Dernière mise à jour présentée à la 43e Assemblée mondiale sur la protection de la vie privée, Mexico, du 18 au 21 octobre 2021

Présenté initialement à la 37e Conférence internationale des commissaires à la protection des données et de la vie privée, Amsterdam, du 26 au 29 octobre 2015.

UN GUIDE SUR LA COOPÉRATION DANS L'APPLICATION DES LOIS

Préparé par :
Le Commissariat à la protection de la vie privée du Canada et
Le Commissariat à l'information du Royaume-Uni

Avec le soutien de :
L'Autorité colombienne de surveillance de l'industrie et du commerce et
Le Commissariat à l'information de Jersey

GPA
Global Privacy Assembly

Table des matières

Introduction

L'Entente mondiale de coopération transfrontière dans l'application des lois de 2014 (« l'Entente ») de la Conférence internationale des commissaires à la protection des données et de la vie privée[1] constituait une « déclaration d'intention générale » en vue d'assurer la coopération entre autorités[2] d'application des lois sur la protection de la vie privée et proposait un cadre visionnaire pour y parvenir.

Initialement, ce guide a été créé afin de donner aux autorités un outil qui leur permettrait de faire leurs premiers pas en vue de participer à l'Entente et de chercher de nouvelles avenues de collaboration. Depuis ces débuts, la coopération mondiale en matière d'application de la loi de protection de la vie privée a augmenté de façon constante et a procuré de nombreux avantages, dont bon nombre seront illustrés dans le présent document. Compte tenu des développements et des progrès dans ce domaine, le Groupe de travail sur la coopération internationale dans l'application des lois (IEWG) s'est employé à recueillir et à partager les leçons tirées par diverses autorités afin d'élaborer un guide pour appuyer et promouvoir la coopération future et une mobilisation accrue à l'échelle mondiale en vue de lutter contre des comportements problématiques liés à la protection des renseignements personnels et des données.

Fondée sur la rétroaction reçue de diverses autorités, cette version mise à jour du guide met l'accent sur les éléments pratiques de la coopération et regroupe, comme points de référence, des études de cas et des exemples d'activités de coopération dans l'application des lois qui ont eu lieu au cours des dernières années.

Le présent guide n'est pas de nature pédagogique ni normative. Il incombe à chaque autorité de déterminer de quelle façon elle souhaite participer à la coopération en matière d'application des lois et en tirer parti. Le guide vise plutôt à donner une orientation utile aux autorités désireuses de coopérer dans l'application des lois et comprend notamment :

i. une liste non exhaustive des enjeux que pourrait rencontrer une autorité qui se prépare à coopérer ou coopère dans l'application des lois;

ii. des modèles, des approches et des solutions éventuelles que les autorités pourraient envisager de mettre en œuvre pour intervenir à l'égard de ces enjeux;

iii. des facteurs à prendre en compte pour déterminer quelles stratégies proposées pourraient être appropriées dans certaines situations.

---

[1] Maintenant appelée l'Assemblée mondiale de la protection de la vie privée (AMVP).

[2] Pour les besoins du présent guide, l'expression « autorités d'application des lois sur la protection de la vie privée » englobe également les autorités chargées de protection des données. De même, la notion de « protection de la vie privée » englobe la protection des données.

Les autorités devraient toujours faire preuve de souplesse et d'innovation dans l'application des approches présentées dans le présent guide. Chaque élément de la situation (p. ex., autorités pertinentes, législation, enjeux et parties à un dossier) nécessite une approche unique en son genre. Il pourrait aussi s'agir d'une forme hybride des approches présentées en détail dans le présent guide, voire d'une approche novatrice complètement différente que nous n'avons pas envisagée ci-après.

Le guide n'est pas fondé sur une législation en particulier, car nous sommes conscients qu'il serait extrêmement difficile de traiter dans le présent document de la vaste gamme de dispositions législatives et de politiques nationales en vigueur.

Collaboration interréglementaire

Les données sont au cœur de notre économie numérique et ne se conforment pas aux limites réglementaires ou géographiques. Cela se reflète dans l'importance croissante accordée aux questions d'intersection qui prennent la forme de nouvelles lois et de nouveaux règlements, d'initiatives stratégiques, de demandes de renseignements et de mesures accrues d'application de la loi prises par les autorités dans les sphères réglementaires. Bien que la coopération dans le domaine de la protection des renseignements personnels soit relativement vaste et de plus en plus fréquente, la coopération interréglementaire, particulièrement entre autorités responsables de la concurrence, en est seulement à ses débuts.

Nous avons donc remanié le guide, en collaboration avec le Groupe de travail sur les citoyens et les consommateurs en matière numérique » (GTCCMN) de l'Assemblée mondiale de la protection de la vie privée (AMVP), pour mettre en évidence et appuyer la coopération interréglementaire. La coopération entre les autorités chargées de l'application des lois en matière de protection des renseignements personnels et d'autres organismes de réglementation peut offrir des moyens nouveaux et utiles pour s'attaquer aux comportements problématiques de façon holistique. À titre d'exemple, les enjeux de protection des renseignements personnels peuvent souvent recouper des enjeux relatifs à la concurrence et à la protection des consommateurs, et ce, de façons nouvelles et complexes, comme le soulignent les rapports annuels 2019 et 2021 du GTCCMN.

Dans ce domaine, la coopération est particulièrement importante et opportune, car nous constatons l'émergence et la transformation de modèles d'affaires axés sur les données qui exploitent les données et les renseignements personnels de façon novatrice et les intègrent à tous les niveaux du processus commercial. Un tableau de concordance contenant des exemples de recoupement des activités se trouve dans le rapport annuel 2021 du GTCCMN.

Les efforts déployés récemment par l'AMVP, le Global Privacy Enforcement Network (**GPEN**, soit le réseau mondial d'application des lois pour la protection de la vie privée) et le Réseau international de contrôle et de protection des consommateurs (**RICPC**) ont souligné ce besoin dans le cadre d'ateliers axés sur des activités d'application de la réglementation croisée et d'expériences concrètes de différentes autorités. Pendant l'atelier de 2019 des praticiens du GPEN, organisé conjointement par le Bureau de la protection des données personnelles du gouvernement de Macao (Chine) et le

Commissariat à la protection des données personnelles de Hong Kong (Chine), les participants ont examiné des activités et des stratégies conjointes pour lutter contre les difficultés liées à l'interréglementation, ainsi que des exemples de pratiques exemplaires.

Ces questions ont fait l'objet de discussions supplémentaires la même année au Digital Clearinghouse, un forum mis sur pied par le contrôleur européen de la protection des données. Les points à retenir de ces discussions se trouvent aux **annexes E et F** du rapport annuel du GTCCMN de 2019 (rapport disponible en anglais seulement) et comprennent notamment les points suivants :

- Il existe un chevauchement croissant entre les autorités de réglementation, que ce soit sur le plan de la compétence, des questions juridiques ou pratiques communes en matière de protection des données ou des pratiques commerciales déloyales auxquelles participent de nombreuses autorités[3].

- Il existe une importante collaboration interréglementaire au niveau stratégique, qui peut servir de fondement à la coopération future aux fins d'application des lois.

- Dans un certain nombre de cas, les autorités de la protection des données (**APD**) et d'autres organismes de réglementation ont participé ensemble à des consultations publiques.

- La compréhension de l'intersection entre la protection des renseignements personnels et d'autres sphères réglementaires, et l'élaboration de stratégies de collaboration interréglementaire en matière d'application des lois, ne font que commencer, mais se développent.

- Un des thèmes récurrents notables est la coopération accrue entre les APD et les autorités responsables de la lutte contre la cybercriminalité et de la cybersécurité, y compris un certain nombre d'exemples de coopération avec la police.

- L'établissement de relations et la désignation de points de contact entre les autorités revêtent une importance cruciale. La confiance et les liens entre les points de contact peuvent parfois faire une différence importante dans la création de conditions favorables à la collaboration.

De plus, en février 2021, lors d'un atelier sur les pratiques exemplaires du RICPC et du GPEN, des professionnels de la protection de la vie privée et de la protection des consommateurs de partout dans le monde ont discuté d'une étude de cas hypothétique portant sur des enjeux liés à une possible intersection réglementaire et à une possible coopération transréglementaire. Les participants ont reconnu l'importante intersection et la complémentarité entre leurs deux sphères réglementaires, ainsi que la possibilité d'une collaboration mutuellement avantageuse dans ce domaine.

[3] Voici quelques exemples : atteinte à la sécurité des données, commerce électronique, fusions dans les secteurs de la technologie, télémarketing, pourriels et pratiques commerciales déloyales liées aux données personnelles (particulièrement dans le contexte des entreprises technologiques).

Plus précisément, les participants ont cerné la nécessité pour les autorités de protection de la vie privée et des consommateurs de trouver des occasions de collaborer et d'établir des partenariats qui pourraient servir de fondement à une future coopération dans l'application des lois. Vous trouverez de plus amples renseignements sur cette séance dans le rapport annuel du GPEN de 2021 à venir.

Au fur et à mesure que les données et les renseignements personnels continuent d'avoir une importance accrue dans les évaluations concurrentielles et une incidence sur les droits des consommateurs, la façon d'aborder et d'améliorer la coopération transréglementaire deviendra une question de plus en plus urgente.

Le présent guide tient compte de la collaboration interréglementaire à travers chaque facette du processus coopératif et met en avant les travaux récents du GTCCMN et d'une variété d'autorités pour présenter des outils, des méthodes, des exemples et des études de cas, permettant ainsi aux autorités d'envisager des travaux interréglementaires.

Avantages de la coopération dans l'application des lois

De plus en plus, les organisations qui traitent des données personnelles exercent une présence multinationale, tant sur le plan physique que dans le domaine du commerce numérique. La fluidité et la fréquence de la circulation transfrontière des données ont fait de la coopération internationale en matière d'application des lois un outil nécessaire à la promotion des droits à la vie privée à l'échelle nationale et internationale. Dans le vrai sens du terme, cette coopération peut être un exercice d'amélioration de l'efficacité et de renforcement de la capacité. L'indépendance des autorités peut également bénéficier du renforcement de la coopération avec d'autres organismes de réglementation, puisque celle-ci aidera à compenser pour les difficultés budgétaires et à amortir les effets des pressions politiques à l'échelle nationale. Les avantages de la coopération continuent de se manifester à mesure que la coopération en matière d'application des lois se répand :

- Les autorités peuvent obtenir des résultats de façon plus efficiente grâce à une enquête ou à une mesure concertée d'application des lois au lieu de démultiplier les mesures faisant double emploi.

- En travaillant ensemble, les autorités peuvent tirer parti de leur « poids » cumulatif et de leurs points forts relatifs afin que leurs mesures d'application des lois donnent des résultats ayant une incidence, même dans les sphères réglementaires, qu'elles ne pourraient pas obtenir individuellement.

- Grâce au partage de renseignements et à l'entraide dans les enquêtes, les autorités pourraient être en mesure de mener ou de faciliter des activités d'application des lois ou des enquêtes qui comprennent des activités à l'extérieur de leur propre territoire.

- Au cours du processus de coopération, chaque autorité peut apprendre grâce aux connaissances et à l'expérience des autres et renforcer par le fait même le savoir-faire individuel et collectif.

