il faut résister à la tentation de limiter la finalité *légitime* à la finalité qui est conforme aux bases légales (ou aux conditions de licéité du traitement) énoncées à l'article 6 du RGPD. Cette disposition, il est vrai, introduit le deuxième principe auquel l'AIPD est assujettie, mais elle ne fonde que partiellement la définition de la notion de *légitimité*. En effet, le G29 interprète la finalité *légitime* comme la finalité qui est légale (*lato sensu*) ; la collecte des données à caractère personnel jouit d'une finalité *légitime* dans la mesure où cette finalité respecte toute disposition applicable dans les circonstances, qu'elle soit de nature législative, jurisprudentielle, coutumière, etc. Par conséquent, dans certains cas, en plus des exigences propres au RGPD (établissant, par exemple, que la finalité de la collecte doit être conforme à au moins une des six bases légales de l'article 6 et en respecter toutes les conditions sous-jacentes), le responsable du traitement peut devoir se conformer à plusieurs autres prescriptions de sources diverses provenant, entre autres, de la réglementation des rapports de consommation ou des relations de travail, de l'encadrement des transactions gouvernement-citoyen, etc.[125] Précisons en outre que, sauf quelques exceptions[126], il n'est pas possible de traiter ultérieurement les données collectées d'une manière *incompatible* avec les finalités (déterminées, explicites et légitimes) initiales. Le traitement ultérieur s'entend de tout traitement consécutif à la collecte des données[127]. Pour être admissible, ce traitement doit réussir un test de compatibilité administré par le responsable du traitement[128].

---

très concise et conviviale. S'il y a lieu, le G29 recommande de renvoyer les parties intéressées (via un hyperlien) à une page Internet secondaire où des informations supplémentaires seraient affichées.

124. *Id.*, p. 17. Le G29 insiste sur le fait que la compréhension que les parties prenantes doivent avoir des finalités ne peut être altérée par des facteurs comme l'origine culturelle ou linguistique, le niveau de littératie ou des besoins particuliers. Le cas échéant, des mesures d'accommodement doivent être envisagées.
125. *Id.*, p. 19.
126. *Id.* Ces exceptions visent notamment le traitement ultérieur à des fins archivistiques dans l'intérêt public, aux fins de recherche scientifique ou historique ou encore à des fins statistiques. Voir aussi le considérant nº 156 et l'article 89 du RGPD, préc., note 7.
127. Opinion concernant le principe de finalité, préc., note 119, p. 20.
128. *Id.*, p 23-27.

Hormis les principes de finalité et de licéité, il faut prendre en compte deux autres principes pour déterminer si une AIPD ou une méthode d'AIPD donnée respecte les critères de nécessité et de proportionnalité : la minimisation des données et la limitation de la conservation des données[129]. Le principe de minimisation des données est énoncé à l'article 5 (1) (c) et exige que les données à caractère personnel soient « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Dans ce sens, il est apparu excessif ou disproportionné de collecter le numéro de sécurité sociale de tous les candidats à un emploi quand, en pratique, cette donnée n'est requise que du candidat retenu[130]. De même, dans une affaire concernant la société de vente à distance de chaussures SPARTOO SAS, il a été jugé excessif et par conséquent contraire à l'article 5 (1) (c) le fait, pour cette société, d'exiger des cyberconsommateurs la numérisation de la carte de santé, en plus de la pièce d'identité, pour justifier de l'identité de ces derniers aux fins de lutte contre la fraude. La formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL)[131] a estimé que « seule la collecte de la carte d'identité était pertinente au regard de la finalité du traitement mis en œuvre. En l'espèce, la collecte de la carte de santé contenant davantage d'informations que la carte d'identité, non pertinentes dans le cadre de la lutte contre la fraude, était excessive[132] ».

Quant au principe de limitation de la conservation des données, il découle de l'article 5 (1 e). Selon ce principe, les données à caractère personnel doivent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées[133] ».