- Les autorités pourraient tirer parti de différents fuseaux horaires pour augmenter considérablement la productivité. Dans certains cas, elles obtiendraient ainsi une couverture presque en tout temps leur permettant d'accomplir beaucoup plus de travail dans un court délai de temps.

- Comme les données ne se conforment pas aux limites réglementaires, travailler en collaboration avec d'autres autorités interréglementaires peut aboutir à des résultats qui font progresser les objectifs des deux régimes sans sacrifier l'un ou l'autre; et

- Le milieu mondial de l'application des lois sur la protection de la vie privée fait savoir aux organisations traitant des données personnelles, ainsi qu'aux particuliers partout dans le monde, que nous regroupons nos efforts et que nous sommes engagés à intervenir à l'échelle internationale pour éliminer les risques d'atteinte à la vie privée d'envergure mondiale.

Coopération en matière d'événements émergents et de tendances stratégiques

Les développements récents ont montré qu'il est viable pour les autorités de collaborer dans les cas où les événements majeurs et où les tendances générales sont importantes à l'échelle mondiale. Ces activités de collaboration importantes ont permis d'établir les attentes d'un plan d'action multilatérale et de jeter les bases de la coopération en matière d'application de la loi. Les tendances et événements suivants constituent seulement quelques exemples qui ont démontré l'importance et l'efficacité d'une réponse mondiale aux nouveaux enjeux et tendances :

Événements majeurs – COVID-19

La pandémie de COVID-19 a présenté d'importantes difficultés en matière de protection des renseignements personnels et des données pour les autorités partout dans le monde alors que les organisations commerciales et les gouvernements ont été obligés de s'adapter rapidement à la nouvelle réalité mondiale. Des données personnelles sont devenues essentielles à l'application d'initiatives en santé, comme la recherche des contacts, les interventions en cas d'éclosion et la

gestion de la vaccination, ainsi que pour d'autres changements associés à la pandémie, comme la scolarisation en ligne et un virage à grande échelle vers le travail à distance[4].

Les problèmes de confidentialité liés à la pandémie de COVID-19 étaient si aigus que le Comité exécutif de l'AMVP a convoqué une réunion extraordinaire en avril 2020 pour y remédier. L'AMVP a donc formé le Groupe de travail 2020 sur la COVID-19 (site en anglais seulement), composé d'autorités du monde entier. Ce groupe de travail international a analysé et rendu compte (document en anglais seulement) des problèmes liés à la COVID-19, a produit un recueil de pratiques exemplaires (document en anglais seulement) et a appuyé la résolution de l'AMVP sur les défis liés à la protection de la vie privée et des données en raison de la pandémie de COVID-19 (document en anglais seulement). Cette approche mondiale a permis d'adopter une démarche holistique et unie pour régler les problèmes liés à la protection de la vie privée dus à la pandémie de COVID-19, de tirer parti des ressources et des talents à l'échelle mondiale et de favoriser l'établissement de relations solides entre les autorités. Elle a également permis aux membres de mettre en commun, sans obstacle, leur expertise.

De même, le GPEN a mené deux initiatives visant à examiner les répercussions de la COVID-19 sur l'application des lois relatives à la protection des renseignements personnels. Le ratissage pour la protection de la vie privée du GPEN de 2020 (en anglais seulement) visait à déterminer si, à l'échelle mondiale, les initiatives et les solutions liées à la COVID-19 qui ont été mises en œuvre par les gouvernements et les organismes du secteur privé avaient bien tenu compte de la protection de la vie privée. Dans le cadre d'une initiative parallèle du GPEN, intitulée « Resetting privacy », dirigée par le Commissariat à l'information du Royaume-Uni et appuyée par 27 autorités, on a examiné les répercussions de la pandémie sur les activités de réglementation et d'application de la loi des autorités de protection de la vie privée et des consommateurs.

Tendances stratégiques – Technologie de reconnaissance faciale

La technologie de reconnaissance faciale (TRF) représente un problème stratégique majeur sur le plan de la protection de la vie privée pour les autorités partout dans le monde. La TRF utilise des données biométriques, généralement considérées comme étant intrinsèquement sensibles, et leur objectif fondamental d'identification soulève un certain nombre de préoccupations en matière de protection des renseignements personnels. Le recours aux TRF est de plus en plus répandu et est utilisé par diverses organisations partout dans le monde, allant de la sécurité nationale et de l'application de la loi aux organisations commerciales offrant ou utilisant des services d'identification et d'authentification.

En réaction à l'augmentation rapide du recours à la reconnaissance faciale, l'AMVP a adopté une résolution sur la technologie de reconnaissance faciale, dans laquelle elle reconnaît l'utilité et la valeur de la TRF, mais aussi les préoccupations et les risques importants qui l'entourent à l'échelle mondiale. Pour analyser la question et y donner suite, l'IEWG et le Groupe de travail sur la protection des

[4] Pour voir un exemple d'initiative conjointe sur le travail à distance, veuillez consulter l'étude de cas à la page 29.

données et l'éthique dans le domaine de l'intelligence artificielle (GTIA) ont conjointement formé le Groupe de travail sur la technologie de reconnaissance faciale (**GTTRF**), un groupe international d'autorités intéressées par la question. Ce groupe de travail a notamment pour mandat :

- d'examiner les risques liés à la TRF
- de formuler des recommandations visant à atténuer ces risques
- d'élaborer et de promouvoir un ensemble de principes et d'attentes que les développeurs et les utilisateurs de la TRF dans le monde devraient respecter pour assurer que les renseignements personnels et la vie privée soient protégés adéquatement

Les travaux à ce sujet se poursuivent au moment de la publication du présent rapport, et d'autres précisions seront affichées sur le site Web de l'AMVP lorsque le rapport annuel du GTTRF sera publié. En plus de créer le GTTRF, l'IEWG a tenu un certain nombre de séances de collaboration consacrées à la technologie de reconnaissance faciale et a mené des enquêtes portant sur la TRF. Au cours de ces séances, diverses autorités ont pu en apprendre davantage sur la TRF, et partager des idées et des informations à ce sujet.

Tendances stratégiques – L'économie numérique accélère les cas de chevauchement réglementaire

L'économie numérique a entraîné la superposition des sphères réglementaires de la protection de la vie privée, de la concurrence et de la protection des consommateurs d'une manière qui n'avait jamais été étudiée ou entièrement comprise auparavant. En raison de ces recoupements présentent, de nombreux compléments réglementaires deviennent des points de tension. On peut soutenir que toutes les autorités, quel que soit le régime, se trouvent à un point d'inflexion sur la voie à suivre, alors qu'elles élaborent des stratégies sur la meilleure façon d'aborder les intersections réglementaires. Ces difficultés et la relation dynamique entre les sphères se sont accentuées en 2020-2021 en raison de la pandémie, qui a accru la dépendance des consommateurs, des entreprises et de la société à tous les éléments du monde numérique.

Les cas de chevauchement réglementaire sont susceptibles d'augmenter en nombre et en complexité à mesure que de plus en plus d'administrations se dirigent vers la création de régimes réglementaires numériques spécialisés. De plus, la capacité des APD de collaborer avec leurs homologues de la protection des consommateurs et de la concurrence sera essentielle à l'atteinte des objectifs réglementaires de chaque sphère. Voici un excellent exemple de cette collaboration en action.

Étude de cas L'enquête de la Commission européenne sur le projet d'acquisition de Fitbit par Google

En août 2020, la Commission européenne (la « CE »), autorité européenne en matière de concurrence) a ouvert une enquête approfondie sur le projet d'acquisition de Fitbit par Google. Comme elle la indiqué dans son communiqué de presse [lien brisé], la CE [traduction] « craint que la transaction proposée ne renforce davantage la position de Google sur les marchés de la publicité en ligne en augmentant la quantité ou les données déjà considérables que Google pourrait utiliser pour personnaliser les publicités qu'elle sert et affiche ». Reconnaissant l'intersection avec la réglementation sur la protection des renseignements personnels, la CE a demandé en juillet 2020 l'aide du Comité européen de la protection des données (EDPB).

Compte tenu de son engagement de longue date à promouvoir le traitement équitable des données personnelles sur les marchés ouverts, en tant que membre de l'EDPB, le contrôleur européen de la protection des données (CEPD) a participé activement à l'enquête de la CE. Cette décision reposait en partie sur la position de longue date du CEPD selon laquelle les lois en matière de concurrence, de protection des consommateurs et de protection des données sont trois domaines stratégiques inextricablement liés dans le contexte de l'économie des plateformes en ligne. Le CEPD considère que la relation entre ces trois domaines devrait être une relation de complémentarité, de convergence et d'application cohérente, et non une relation où un domaine en remplace un autre ou crée des frictions avec celui-ci.

L'un des principaux défis auxquels le CEPD a dû faire face était le court délai imposé par les exigences procédurales de la CE et les échéances strictes. Par conséquent, le CEPD a établi l'ordre de priorité des principaux domaines d'intérêt, en commençant par une analyse des domaines où les répercussions négatives possibles de la fusion pour la protection des renseignements personnels et des données étaient les plus probables. Le CEPD a ensuite mis l'accent sur toute friction liée à la protection de la vie privée et des données qui pourrait être déclenchée par des mesures favorables à la concurrence, par exemple des situations où des tiers pourraient avoir accès aux données personnelles. En fin de compte, les efforts du CEPD lui ont permis de mieux connaître les spécificités du droit de la concurrence et les procédures applicables à l'évaluation des fusions dans le contexte du droit de la concurrence.

Compte tenu de cette expérience, le CEPD est d'avis qu'une coopération institutionnalisée et structurée entre les autorités de protection des données et de concurrence, qui offrirait un cadre juridique clair pour la coopération administrative et la communication d'informations pertinentes, améliorerait grandement la collaboration dans les situations où la protection des données et la concurrence sont en jeu.

Préparation des bases de la coopération

Établissement de relations de coopération dans l'application des lois

Bien que la législation et les ententes d'échange de renseignements permettent de coopérer, et ce, souvent jusqu'à l'échelle mondiale[5], ce sont les relations interorganismes et interpersonnelles dûment entretenues qui ouvrent les voies de communication et qui offrent l'aisance, la confiance et le savoir organisationnel[6], lesquels sont nécessaires pour faire de la coopération une réalité. Pour établir et développer de telles relations, les autorités peuvent se regrouper et participer activement à divers réseaux de coopération en matière de protection de la vie privée et d'application des lois, en prenant part à des appels mensuels ou en se portant volontaire pour contribuer à des initiatives ou siéger au sein de groupes de travail.

- À titre d'exemple, le GTIE tient régulièrement des séances « à huis clos de coopération en matière d'application des lois » au cours desquelles les autorités se réunissent pour discuter de questions d'application de la loi d'intérêt mondial. Parmi les sujets traités précédemment, mentionnons la récupération de données en ligne, la technologie de reconnaissance faciale et le bourrage d'identifiants. Ces séances ont donné lieu à des activités de collaboration aux fins de surveillance de la conformité, notamment :
    - une enquête conjointe du Commissariat à l'information du Royaume-Uni et du Commissariat à la protection de la vie privée de l'Australie dans les pratiques de traitement des renseignements personnels de Clearview AI[7]
    - une lettre conjointe destinée aux entreprises de vidéoconférence ainsi que la mobilisation de ces dernières
    - une initiative, lancée et dirigée par l'Autorité de régulation de Gibraltar, visant à élaborer une orientation à l'intention des entreprises et des particuliers pour atténuer le risque de bourrage d'identifiants[8].

---

[5] La prise en compte de valeurs communes tout au long du processus jusqu'au niveau mondial est déjà nécessaire lorsqu'on considère la façon dont chaque autorité peut mieux servir les intérêts et les droits des particuliers à l'ère du numérique et de la mondialisation. Les différents gouvernements ont notamment des sources d'inspiration commune des textes acceptés à grande échelle (sinon à l'échelle planétaire, sous une forme intentionnellement diversifiée comme c'est le cas à l'heure actuelle) comme l'article 12 de la Déclaration universelle des droits de l'homme : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance ni d'attaques à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. » ou la Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée, formulée en 2007.

[6] En tirant parti des forces, des moyens juridiques et des priorités stratégiques de certaines autorités.

[7] En juillet 2020, le Commissariat à l'information du Royaume-Uni et le Commissariat à la protection de la vie privée de l'Australie ont annoncé publiquement (en anglais seulement) qu'ils menaient une enquête conjointe sur les pratiques de Clearview AI.

[8] Cette orientation devrait être diffusée plus tard en 2021.

- De plus, le Global Privacy Enforcement Network (GPEN) tient des conférences téléphoniques et des réunions mensuelles pour discuter des questions d'application de la loi, des tendances et des expériences des membres participants. En général, deux conférences téléphoniques sont prévues chaque mois. Conformément au caractère international du GPEN, l'un des appels est prévu à l'intention des membres du Pacifique, et l'autre, des membres de l'Atlantique. Pendant ces appels, les discussions ont notamment porté sur l'application des lois en matière de protection des renseignements personnels pendant et après la pandémie de COVID-19, les initiatives de villes intelligentes, la surveillance des examens en ligne et l'utilisation de l'intelligence artificielle dans le secteur public.

- De même, dans le domaine de la coopération interréglementaire, le GTCCMN met l'accent sur l'intersection de la protection de la vie privée, de la protection des consommateurs et de la concurrence. Dans le cadre de son mandat, il offre aux autorités une tribune pour discuter des efforts de collaboration. Ses travaux ont également visé à sensibiliser davantage les participants de diverses tribunes à la nécessité d'accroître la collaboration interréglementaire.

- Les autorités peuvent aussi organiser des rencontres en personne ou des téléconférences pour établir des relations, d'abord entre les dirigeants et d'autres cadres supérieurs des organismes, puis entre les responsables sur le plan opérationnel (p. ex., participation régulière à des appels opérationnels);

- Les autorités peuvent prendre part à des détachements, à des échanges d'employés ou à des activités de formation conjointes, les organismes auront ainsi l'occasion de se familiariser avec des partenaires éventuels, puisque leurs employés auront acquis des connaissances approfondies à l'égard de ces partenaires. Par exemple, l'Autorité de régulation de Gibraltar et l'Institut fédéral de l'accès à l'information et de la protection des données du Mexique[9] ont effectué une visite de familiarisation d'une semaine durant laquelle les délégués ont pu assister à des séances pour en apprendre davantage sur les politiques et les procédures, et observer des activités d'application de la loi. En date de la publication, il convient également de noter que la Commission fédérale du commerce des États-Unis (**FTC**) a un programme international de stage (International Fellows Program) ouvert, qui permet aux autorités d'envoyer du personnel à la FTC pour une période de trois à six mois. Les représentants étrangers participent à des enquêtes, à des mesures d'application de la loi et à d'autres projets avec des avocats, des enquêteurs et des économistes de la FTC pour partager leurs connaissances et leur expérience avec leur autorité d'origine;

- Les autorités peuvent également envisager la création de groupes collaboratifs à l'échelle nationale. Au Royaume-Uni, le Digital Regulation Cooperation Forum (**DRCF**, forum de coopération sur la réglementation des technologies numériques) est un groupe composé de divers organismes

[9] Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México

nationaux de réglementation[10], dont le Commissariat à l'information du Royaume-Uni, et d'autorités de la concurrence, de protection des consommateurs, des télécommunications et des finances, qui cherchent à coopérer et à coordonner leurs activités liées à l'économie numérique.

Ententes d'échange de renseignements

L'échange de renseignements confidentiels ou de données personnelles est souvent crucial pour la coopération dans l'application des lois (même s'il s'agit uniquement de permettre aux autorités de faire savoir à leurs homologues qu'elles enquêtent sur un dossier ou qu'elles envisagent de le faire). Dans de nombreux cas, les parties seront en mesure d'échanger cette information, dans le respect des limites de leur législation, en vertu d'un protocole d'entente ou d'une entente n'ayant pas force exécutoire. Ce type de document énonce les attentes de chaque partie concernant les circonstances permettant le partage d'information. Mentionnons toutefois que pour des raisons pratiques ou légales, certaines autorités ne seront pas en mesure d'échanger des renseignements en vertu d'ententes non exécutoires, tandis que d'autres ne seront peut-être pas en situation de ratifier des ententes exécutoires.

Comme de nombreuses ententes seront dictées par des enjeux ou des besoins, une entente conclue au préalable pourra aider à gagner du temps lorsque la possibilité de coopération se présentera. En outre, elle permettra d'avoir régulièrement des discussions, ce qui aidera par le fait même à détecter les possibilités de coopération.

Les autorités peuvent également opter pour l'échange de renseignements en vertu d'ententes bilatérales entre des partenaires établis. Toutefois, les ententes de portée générale, comme l'entente de l'AMVP ou l'Accord de coopération sur la protection transfrontière des données de la Coopération économique Asie-Pacifique (APEC, site en anglais), offrent une marge de manœuvre pour le partage multilatéral. Des ententes de portée générale peuvent se révéler particulièrement utiles pour atténuer les risques touchant de nombreuses administrations, comme des atteintes à la protection des données à l'échelle mondiale, tout en permettant à toute autorité participante de refuser de collaborer et de choisir les partenaires avec lesquels elle partagera les informations.

Parfois, des ententes bilatérales continues ou générales ne sont pas disponibles en raison de contraintes législatives ou stratégiques. Dans de tels cas, les autorités devraient envisager d'avoir recours à des protocoles d'entente ou à des accords limités pour ces cas particuliers. Ces types d'ententes peuvent se révéler particulièrement utiles dans le cadre d'une première collaboration ou d'exercices de validation de principe, et ouvrir la voie à des ententes plus vastes – un tel arrangement pourrait servir, par exemple, de point de départ pour une collaboration interréglementaire où une autorité appuierait l'enquête d'une autre.

[10] Composé d'organismes du Royaume-Uni : la Competition and Markets Authority (CMA, Autorité de la concurrence et des marchés), l'Information Commissioner's Office (ICO, Commissariat à l'information du Royaume-Uni), l'Office of Communications (Ofcom, Bureau des communications) et la Financial Conduct Authority (FCA, Autorité britannique de surveillance des pratiques financières).

Les autorités peuvent être assujetties à des lois exigeant un traitement spécial des données personnelles, y compris en ce qui concerne les transferts internationaux de données personnelles. Si une ou plusieurs autorités sont soumises à de telles exigences, elles pourraient souhaiter envisager l'une des deux options suivantes :

- convenir qu'aucune donnée personnelle ne sera échangée (en reconnaissant qu'il est rarement nécessaire de communiquer des données personnelles aux fins de coopération dans l'application des lois);

- prévoir dans l'entente, ou en plus de celle-ci, des dispositions qui énoncent de façon claire et détaillée les exigences des parties ou les limites qu'elles doivent respecter en matière d'échange de renseignements.

(Remarque : Pour un exemple de telles dispositions dans une convention générale, voir l'article 7 et l'annexe 1 de l'entente de l'AMVP. Pour un exemple tiré d'un protocole d'entente bilatéral entre les autorités de protection des données qui traite de la question des données personnelles, voir l'article IV de protocole d'entente entre la commissaire à la protection de la vie privée du canada et l'information commissoner du Royaume-Uni)

Certaines autorités peuvent exiger le consentement de l'individu concerné avant de transmettre ses données personnelles à un tiers. Lorsqu'il est impossible d'obtenir son consentement, une autorité peut décider d'aller de l'avant en retenant l'option i) ci-dessus.La coopération reposera en grande partie sur la confiance entre les parties qui échangent des renseignements. À cette fin :

i. la partie qui communique les renseignements devrait énoncer expressément le détail[11] de ses exigences concernant le traitement[12] de l'information partagée;

ii. lorsque la loi le permet, la partie qui reçoit les renseignements devrait les traiter comme de l'information confidentielle[13] à moins que l'autorité qui les a fournis ait expressément consenti à ce que ce ne soit pas le cas.

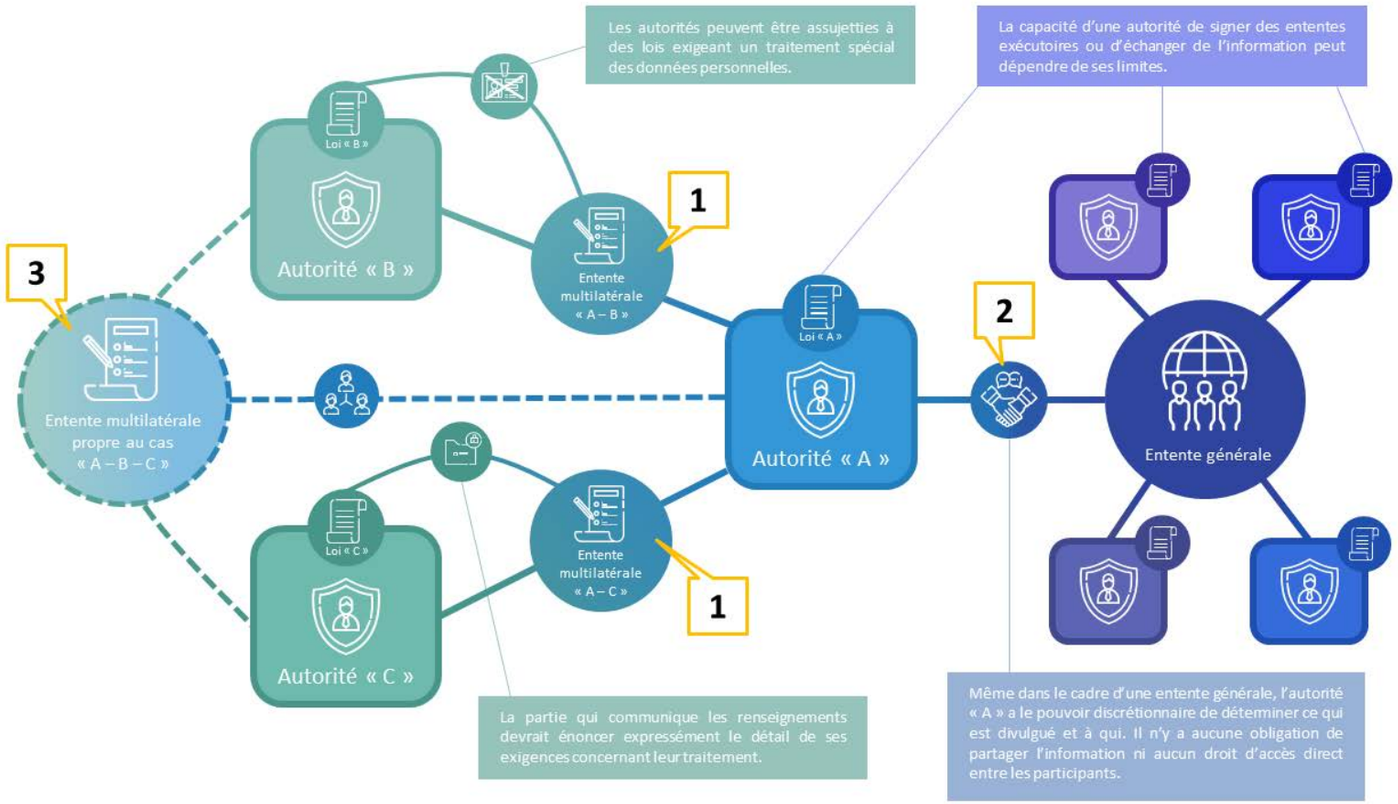
(Remarque : Pour obtenir un exemple de processus documenté de réponse à des demandes de communication de renseignements confidentiels, veuillez consulter l'alinéa 6.1iv) de l'entente de l'AMVP

[11] Pour voir un exemple, veuillez consulter l'article 6 de l'entente de l'AMVP, à l'annexe A.