---

129. Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD) ; norme ISO/IEC 29134, préc., note 52, section 6.3.3.
130. Groupe de travail « Article 29 » sur la protection des données, *Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel*, 5062/01 FR/Final WP 48, adopté le 13 septembre 2001, p. 23 : l'avis porte sur l'article 6 de l'ancienne directive (Directive 95/46/CE, préc., note 37) qui prévoyait que les données à caractère personnel devaient être « adéquates, pertinentes et non excessives ».
131. La formation restreinte de la CNIL est un organe de la Commission nationale de l'informatique et des libertés de France qui rend des décisions et prononce des mesures en cas de non-conformité au RGPD et à la loi.
132. *Délibération de la formation restreinte nº SAN-2020-003 du 28 juillet 2020 concernant la société SPARTOO SAS*, par. 41, [En ligne], [www.legifrance.gouv.fr/cnil/id/CNILTEXT000042203965/] (16 avril 2023) (ci-après « Délibération nº SAN-2020-003 »). Pour des commentaires de la décision, voir notamment Alain Bensoussan, Virginie Bensoussan-Brulé et Jérémy Bensoussan, *Jurisprudence. Données personnelles 2018-2020 : Décisions tendances*, Paris, Lexing, 2021, p. 207 et suiv.
133. Délibération nº SAN-2020-003, préc., note 132.

Dans l'affaire *SPARTOO SAS* précitée, la mise en cause avait fixé à deux ans la durée de conservation des données de ses anciens clients, période pendant laquelle elle entendait promouvoir ses produits auprès de ces derniers. En revanche, la durée de conservation des données des prospects était de cinq ans, la société la justifiant par le caractère généraliste de sa plateforme de commerce électronique. Or, si le terme de deux ans est apparu proportionné au vu de la finalité du traitement (en l'espèce, aux fins de prospection), la formation restreinte de la CNIL a conclu que la durée de cinq ans, s'agissant des données des prospects, excède la durée nécessaire au regard des finalités pour lesquelles ces données sont traitées[134]. Il s'agit, en définitive, de limiter la durée de conservation des données au strict minimum[135]. La formation restreinte de la CNIL considère que trois ans, à compter du dernier contact que la personne concernée a avec l'entreprise, constituent une référence permettant d'apprécier une durée de conservation appropriée[136].

Relativement aux deuxièmes mesures, c'est-à-dire celles qui contribuent aux droits des personnes concernées, l'AIPD doit permettre de dire si les opérations de traitement à l'étude sont transparentes quant aux informations, communications et modalités d'exercice des droits de ces personnes[137]. Six droits sont visés[138]. Naturellement, la conformité recherchée va au-delà de l'information de la personne concernée, c'est-à-dire qu'il n'est pas suffisant, pour le responsable du traitement, d'énumérer ou de divulguer toutes les mentions obligatoires au sujet de ces droits. La

134. *Id.*, par. 43-53.

135. RGPD, préc., note 7, considérant nº 39.

136. *Délibération de la formation restreinte nº SAN-2020-008 du 18 novembre 2020 concernant la société CARREFOUR FRANCE*, par. 32 [En ligne], [www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756] (16 avril 2023). La formation restreinte de la CNIL se base notamment sur le projet de *Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales*, [En ligne], [www.legifrance.gouv.fr/jorf/id/JORFTEXT000045538574] (16 avril 2023) (ci-après « Référentiel CNIL »). Selon ce projet de référentiel (adopté et publié au Journal officiel de la République française nº 0085 du 10 avril 2022), le dernier contact d'un client peut être un achat ou la date d'expiration d'une garantie ; pour le prospect, il peut s'agir d'un « clic sur un lien hypertexte contenu dans un courriel renvoyant vers le produit promu » (p. 11).

137. Cette obligation d'information est énoncée aux articles 12 à 14 du RGPD, préc., note 7. Les mesures envisagées dans le cadre de l'opération de traitement faisant l'objet de l'AIPD doivent s'y conformer. Voir les Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD).

138. Ces droits sont les suivants : le droit d'accès, le droit à la portabilité des données, le droit de rectification, le droit à l'effacement ou droit à l'oubli, le droit d'opposition et le droit à la limitation du traitement. Voir respectivement les articles 15, 20, 16, 18, 19 et 21 du RGPD, préc., note 7.

conception (technique) de l'opération de traitement doit, en plus, rendre ces droits effectifs. Dans ce sens, l'exercice du droit à la limitation du traitement, par exemple, doit mener à l'activation de mesures techniques et organisationnelles appropriées, comme celles que décrit le considérant nº 67 du RGPD, à savoir « déplacer temporairement les données sélectionnées vers un autre système de traitement », « rendre les données […] inaccessibles aux utilisateurs », les retirer temporairement d'un site Internet ou, s'agissant de fichiers automatisés, empêcher que les données fassent l'objet de traitements ultérieurs ou soient modifiées. Le sous-traitant est tenu des mêmes exigences. Le cas échéant, les garanties entourant les transferts internationaux des données sont consignées dans l'AIPD[139].

L'ultime critère d'acceptabilité de l'AIPD évoque la notion de risque.

2.2.3 L'évaluation et la gestion des risques pour les droits et libertés des personnes concernées

Le responsable du traitement est soumis à deux questions pratiques :

1) Quelle est l'ampleur des risques des opérations de traitement pour les droits et libertés des personnes concernées[140] ?
2) Comment gérer ces risques ?

Pour répondre à ces questions, le responsable du traitement doit s'appuyer sur la description systématique qu'il a faite des opérations de traitement, incluant les garanties relatives au principe de nécessité et de proportionnalité. S'il y a des risques résiduels élevés, risques qui continueraient d'exposer les personnes à des conséquences importantes, irréversibles[141], pour lesquels le responsable du traitement est incapable d'identifier des mesures d'atténuation suffisantes, c'est-à-dire des mesures pouvant réduire le risque à un niveau acceptable[142], l'article 36 du RGPD oblige ce responsable à consulter l'autorité de contrôle en lui communiquant, entre autres, l'intégralité de l'AIPD.

Concernant la première question (« Quelle est l'ampleur des risques des opérations de traitement pour les droits et libertés des personnes

139. RGPD, préc., note 7, art. 28 et chap. V ; Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD).
140. RGPD, préc., note 7, art. 35 (7) (c) ; Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD).
141. Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD).
142. L'incapacité d'atténuer les risques résiduels élevés peut être due à l'indisponibilité des techniques pertinentes et aux coûts liés à leur mise en œuvre. Cette hypothèse est envisagée par le considérant nº 84 du RGPD, préc., note 7.

concernées ? ») : elle doit être comprise selon les considérants nos 77 et 83 du RGPD. La question conduit ainsi à déterminer l'origine, la nature, la particularité, la probabilité et la gravité de tout scénario décrivant un événement et ses effets sur les droits et libertés des personnes.

Au départ, les actifs (humain, matériel, logiciel, etc.), sur lesquels reposent les données à caractère personnel et leur traitement, sont sujets à une série de menaces, qui sont des ensembles de faits ou de signes faisant craindre des événements néfastes[143]. La norme ISO/IEC 29134 identifie six faits (ou menaces courantes) : d'après leur nature, les actifs peuvent subir un détournement d'usage ; ils peuvent être endommagés ; ils peuvent être infiltrés et observés clandestinement ; on peut être privé de ces actifs ; ou encore ils peuvent être altérés ou surexploités. Ces faits ou menaces courantes font craindre une longue liste d'événements néfastes dont trois, en particulier, doivent être documentés dans l'AIPD dans la mesure où ils ont un effet sur les droits et libertés des personnes concernées : 1) la perte de confidentialité, c'est-à-dire l'aliénation du caractère secret des données, l'accès illégitime aux données ; 2) la perte d'intégrité, soit l'altération non désirée des données ; et 3) la perte de disponibilité, qui est envisagée comme la disparition des données[144].

Il faut ensuite déterminer l'impact potentiel de chacun de ces trois événements ou leurs conséquences possibles, c'est-à-dire déterminer à quel point ces événements peuvent être néfastes ou nuisibles. Cet impact est *négligeable* quand l'événement a peu ou n'a pas d'inconvénients pour les personnes concernées ; il est *limité* quand ces dernières sont confrontées à des inconvénients importants, qu'elles pourront surmonter nonobstant quelques difficultés ; l'impact est *significatif* lorsque, pour surmonter ces inconvénients importants, les personnes concernées sont sujettes à de sérieuses difficultés (par exemple, l'atteinte à leur réputation) ; un impact *maximal*, enfin, suppose des conséquences importantes, voire irréversibles, lesquelles, au surplus, sont insurmontables (comme le décès de la personne concernée)[145]. Une échelle similaire, en dernier ressort, doit servir à évaluer la probabilité d'exécution des menaces, à savoir dans quelle mesure les propriétés des actifs sur lesquels reposent les données et leur traitement peuvent être exploitées pour exécuter les menaces identifiées et provoquer les événements néfastes et leurs conséquences. La probabilité d'exécution d'une menace sera jugée négligeable, limitée, significative

143. DAC, préc., note 9, *s.v.* « Menace ».

144. Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD). La norme ISO/IEC 29134, préc., note 52, section 6.4.4.1. et annexe B, ajoute d'autres événements néfastes.