[12] Pour voir un exemple, veuillez consulter l'article V du protocole d'entente entre la Commission fédérale du commerce des États-Unis et l'Autorité de protection des données des Pays-Bas, à l'annexe B.

[13] Pour voir un exemple, veuillez consulter l'article V du protocole d'entente entre le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information du Royaume-Uni, à l'annexe B.

Figure 1 : Les organisations peuvent utiliser divers mécanismes de partage de l'information en fonction des exigences législatives et des besoins opérationnels



Dans cette illustration, l'autorité « A » a ouvert une enquête sur une multinationale et souhaite partager l'information avec les autorités partenaires en vue de soutenir sa propre enquête et d'envisager une éventuelle application coordonnée. Elle le fait de trois façons :
(1) L'autorité « A » communique avec les autorités « B » et « C » (des partenaires proches) dans le cadre d'ententes bilatérales préexistantes, en évaluant soigneusement l'échange de renseignements personnels et en établissant les exigences relatives à l'utilisation de renseignements partagés. L'autorité détermine en fin de compte que l'échange de renseignements personnels n'est pas nécessaire puisque les autorités souhaitent davantage évaluer la technologie et les pratiques connexes de l'organisation.
(2) L'autorité « A » communique, au moyen de l'entente de l'AMVP, avec deux de ses homologues participants dans le secteur de compétence où l'organisation visée par l'enquête exerce ses activités, afin d'obtenir des renseignements qui pourraient avoir un rapport direct avec son enquête.
(3) L'autorité « A » constate que les autorités « B » et « C » disposent toutes les deux de renseignements importants et sont touchées par ce cas, mais qu'il n'existe actuellement aucun moyen d'échanger des renseignements. Après discussion avec les deux autorités, l'autorité « A » participe à l'élaboration d'une entente multilatérale propre pour ce cas pour permettre aux trois autorités de travailler ensemble. Les autorités « B » et « C » peuvent donc utiliser cet arrangement pour jeter les bases d'une coopération future

Figure 2 : Légende des symboles

Icône	Concept Représenté
	Autorité de protection des données.
	Loi constitutive de l'autorité de protection des données.
	Entente entre les autorités de protection des données.
	Réseau de coopération internationale entre autorités.
	La pouvoir discrétionnaire d'une autorité sur ce qui est partagé au sein d'un réseau de coopération.
	Restrictions sur la façon dont les informations personnelles sont partagées entre les autorités.
	Informations partagées entre les autorités.
	Participation à la rédaction d'une entente entre autorités.
	Organisation externe (c-à-d. pas une autorité de protection des données).
	Notification à une organisation externe que les informations fournies sont partagées.
	Enquête menée par une autorité de protection des données.
	Informations pertinentes pour une enquête.
	Partenariat établi entre les autorités.
	Pouvoirs d'application de la loi d'une autorité à l'encontre des organisations relevant de sa juridiction.
	Coordonner des enquêtes distinctes.
	Assister à l'enquête d'une autre autorité.
	Les communications publiques d'une autorité (ex. communiqué de presse, lettre ouverte, déclaration publique).

Remarque : Avant de communiquer des renseignements confidentiels obtenus auprès d'une organisation dans le cadre d'une enquête, l'autorité devrait déterminer s'il est approprié d'informer l'organisation en question que ces renseignements ont été ou pourraient être communiqués. Il est possible qu'il n'existe aucune exigence législative l'obligeant à le faire. Toutefois, le fait de ne pas en informer l'organisation pourrait avoir des conséquences pour les secrets commerciaux (ou les renseignements commerciaux confidentiels) ou nuire aux futures relations avec celle-ci, ou avec d'autres organisations, si le dossier attire l'attention.

> Avant de communiquer des renseignements confidentiels, l'autorité devrait effectuer une analyse approfondie des exigences législatives auxquelles elle doit se conformer (p. ex., la législation ou les conventions habilitantes) pour s'assurer qu'elle comprend bien les situations et les limites en vertu desquelles elle peut partager des renseignements confidentiels et des données personnelles.

À titre de référence, des exemples de protocole d'entente se trouvent à l'**annexe B** et dans le répertoire de coopération en matière d'application de la loi. Comme l'objectif du répertoire est d'être une ressource vivante, **nous encourageons fortement les autorités à envisager d'ajouter de nouveaux documents au répertoire dans la mesure du possible afin de faciliter une coopération accrue en matière d'application de la loi**.

Protocoles et formation sur la coopération dans l'application des lois

Il pourrait être pertinent pour les autorités d'élaborer un protocole interne de coopération dans l'application des lois et de donner une formation aux employés chargés de l'application des lois pour qu'ils aient une bonne connaissance des avantages et des options à leur disposition en matière de coopération dans l'application des lois ainsi que de leurs cadres législatifs et réglementaires respectifs. Idéalement, il s'agit de créer un climat où cette coopération leur viendra « naturellement » dans le cadre de leurs activités courantes et de les doter d'un outil de plus en matière de conformité – un climat où l'autorité sera en mesure de réagir rapidement aux possibilités de coopération lorsqu'elles se présentent. De même, des séances de formation sur d'autres sphères réglementaires pertinentes pourraient aider à combler le manque d'information et à jeter les bases d'une future coopération transréglementaire.

Les questions relatives à la vie privée évoluent souvent rapidement et nécessitent une réponse rapide. Les autorités sont exhortées à répondre aux demandes de coopération en temps opportun et de manière efficace. Il est possible d'atteindre cet objectif en offrant de la formation et du perfectionnement au personnel à l'interne dans le cadre d'un protocole de coopération en matière d'application des lois pour faciliter une réaction rapide aux possibilités de coopération lorsqu'elles se présentent.

Détection et évaluation des possibilités de coopération

Les autorités détermineront les possibilités de coopération par divers moyens : reportages dans les médias, plaintes du public, recherche interne, groupes de travail et réseaux d'application de la loi (y compris ceux d'autres sphères réglementaires, dans la mesure du possible), etc. Au moment de déterminer si un enjeu peut donner lieu à un type de coopération quelconque dans l'application des lois, les autorités peuvent se demander s'il présente :

- un risque pour plusieurs pays ou régimes réglementaires;
- un risque de préjudice appréciable ou d'incidence de grande portée;
- une question nouvelle ou stratégique en matière de protection de la vie privée.

Les autorités devront développer un processus décisionnel interne afin de s'assurer qu'elles ont réfléchi comme il se doit aux possibilités de coopérer avec une autre autorité et qu'elles ont une bonne idée des lois applicables (de façon générale en vertu d'une entente avec leurs services juridiques respectifs). L'absence de compétence géographique ou réglementaire n'empêche pas nécessairement la coopération, selon le cadre juridique applicable et les faits inhérents à l'enjeu en question, mais elle devrait être prise en compte. Les autorités devraient envisager de ratisser large lorsqu'elles demandent de l'information, car l'expertise et les renseignements clés peuvent être largement répartis entre les homologues nationaux, internationaux et transréglementaires.

L'outil d'alerte du GPEN offre aux participants une plateforme pour échanger des renseignements se rapportant à des enquêtes en cours ou éventuelles, ce qui aidera à détecter les possibilités de coopération.

Contact avec des partenaires potentiels

Il pourrait être plus facile de coopérer dans un premier temps avec des partenaires établis avec lesquels l'autorité a déjà conclu une entente d'échange de renseignements ou lorsqu'il existe un cadre juridique commun. Une fois qu'elle sera à l'aise de coopérer dans l'application des lois, l'autorité pourra juger utile d'accroître ses partenariats stratégiques.

Le ou les partenaires appropriés dans chaque cas particulier varieront en fonction des faits, mais la meilleure façon de les choisir consiste à prendre en compte les synergies pouvant découler éventuellement de la coordination – p. ex., les cas où le partenaire potentiel peut, entre autres :

- avoir lui aussi un intérêt dans l'enjeu;
- avoir accès à des éléments de preuve pertinents, par exemple des plaintes de consommateurs, ou avoir la capacité d'obtenir et de partager des documents et des dossiers pertinents;
- avoir une compétence incontestable dans le domaine (dans des cas où la compétence d'autres partenaires éventuels pourrait être mise en doute);
- être établi à proximité de la région ou du fuseau horaire où l'organisation exerce ses activités (pour faciliter la tenue de téléconférences ou la communication en personne — p. ex. une visite sur place);
- être en mesure de traiter avec l'organisation dans sa langue première;
- avoir la capacité de communiquer avec les autres partenaires dans une langue commune;
- avoir déjà établi une relation avec l'organisation;
- avoir une expertise technique ou stratégique pertinente, particulièrement lorsque la conduite en cause peut ou doit être abordée par les autorités dans différentes sphères réglementaires;
- détenir des pouvoirs d'application de la loi qui peuvent aider à obtenir réparation, notamment pour des individus touchés par une contravention alléguée;
- disposer de ressources pour partager la charge de travail associée à une enquête complexe.