145. Norme ISO/IEC 29134, préc., note 52, annexe A.

ou maximale selon qu'il apparaîtra respectivement impossible, difficile, possible ou extrêmement facile d'exploiter les propriétés de ces actifs pour exécuter la menace. L'annexe A de la norme ISO/IEC 29134 l'illustre dans l'exemple suivant : la probabilité que des documents papier stockés dans une pièce soient volés (ce qui entraînerait, par exemple, une perte de disponibilité des données contenues dans ces documents) peut être jugée négligeable si cette pièce est protégée par un dispositif restreignant son accès, comme un lecteur de badge ou une serrure à code d'accès. Dans un tel scénario, les données reposent sur des actifs dont les propriétés, c'est-à-dire le support papier des documents, l'espace clos de stockage et le contrôle d'accès de cet espace, permettent de minimiser la menace[146]. En revanche, la probabilité d'un vol serait maximale si les mêmes documents étaient simplement stockés dans un espace public ouvert, tel un hall (le vol des documents, dans ce contexte, semble en effet extrêmement facile)[147].

Concernant la seconde question (« Comment gérer ces risques ? ») : le responsable du traitement est appelé à identifier les garanties, les mesures et les mécanismes de sécurité qui sont nécessaires pour diminuer ou rendre moins important le risque de perte de confidentialité, de perte d'intégrité ou de perte de disponibilité des données[148]. La protection des données s'en trouverait assurée, et le responsable du traitement serait en mesure d'apporter la preuve du respect du RGPD[149]. Selon l'opération de traitement anticipée, il peut s'agir de mesures organisationnelles (sensibiliser les utilisateurs, adopter des politiques de protection des données, gérer les incidents, etc.) et de mesures techniques ou de sécurisation du système d'information (tracer les accès, sécuriser les serveurs ou les sites Web en limitant l'accès aux interfaces d'administration ou en utilisant le protocole Transport Layer Security (TLS) qui tire parti des algorithmes de chiffrement pour l'authenticité et la confidentialité des échanges de données, etc.)[150].

Revenant au contexte québécois et à notre exemple de l'application de technologie financière, l'approche minimaliste de la nouvelle version de la Loi sur le secteur privé relativement à l'EFVP des projets de SI et de

146. *Id*.
147. *Id*.
148. Considérant nº 90 du RGPD, préc., note 7.
149. RGPD, préc., note 7, art. 35 (7) (d) ; Lignes directrices concernant l'AIPD, préc., note 30, annexe 2 (Critères d'acceptabilité d'une AIPD).
150. Référentiel CNIL, préc., note 136, p. 6 et 7 ; GDT, s.v. « Protocole TLS » ; CNIL, *Analyse d'impact relative à la protection des données – La méthode*, février 2018, p 7, [En ligne], [www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf] (16 avril 2023).