Une autorité peut communiquer avec une autre autorité par divers moyens, notamment :

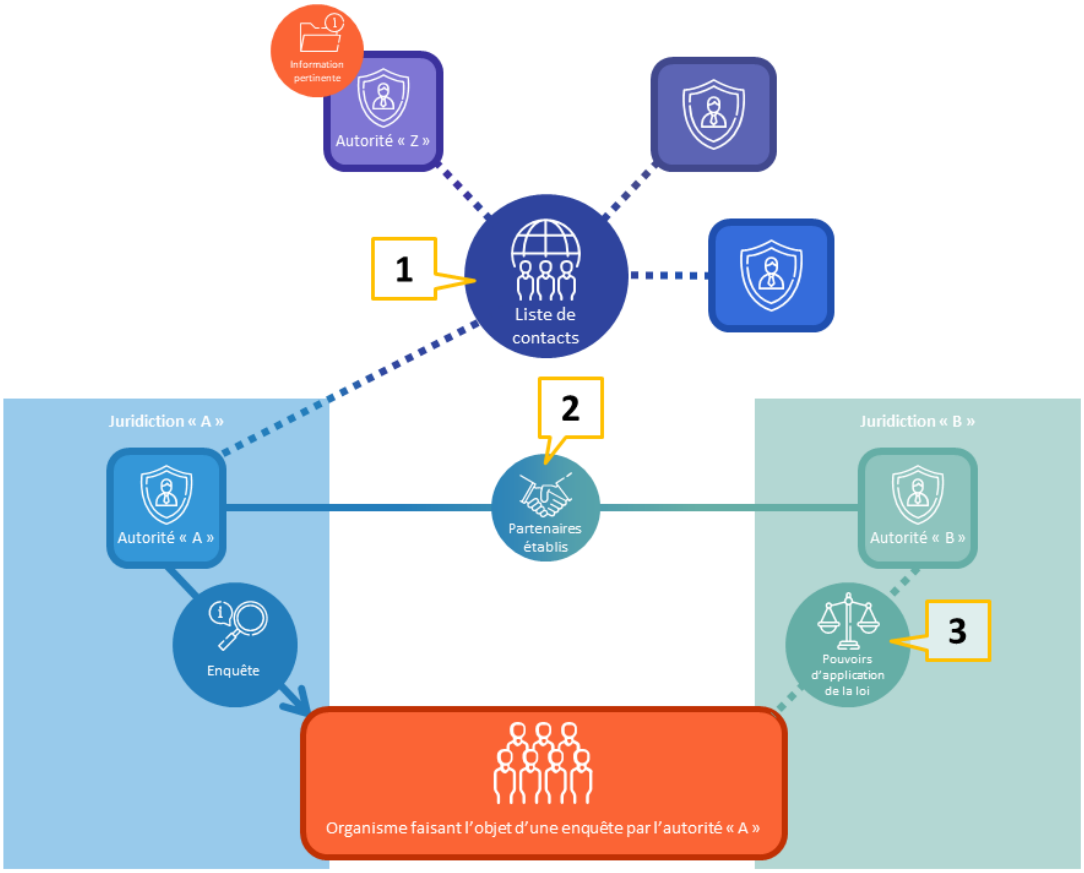
i. la liste des contacts existants de l'organisation pour les partenaires établis;

ii. des listes de contacts à sa disposition, par exemple,
    - l'entente de l'AMVP;
    - le GPEN : la liste des personnes-ressources de l'application de la loi ou du mécanisme de contact Outil d'alerte;
    - d'autres réseaux mondiaux, régionaux ou linguistiques tels que :
        - le Réseau d'application des communications non sollicitées (UCENet);
        - le Réseau ibéroaméricain de protection de données (RIPD);
        - le Comité européen de la protection des données (EDPB);
        - l'Association francophone des autorités de protection des données personnelles (AFAPDP).

Un organisme non autorisé en vertu de la loi à communiquer des données personnelles peut commencer par communiquer des détails généraux sur l'enjeu en question. Si les deux autorités ont mutuellement intérêt à approfondir la question, elles pourront alors prendre les mesures voulues pour échanger davantage de renseignements – p. ex., conclure une entente officielle.

Dans la mesure du possible, pour éviter les délais associés à la traduction, les autorités devraient s'efforcer de communiquer avec des partenaires éventuels dans une langue comprise mutuellement.

Figure 2 : Distribution de l'information et des capacités pertinentes entre les organisations



Dans ce cas, l'autorité « A » veut déterminer et évaluer l'aide que les autorités peuvent fournir dans le cadre de l'enquête. Elle le fait de trois façons :

(1) L'autorité « A » utilise l'outil d'alerte du GPEN pour informer les autorités participantes de son enquête et reçoit une réponse de l'autorité « Z » qui indique qu'elle a déjà examiné l'organisation. L'autorité « Z » lui communique de l'information qui l'aide à établir les motifs d'ouverture d'une enquête.

(2) L'autorité « A » communique ensuite avec l'autorité « B », un partenaire établi de coopération en matière d'application de la loi qui a également compétence sur l'organisation visée par l'enquête. Elles conviennent de coordonner les mesures d'exécution compte tenu des synergies possibles :

- L'autorité « A » peut tirer parti de sa proximité géographique avec l'administration centrale de l'organisation pour servir de principal point de contact pour la collecte d'éléments probants

(3) L'autorité « A » indique que l'autorité « B » serait en mesure de tirer parti des pouvoirs d'application de la loi qui ne lui sont pas conférés (pouvoir d'émettre des ordonnances et des sanctions pécuniaires) pour assurer le respect de ses conclusions définitives.

Modèle de coopération dans l'application des lois

La grille ci-après et le graphique de cheminement connexe serviront de base à notre analyse.

Figure 3 : Grille de coopération dans l'application des lois

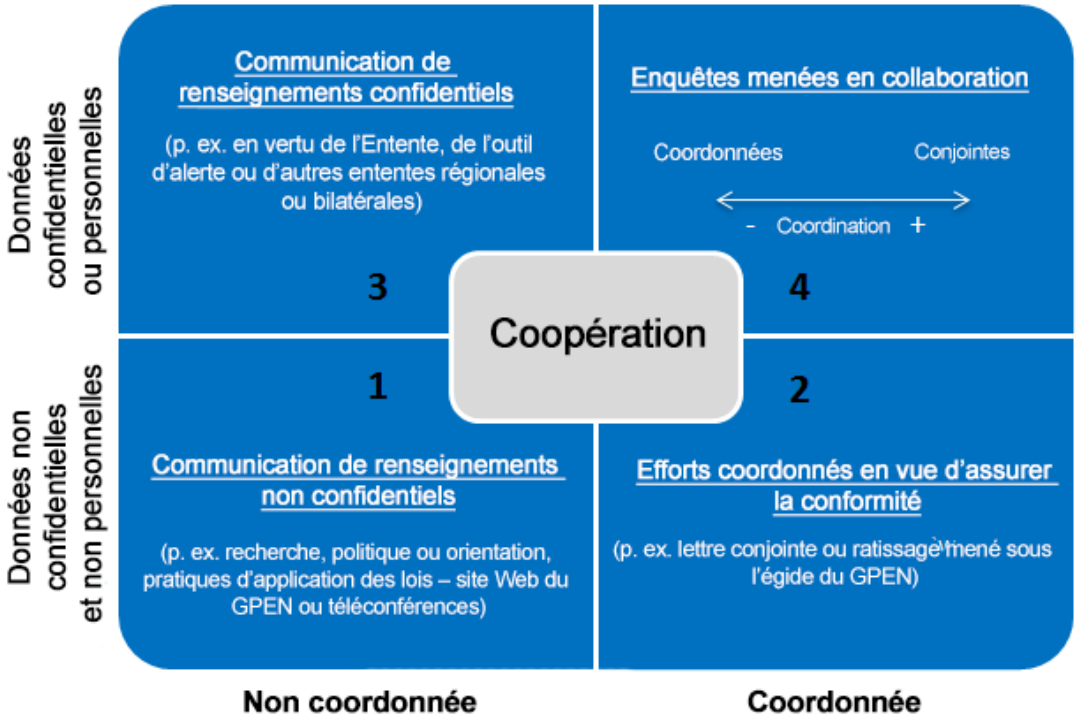
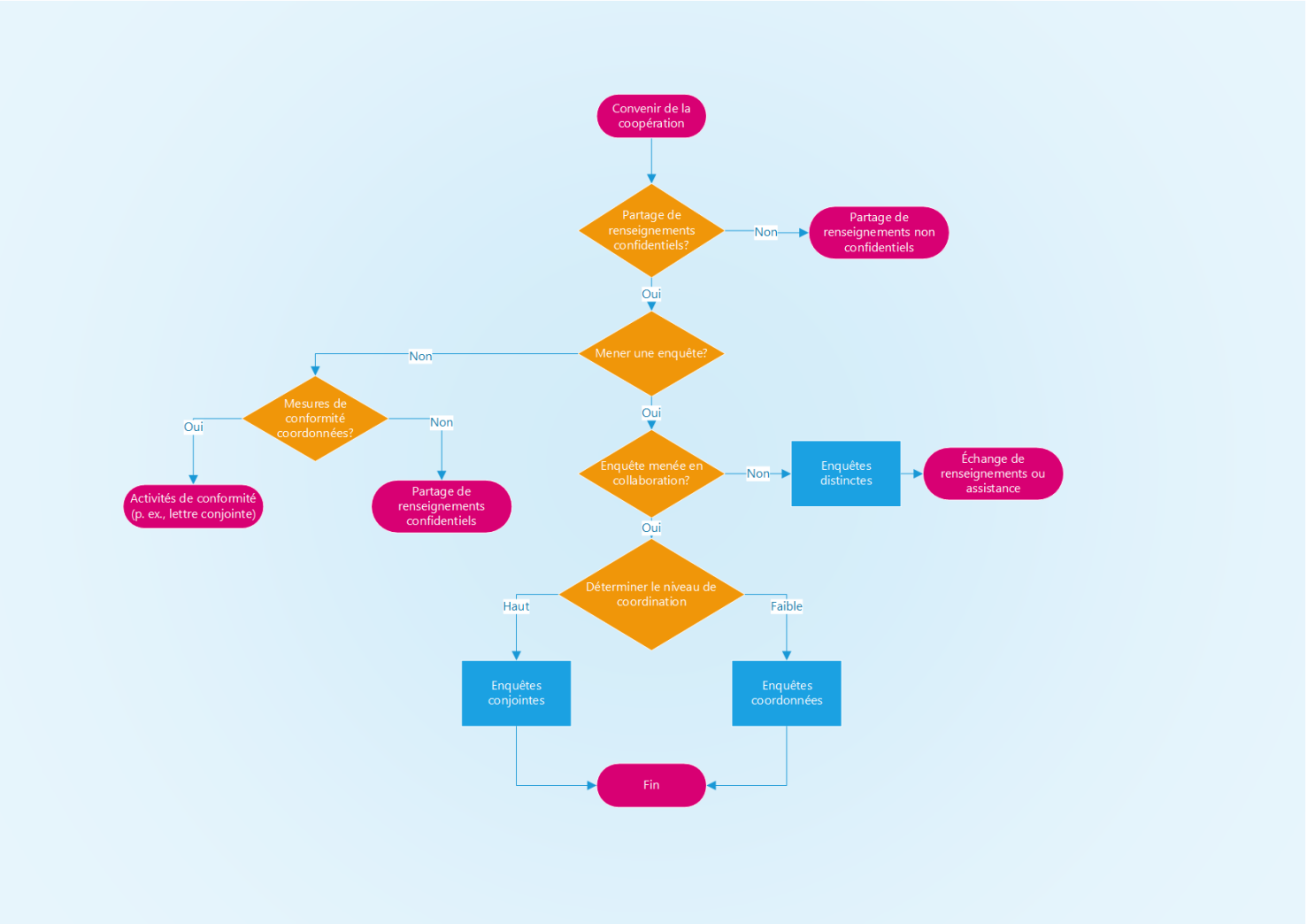


Figure 4 : Graphique de cheminement pour la coopération dans l'application des lois



Modèle de coopération dans l'application des lois

La coopération en matière d'application de la loi peut prendre plusieurs formes, que ce soit entre les APD ou entre les régimes réglementaires :

1. **Échange de renseignements non confidentiels et d'expérience** – par exemple, politique, recherche ou pratique générales sur des questions ayant trait à l'application des lois, par l'intermédiaire de divers réseaux ou au moyen de plateformes Web ou de réunions (en général, en dehors du cadre du présent guide).

2. **Mesure concertée en matière de conformité** – ne donnant généralement pas lieu à l'échange de renseignements confidentiels (p ex., initiatives thématiques comme les ratissages du GPEN ou la correspondance conjointe avec certaines organisations en dehors d'une enquête officielle).

3. **Partage de renseignements confidentiels ou de données personnelles, et assistance** – une ou plusieurs enquêtes distinctes et unilatérales non coordonnées, appuyées par le partage de renseignements ou une autre forme d'aide – par exemple, sur la base de protocoles d'entente comme l'entente de l'AMVP ou d'une autre entente multilatérale ou bilatérale.

   Remarque : Il peut s'agir d'aider une autorité d'un autre régime de réglementation[14] à mener son enquête – par exemple :
   - lorsqu'une autorité de protection des consommateurs ou de concurrence lance une enquête, mais qu'une autorité de protection de la vie privée n'a pas d'enquête comparable, il est possible que cette dernière, qui a l'avantage de connaître le fonctionnement de certaines fonctions de protection de la vie privée, aide son homologue interréglementaire à tenir compte de ces facteurs dans son analyse en partageant des renseignements propres au cas;
   - lorsque l'autorité A demande l'aide de l'autorité B pour recueillir des éléments de preuve auprès d'une tierce partie compétente relevant de sa compétence;

4. **Enquêtes menées en collaboration** (avec échange de renseignements confidentiels) pouvant comprendre divers niveaux de coordination le long d'un continuum allant de :

   - **Enquêtes distinctes, mais coordonnées** comportant une coordination de certains aspects de la procédure d'enquête (p. ex., collecte de renseignements ou communication publique); jusqu'aux :

   - **Enquêtes conjointes** comportant une coordination de la plupart ou de l'ensemble des aspects tout au long de la procédure d'enquête.

Dans le présent guide, nous mettons surtout l'accent sur les formes de coopération dans l'application des lois (voir ci-dessus) permettant de nous pencher sur des enjeux associés à des organisations particulières, comme ceux qui pourraient donner lieu : 2) à des activités conjointes de conformité; 3) au partage de renseignements confidentiels; et 4) à des enquêtes menées en collaboration.

Encore une fois, ces modes de coopération ne sont ni incompatibles ni exhaustifs. Par exemple :

- Des autorités pourraient dans un premier temps se contenter d'échanger des renseignements confidentiels ou d'envoyer une lettre conjointe visant à assurer la conformité, mais de décider par la suite d'amorcer une enquête qui sera menée en collaboration.
- Deux autorités participant à une enquête conjointe pourraient échanger des renseignements confidentiels avec une autre autorité menant une enquête distincte sur le même enjeu.[15]

---

[14] Pour voir un exemple d'une telle aide, veuillez consulter l'étude de cas à la page 32.

[15] Pour un exemple d'une telle collaboration, veuillez consulter l'étude de cas d'Ashley Madison à partir de la page 37.

Choix de la forme de coopération appropriée dans l’application des lois

Échange de renseignements non confidentiels et d’expérience (point 1)

Bien que les ressources, les limites législatives ou les considérations stratégiques puissent créer des obstacles à la coopération dans certaines circonstances, il est important de reconnaître que la coopération dans l’application des lois peut être aussi simple et informelle que la mise en commun de pratiques exemplaires ou de stratégies d’application novatrices ou l’échange d’autres renseignements non confidentiels.

Dans cette optique, les autorités sont encouragées à être aussi réciproques que possible dans leurs partenariats de coopération, ce qui renforcera la confiance entre les partenaires et favorisera une coopération accrue. À cette fin, les autorités peuvent commencer modestement en choisissant de partager des renseignements non confidentiels ou d’échanger sur leur expérience en vue de s’appuyer mutuellement, alors qu’elles s’efforcent d’obtenir de meilleurs résultats pour les personnes de leur compétence respective et de développer des partenariats solides à l’avenir.

Comme nous l’avons déjà souligné, les autorités peuvent également partager leur expérience au moyen de mécanismes comme des détachements et des échanges de personnel et des activités comme l’atelier des praticiens de l’application des lois du GPEN et l’atelier virtuel conjoint de février 2021 organisé par le RICPC et le GPEN pour examiner, de manière concrète, les recoupements entre la protection des consommateurs et la protection de la vie privée et la coopération en matière d’application de la réglementation.

Mesure concertée visant à assurer la conformité (point 2)

Outre la coordination et la collaboration dans le cadre des enquêtes, les autorités peuvent également envisager des mesures plus informelles visant à assurer la conformité. Ces mesures concertées peuvent permettre de recueillir des renseignements précieux et offrent souvent davantage de souplesse que les enquêtes officielles. Dans de nombreux cas, ces formes de collaboration se sont révélées très efficaces pour promouvoir le respect des lois relatives à la protection des renseignements personnels.

Ratissages

Les autorités peuvent envisager de participer à des ratissages pour la protection de la vie privée avec des partenaires d'application de la loi. Chaque année, les autorités membres du GPEN effectuent un ratissage sur une question ou un domaine d'intérêt différent[16]. Pendant ces ratissages, des autorités du monde entier évaluent généralement les pratiques de centaines d'organisations dans divers pays. Ces ratissages sont de nature informelle et mettent l'accent sur la collecte de renseignements dans le but de cerner les tendances et les préoccupations relatives à divers sujets liés à la protection de la vie privée et d'encourager les organisations « ratissées »[17] à respecter les mesures de conformité connexes.

Lettres conjointes

Au lieu d'amorcer une enquête officielle, les autorités peuvent choisir d'envoyer une lettre conjointe à une ou plusieurs organisations. De façon générale, l'envoi d'une lettre de cette nature ne nécessite pas l'échange de renseignements confidentiels ou de données personnelles.

Cette pratique peut s'avérer particulièrement appropriée lorsque le temps presse et/ou que les autorités estiment pouvoir obtenir des résultats en temps opportun sans avoir à y consacrer les ressources coûteuses qui sont nécessaires à la réalisation d'une enquête officielle.

En général, les autorités suivent certaines étapes dans l'élaboration et la publication d'une lettre conjointe.

Rédaction

Une ou deux autorités peuvent prendre l'initiative en proposant la lettre à un groupe d'autorités[18], en offrant de la rédiger et en faisant des suggestions, par exemple, sur :

- les enjeux à aborder dans la lettre et l'objectif visé de celle-ci;
- l'organisation ou les organisations auxquelles elle devrait être envoyée;
- l'intention de rendre la lettre publique ou non.

Dans la lettre, les signataires peuvent mentionner une infraction à des dispositions législatives précises, mais ils peuvent aussi choisir de ne pas le faire car celles-ci peuvent varier d'un pays à l'autre. Ils pourraient aussi y faire état de préoccupations concernant les grands principes de protection de la vie privée (p. ex., les Lignes directrices de l'OCDE sur la protection de la vie privée) ou poser des questions factuelles pour aider les signataires à mieux comprendre la pratique ou la technologie nouvelle. En outre, les signataires devraient s'entendre sur s'ils attendent ou non une réponse de l'organisation, afin que la lettre puisse être rédigée en conséquence. Il est souvent avantageux de

---

[16] Les sujets précédents comprennent : Responsabilité en matière de protection de la vie privée (2018), L'Internet des objets (2016) et Applications mobiles (2014).

[17] Les autorités concernées par les ratissages peuvent choisir (et ont choisi) de réaliser un suivi auprès des organisations ratissées de leur territoire en envoyant des lettres de conformité faisant état des préoccupations observées et en encourageant les améliorations à apporter pour se conformer aux lois applicables.

[18] P. ex., par l'entremise des « séances d'application de la loi fermées » du GTIE, de l'outil d'alerte GPEN ou des relations directes multilatérales.

collaborer activement avec l'organisation et d'établir des échéanciers. Ces efforts peuvent permettre d'apporter des améliorations positives à la protection de la vie privée, et ce, de manière efficiente, comme l'indique l'étude de cas à la page 29.

La rédaction de la lettre peut prendre de quelques jours à quelques mois selon le nombre de signataires et la contribution de chaque autorité. Si les autorités peuvent faire preuve de souplesse en ce qui a trait à la formulation, cela aide généralement les rédacteurs à finaliser la lettre rapidement en ralliant autant de signataires que possible pour avoir le maximum d'impact.

Remarque : Pour des raisons pratiques, lorsqu'ils doivent obtenir plusieurs signatures, ce qui requiert un important travail de coordination, les rédacteurs peuvent demander une version PDF du logo ou de la signature de chaque autorité pour l'intégrer avant d'envoyer la lettre conjointe au nom de tous les signataires.

Suivi

Avant de rédiger et d'envoyer la lettre, les signataires peuvent discuter des stratégies de suivi potentielles, par exemple :

i. Si la lettre vise simplement à sensibiliser l'entreprise ou le public à la protection de la vie privée, les signataires peuvent fort bien ne prendre aucune mesure de suivi ou, sous réserve des limites prévues par la loi, se contenter de rendre publique la réponse de l'organisation.

ii. Si la lettre se rapporte à un grave problème de protection de la vie privée qu'elle n'a pas réussi à résoudre, une ou plusieurs autorités peuvent choisir de faire enquête sur la question (éventuellement en collaboration).

En définitive, il revient à chaque autorité de déterminer les mesures qu'elle prendra en plus de l'envoi de la lettre conjointe. Les signataires devraient toutefois s'informer mutuellement des mesures de suivi qu'ils ont l'intention de prendre.

Exemples

Voici deux exemples généraux qui illustrent les situations dans lesquelles une lettre conjointe peut être appropriée, mais d'autres situations pertinentes peuvent survenir :

- Lorsqu'il y a des enjeux ou des risques qui pourraient être importants et qui touchent diverses administrations, il pourrait être possible d'assurer la conformité en envoyant à l'organisation ou aux organisations en cause une lettre qui les incite à respecter les attentes des signataires.
- Cette mesure, que l'on peut mettre en œuvre très rapidement en utilisant des ressources très limitées, pourrait s'avérer efficace, même dans les situations où la compétence n'a pas été clairement établie.
- Au moment de la publication du présent guide, l'exemple le plus récent est la lettre ouverte aux entreprises de vidéoconférence publiée conjointement par six autorités.

- Cette lettre expose les préoccupations et les pratiques exemplaires en matière de protection de la vie privée des EV dans le contexte de la COVID-19 (dont il est question plus en détail dans une étude de cas ci-dessous). Un autre exemple, présenté à l'**annexe C,** est une lettre conjointe de conformité envoyée par sept autorités à Insecam, un site Web de diffusion en continu.