PES est ouvertement écartée lorsqu'une entreprise entend communiquer un renseignement personnel à l'extérieur du Québec ou lorsqu'elle confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver, pour son compte, un tel renseignement[151]. Ce serait l'hypothèse de notre technologie financière dans la mesure où celle-ci a recours à des services infonuagiques avec des centres de données situés à l'extérieur du Québec. Dans ce cas particulier, le législateur est plus directif, comme si l'enjeu de la protection des renseignements personnels était différent ou plus prégnant à l'égard des flux transfrontières. En l'occurrence, non seulement l'EFVP est une exigence préalable à satisfaire, mais l'évaluation doit tenir compte de divers éléments fondamentaux dont l'énumération rappelle clairement les critères de l'AIPD que l'on vient d'analyser. Au Québec, l'entreprise doit considérer la sensibilité du renseignement à caractère personnel (il s'agit de l'un des neuf critères à la lumière desquels le responsable du traitement peut décider si une AIPD est nécessaire pour une opération de traitement du fait d'un risque élevé inhérent) ; la finalité de son utilisation (cet élément correspond au principe de finalité abordé sous les critères de nécessité et de proportionnalité de l'AIPD) ; les mesures de protection dont le renseignement bénéficierait (dans l'AIPD, cet élément est traité sous le critère relatif au risque et sous-entend une cartographie des menaces, du risque, de son impact et de sa probabilité d'exécution). De plus, le régime juridique applicable dans l'État de destination doit être considéré[152]. Même alors, une entente écrite est nécessaire. Celle-ci doit tenir compte des résultats de l'EFVP et, le cas échéant, elle doit prévoir des mesures pour atténuer les risques identifiés.

Devant l'approche minimaliste du texte québécois (concernant les projets de SI ou de PES), l'analyse comparée a permis d'esquisser quelques éléments fondamentaux de la réalisation de l'EFVP afin d'illustrer les exigences en la matière concernant notamment les technologies financières. L'intention n'est pas d'inciter l'importation telle quelle de ces éléments en raison des contextes différents dans lesquels s'inscrivent l'EFVP et l'AIPD. Des adaptations seront nécessaires. Il est aisé de constater à partir de l'expérience européenne que l'apport des guides et des lignes directrices ne retire pas la pertinence d'orientations fondamentales sur la réalisation de l'EFVP dans le cadre d'un texte législatif. La seule prescription d'une

151. Loi sur le secteur privé, préc., note 6, art. 17 (nouveau). La disposition excepte la communication prévue au paragraphe 7 du premier alinéa de l'article 18 (communication en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée).

152. *Id.*, art. 17 al.1 (4º) (nouveau).

proportionnalité de l'EFVP selon le projet de SI ou de PES ne saurait suffire à rassurer. L'exercice amorcé dans l'hypothèse de la communication des renseignements à l'extérieur du Québec n'est qu'une preuve supplémentaire de l'utilité de telles orientations dans la Loi.

Conclusion

Le RGPD se distingue de la nouvelle version de la Loi sur le secteur privé concernant l'AIPD. Le règlement propose des critères d'acceptabilité précis et uniformes. Normalement, l'AIPD débouche sur un rapport que le responsable du traitement n'a pas l'obligation de publier. Mais il peut rendre disponibles un résumé ou les conclusions, ce qui est de bonne pratique selon le G29, dans la mesure où le document fournit « des gages de responsabilité » et « de transparence », outre qu'il suscite « la confiance » dans l'opération de traitement qui est entreprise[153].

Les critères d'acceptabilité de l'AIPD pourraient-ils orienter la réalisation de l'EFVP ? Les recommandations consécutives à l'enquête concernant Tim Hortons ont déjà confirmé certains des critères dans le cadre de l'EFVP, notamment les critères de nécessité et de proportionnalité. Or, le niveau de détails des critères européens est tel que de les appliquer systématiquement à tout projet de SI et de PES entraînerait un fardeau peut-être trop important pour les entreprises. Il semble que le législateur québécois ait renoncé à imposer ce fardeau.

À tout considérer, il y a deux cas de figure en droit québécois : 1) un encadrement minimaliste de l'EFVP réalisée pour les projets de SI ou de PES ; et 2) un encadrement plus précis, en apparence plus contraignant, de l'EFVP effectuée en vue des flux transfrontières de données (c'est aussi le cas, dans une certaine mesure, lors de la communication d'un renseignement personnel à des fins d'études, de recherche ou de production de statistiques[154]). L'avenir nous dira si, par ce dualisme, le législateur parvient à un équilibre réel entre le fardeau qu'il impose aux entreprises assujetties à l'EFVP et l'objectif de protection des renseignements personnels.

153. Lignes directrices concernant l'AIPD, préc., note 30, p. 21.
154. *Id.*, art. 21 (4°) et (5°) (nouveau) : la communication peut s'effectuer si l'EFVP conclut que « les renseignements personnels sont utilisés de manière à en assurer la confidentialité [et que] seuls les renseignements nécessaires sont communiqués ».