- Lorsqu'une organisation se prépare à lancer, ou a lancé récemment, une nouvelle pratique ou technologie de protection de la vie privée qui soulève des préoccupations importantes à cet égard, les autorités peuvent envoyer une lettre conjointe pour :
    - donner à l'organisation la possibilité d'expliquer comment elle se conforme aux lois relatives à la protection de la vie privée ou lui demander de modifier ses pratiques en matière de protection de la vie privée dans le but d'éviter d'y contrevenir
    - si la lettre est publiée, sensibiliser le public à d'éventuels enjeux relatifs à la vie privée et montrer la solidarité qui existe entre les autorités concernant cet enjeu.
- Au moment de la publication du présent guide, un exemple récent est la lettre ouverte conjointe sur les attentes mondiales en matière de protection des renseignements personnels du réseau Libra, signée par sept autorités à l'échelle mondiale.
    - Cette lettre expose les préoccupations et les questions en matière de protection de la vie privée à l'intention des membres de l'association Libra[19] en ce qui a trait à leurs pratiques de traitement de l'information prévues. Un autre exemple, présenté à l'**annexe C,** est une lettre conjointe envoyée à Google au nom de 38 autorités en vue d'obtenir de plus amples renseignements sur le produit Google Glass.

[19] L'association Libra, maintenant connue sous le nom d'association Diem, est un groupe d'entités du secteur privé, dirigé par Facebook, qui est en train de créer un nouveau réseau de cryptomonnaie et de paiement numérique soutenu par le secteur privé. À la date de publication du présent guide, le réseau demeure à l'étape de la planification et de l'approbation réglementaire.

Étude de cas – Lettre ouverte aux entreprises de vidéoconférence : Au début de 2020, le Groupe de travail sur la coopération internationale en matière d'application de la loi de l'AMVP a tenu une série de discussions sur divers risques relatifs à la protection des renseignements personnels en raison de la pandémie de COVID-19. L'une de ces discussions portait sur les préoccupations et les risques en matière de la protection des renseignements personnels associés à une forte augmentation mondiale de l'utilisation des produits de vidéoconférence en raison de la pandémie. Au cours de cette séance, six APD participantes ont convenu de prendre des mesures coordonnées.

Le 21 juillet 2020, les six APD ont publié conjointement une lettre ouverte aux entreprises de vidéoconférence en réponse aux risques nouveaux et élargis pour la protection des renseignements personnels liés à la technologie et à sa mise en œuvre. Dans la lettre, elles énonçaient leurs préoccupations et des pratiqes exemplaires concernant : i) la sécurité; ii) la protection de la vie privée intégrée par défaut dès la conception; iii) l'importance pour les plateformes de vidéoconférence de connaître leur auditoire; iv) la transparence et l'équité; et v) le contrôle des utilisateurs finaux. Bien que la lettre ouverte était destinée à toutes les entreprises de vidéoconférence, elle a été envoyée directement à Microsoft, à Cisco, à Zoom, à Google et à Houseparty. Au moment de la publication du présent guide, tous les destinataires, à l'exception de Houseparty, ont répondu à la lettre et expliqué les mesures qu'ils avaient prises pour se conformer aux exigences en matière de données et de protection de celles-ci, y compris leurs politiques, outils, pratiques et mesures de sécurité. Les signataires conjoints ont également communiqué avec chacune de ces entreprises dans le cadre d'une série de réunions virtuelles sur diverses plateformes de vidéoconférence, afin de clarifier certains sujets de préoccupation résiduelle et de mieux comprendre leurs plateformes et leurs pratiques en matière de protection des renseignements personnels.

Cet effort de collaboration a produit plusieurs avantages, tels que :

- cerner et aborder de façon holistique les préoccupations mondiales en matière de protection des renseignements personnels;
- prévenir le dédoublement des efforts et économiser des ressources grâce à une approche de conformité informelle convenue par toutes les autorités participantes;
- tirer parti de l'expertise de six autorités mondiales pour le processus de rédaction, de communication et de mobilisation;
- exécuter une mesure d'application évolutive permettant aux APD de diverses tailles de participer à des mesures coordonnées et d'en tirer profit;
- tirer parti des divers fuseaux horaires, ainsi que des forces et des relations professionnelles de chacun des signataires pour diviser le travail lié à la mobilisation des entreprises de vidéoconférence à différents endroits.

Cette initiative mondiale de conformité a sera bientôt finalisé avec la publication d'un énoncé final sur les conclusions, les leçons tirées et les attentes pour encourager la conformité et les pratiques exemplaires à grande échelle dans l'ensemble du secteur. En décembre 2020, les signataires ont invité Houseparty à travailler avec eux, y compris au moyen d'un communiqué. Jusqu'à présent, Houseparty n'a pas répondu au groupe de signataires, mais a communiqué directement avec le Commissariat à l'information du Royaume-Uni (ICO) dans le cadre d'enquêtes qui ne sont pas visées par la lettre conjointe. En septembre 2021, l'entreprise Houseparty a annoncé qu'elle cesserait d'offrir ses services de vidéoconférence.

Coordination générale

Les autorités ne se limitent pas aux lettres conjointes et aux ratissages. Elles peuvent participer à diverses formes d'activités de coordination et de coopération hors du cadre des enquêtes, y compris la coordination de l'acceptation et du traitement de plaintes ou des activités de renseignement. Cela peut être particulièrement utile lorsqu'une collaboration interréglementaire est envisagée, dans les cas où les options formelles de collaboration d'enquête ne sont pas encore entièrement élaborées.

Étude de cas – The Australian Consumer Data Right : The Australian Consumer Data Right - Le CDR (soit le droit des consommateurs en matière de données) est une initiative du gouvernement australien visant à donner aux consommateurs un plus grand contrôle sur leurs données. Cette initiative permet à un consommateur de demander à un détenteur de données de fournir ses données visées par le CDR à un destinataire de données accrédité, dans un format conforme au CDR. Bien que le Département du Trésor fédéral australien et le Data Standards Body participent au système de CDR, c'est le Commissariat à la protection de la vie privée de l'Australie (OAIC, Office of the Australian Information Commissioner) et la Commission australienne de la concurrence et de la consommation (ACCC, Australian Competition and Consumer Commission) qui l'appliquent.

À la lumière de leur mandat commun d'application du CDR, ils ont pris de nombreuses mesures de coopération de base décrites dans le présent guide (c.-à-d. conclure un protocole d'entente et élaborer de solides ententes d'échange de renseignements). La nature continue de leur responsabilité partagée en matière de réglementation leur a également permis d'élaborer et de publier publiquement une *politique de conformité et d'application de la loi* conjointe. Accessible en ligne et rédigée à l'intention des consommateurs et des participants à l'initiative CDR, la politique décrit l'approche que l'OAIC et l'ACCC adopteront pour encourager la conformité aux règles et aux lois sur le CDR et la façon dont ils réagiront en cas d'infraction au cadre réglementaire.

Compte tenu de la nature coréglementaire du régime de CDR et de l'intention de le déployer secteur par secteur à l'échelle de l'économie, un certain nombre d'organismes peuvent aider les consommateurs à traiter leurs demandes et leurs plaintes. Afin d'assurer la simplicité et la commodité pour les consommateurs et de s'assurer qu'ils ne sont pas transmis entre les organismes de réglementation ou d'autres organismes, une approche « sans fausse route » a été appliquée aux contacts et aux plaintes — les consommateurs sont dirigés vers un point de contact unique sur le site Web de l'initiative CDR, où l'OAIC et l'ACCC trient les demandes de renseignements, les rapports ou les plaintes pour s'assurer qu'ils sont transmis à l'organisme de réglementation ou à l'organisme visé.

Coordination en matière de politiques et de recherche

Bien que cela dépasse la portée du présent guide, il importe de mentionner la valeur de la collaboration en matière de politiques et de recherche entre les APD et d'autres organismes de réglementation à l'échelle mondiale. Grâce à des mécanismes, tels que les divers groupes de travail de l'AMVP, y compris le groupe de travail sur les politiques stratégiques[20], et d'autres initiatives et publications de recherche bilatérales et multilatérales, les autorités peuvent combiner leur expertise et acquérir des connaissances mondiales particulièrement utiles à l'ère où les pratiques de données novatrices sont en constante évolution.

En particulier, les autorités peuvent obtenir d'importants avantages en collaborant à la recherche des tendances techniques en matière de protection de la vie privée et d'économie numérique, en travaillant avec des autorités partenaires qui ont une plus grande capacité technique (p. ex., laboratoires techniques). Ces activités favorisent une approche globale et holistique en matière d'application des lois et de conformité générale. Elles revêtent une grande importance dans l'établissement et le développement de relations avec des autorités pouvant constituer des partenaires potentiels.

Partage de renseignements confidentiels ou de données personnelles, et assistance (point 3)

Dans certaines situations, une autorité peut choisir de communiquer des renseignements ou de prêter assistance (en vertu du pouvoir conféré par la loi ou une entente) à l'appui d'une enquête en cours ou future d'une autre autorité. Les paragraphes ci-après illustrent des situations où cette approche pourrait être appropriée.

i. Dans le cadre de son enquête, l'**autorité A** obtient, à travers ses propres preuves, des renseignements concernant les pratiques d'une organisation relevant de la compétence de l'**autorité B**. L'**autorité A** n'a pas compétence sur l'organisation en question ou croit que l'**autorité B** serait mieux placée pour enquêter en raison de son emplacement géographique, de sa langue, de ses pouvoirs législatifs ou de sa relation avec l'organisation. L'**autorité A** pourrait donc s'adresser à l'**autorité B** pour déterminer si elle aimerait recevoir les renseignements et si elle serait en mesure de faire enquête.

ii. L'**autorité A** et l'**autorité B** enquêtent chacune sur la même question ou des questions connexes, mais elles ne souhaitent pas coordonner leurs enquêtes (p. ex., en raison de différences législatives ou des calendriers de réalisation souhaités). Afin d'assurer l'uniformité,

[20] Les récents rapports du Groupe de travail sur les politiques stratégiques (PSWG) portent sur les sujets suivants : les cadres et normes mondiaux, l'économie numérique et la relation entre la protection de la vie privée/des données et d'autres droits et libertés.

ces autorités pourraient s'entendre pour échanger leurs éléments de preuve recueillis dans le cadre de leurs enquêtes respectives, leurs conclusions ou leurs suivis.

iii. **L'autorité A** mène une enquête et estime que l'**autorité B** pourrait détenir ou être en mesure d'obtenir des informations qui lui seraient utiles pour son enquête. L'**autorité A** pourrait donc approcher l'**autorité B** pour établir si elle est en mesure de fournir une telle aide[21].

Étude de cas – Enquête sur Facebook/WhatsApp de la Bundeskartellamt : En 2019, la Bundeskartellamt (BKartA), l'autorité de la concurrence allemande, a constaté que les conditions de service de Facebook/WhatsApp, ainsi que la manière et la mesure dans laquelle il recueille et utilise les données équivalent à un abus de domination et a interdit à Facebook/WhatsApp de combiner les données des utilisateurs provenant de différentes sources.* Comme la conduite en cause impliquait une infraction au Règlement général européen sur la protection des données (RGPD), la BKartA a demandé et obtenu l'aide des autorités de protection des données (APD) d'Allemagne, soit le commissaire à la protection des données de Hambourg (HDPC) et le commissaire fédéral à la protection des données et à l'accès à l'information de l'Allemagne (BfDI, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit). En décidant d'aider le BKartA, les APD ont reconnu le chevauchement des objectifs de protection des droits des consommateurs, y compris la protection des données personnelles des consommateurs. Les APD ont également adopté le point de vue selon lequel un échange d'opinions juridiques entre les autorités est toujours utile, car il permet d'assurer l'interprétation et la mise en œuvre uniformes du RGPD et que la protection des données et les lois sur la concurrence devraient aller « de pair ».

Pour tirer le meilleur parti de cette collaboration, les organismes en cause étaient conscients des avantages d'élaborer une stratégie de collaboration étroite fondée dans ce cas particulier et pour traiter d'autres enjeux pertinents. Entre autres, cela a donné lieu à un échange réussi de points de vue entre les autorités – ce qui a permis au BKartA d'obtenir une deuxième opinion et d'obtenir l'appui des APD à l'égard de sa décision. Parallèlement, les APD ont pu obtenir des renseignements sur l'enquête de BKartA et jeter les bases d'un partenariat continu avec BKartA à l'avenir.

*En septembre 2021, on était encore en attente d'une décision finale du tribunal compétent (Oberlandesgericht Düsseldorf). Le tribunal avait déposé des questions d'orientation à la Cour européenne de justice de l'Union européenne. Facebook/WhatsApp avait contesté en justice la décision de 2019 de la BKartA.

Dans tous les cas, chaque autorité doit s'assurer qu'elle est autorisée, en vertu de la législation qui la régit, à communiquer des renseignements à une autre autorité ou à lui venir en aide. Elle doit également préciser clairement par écrit les modalités en vertu desquelles elle communique des

[21] Soit en vertu d'une autorisation législative ou d'une entente comme celle de l'APEC ou celle de l'AMVP.

renseignements ou apporte son aide. Une autorité autorisée par la loi à communiquer des renseignements peut choisir de le faire même si l'autorité qui les reçoit ne peut lui rendre la pareille.

De plus, une autorité qui reçoit de l'information devrait s'assurer de bien comprendre les fins auxquelles les renseignements reçus peuvent être utilisés en fonction de l'entente d'échange de renseignements et des lois qui la régissent. À titre d'exemple, une autorité doit s'assurer de comprendre qu'elle pourrait i) faire référence à l'information dans des conclusions écrites, en respectant les modalités de l'entente d'échange de renseignements; ou ii) utiliser l'information reçue en preuve dans des procédures judiciaires nationales, compte tenu du type de procédure en question (p. ex., administrative, civile ou criminelle) et de toute exigence particulière en matière de preuve dans son propre cadre juridique (p. ex., équité procédurale).

Les partenaires devraient aussi établir une compréhension commune des exigences particulières en matière de protection des données qui seront échangées. Les mesures convenues devraient tenir compte de la nature des renseignements en question et du préjudice qui pourrait résulter de leur communication non autorisée, de leur perte accidentelle ou de leur destruction. Il peut s'agir, par exemple, i) de la transmission au moyen d'une plateforme existante (p. ex., outil d'alerte du GPEN) ou par courriel protégé par chiffrement ou par mot de passe; ii) de la limitation de l'accès du personnel en fonction des besoins; et iii) du stockage sous forme chiffrée ou dans un classeur sous clé.

> Une autorité qui a reçu des renseignements devrait les traiter comme de l'information confidentielle et, si la loi le permet, obtenir le consentement écrit de l'autorité qui les a fournis avant de les communiquer de quelque façon que ce soit.

Enquêtes menées en collaboration (point 4)

Une enquête menée en collaboration, qu'elle soit « conjointe » ou « distincte, mais coordonnée », peut offrir aux autorités participantes l'occasion d'éviter le dédoublement des efforts, de tirer parti des forces relatives de l'autre et d'obtenir une coopération accrue de la part du ou des sujets de l'enquête, en vue d'obtenir des résultats marqués de manière plus efficace et d'en amplifier l'impact en attirant une plus grande attention à l'échelle nationale et internationale ou en établissant une position interréglementaire combinée.

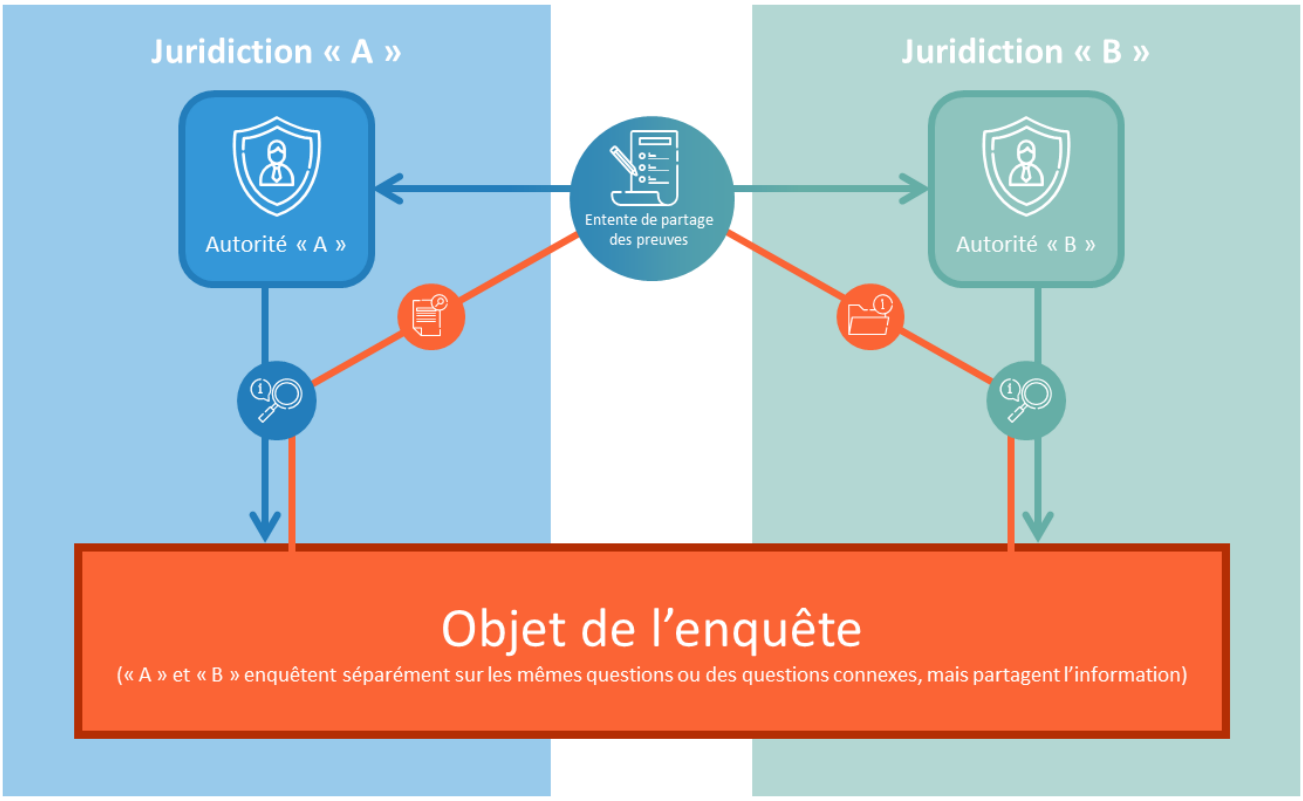
Formes d’enquêtes menées en collaboration

Les enquêtes menées en collaboration impliquent généralement l’échange de renseignements confidentiels, mais pas nécessairement de renseignements personnels. Ces enquêtes comprendront également la coordination de certaines activités liées à l’application de la loi. Cette collaboration proprement dite peut s’inscrire dans un continuum et faire appel à une combinaison d’approches présentées ci-après (en particulier lorsque plus de deux autorités sont impliquées).

i. **Enquêtes distinctes, mais coordonnées :** Dans d’autres situations, deux autorités ou plus peuvent déterminer qu’il serait plus efficace et efficient de mener des enquêtes distinctes, mais simultanées en coordonnant certains aspects limités de la procédure d’enquête (p. ex., une analyse technique ou la publication de conclusions complémentaires). Voici quelques exemples de ces situations :

    - La loi qui la régit empêche une autorité de mener des enquêtes conjointes (p. ex., elle l’oblige à envoyer des avis distincts, à présenter des demandes de renseignements distinctes ou à formuler des conclusions distinctes).
    - Les autorités en sont à des étapes différentes de la procédure d’enquête.
    - Les lois ou les politiques auxquelles sont assujetties les autorités peuvent comporter des différences importantes (de sorte qu’elles voudront faire enquête sur des enjeux très différents).

Figure 5 : **Enquêtes distinctes, mais coordonnées**



Dans cette situation, l'autorité « A » a ouvert une enquête sur l'organisation préoccupante environ trois mois après que l'autorité « B » a amorcé sa propre enquête. L'organisation est une multinationale qui exerce ses activités dans les deux pays. L'autorité « A » a noté un billet de l'autorité « B » dans le forum de discussion du GPEN demandant si d'autres autorités se penchaient sur la question et a communiqué avec celle-ci, compte tenu de l'Accord de coopération sur la protection transfrontière des données de l'APEC, pour en discuter davantage. À la lumière de cette discussion, les autorités ont déterminé qu'elles avaient des intérêts qui se chevauchaient à l'égard de l'organisation. L'autorité « B » avait choisi de concentrer son enquête sur les questions de consentement et de conservation, tandis que l'autorité « A » s'intéressait principalement aux questions relatives au consentement, à l'exactitude et à la nécessité/proportionnalité. Compte tenu des différentes étapes d'enquête et de l'orientation des autorités, il a été déterminé que la meilleure façon d'aller de l'avant consistait à coordonner leurs enquêtes distinctes au moyen de l'échange d'information.

ii. **Enquêtes conjointes** : Deux autorités ou plus peuvent s'entendre pour coordonner la plupart des aspects d'une enquête (y compris la collecte et l'analyse de renseignements, la rédaction de rapports et les communications) en ce qui a trait à une série d'enjeux convenue. L'organisation visée peut avoir l'impression qu'il s'agit d'une seule enquête. Une enquête conjointe pourrait être appropriée dans certaines situations, par exemple :

- la question présente un risque de préjudice élevé ou touche un grand nombre de personnes au sein du pays de deux autorités ou plus;

- la question constitue une infraction apparente à diverses compétences géographiques ou réglementaires;
- chaque autorité s’assure d’avoir compétence sur l’organisation et la question;
- on observe une certaine concordance entre les lois applicables et les positions stratégiques connexes concernant les enjeux en question;
- chaque autorité mènerait, autrement, une enquête indépendante.

-

Compte tenu de l’uniformité relative de la législation des différentes autorités en ce qui a trait aux mesures de sécurité, les atteintes d’envergure mondiale peuvent souvent représenter une excellente occasion pour toutes les formes de collaboration.

Étude de cas – Ashley Madison : En 2015, une fuite de données a eu lieu relativement à Ashley Madison, un site Web de rencontres alternatif pour adultes exploité par Avid Life Media Inc. (ALM), qui fait maintenant affaire sous le nom de Ruby Life inc. Le siège social de Ruby Life inc. est établi au Canada, mais ses sites Web ont une portée mondiale et comptent des utilisateurs dans plus de 50 pays, y compris en Australie et aux États-Unis.

À la lumière des discussions animées par le réseau d'application des lois du GPEN, il a été déterminé qu'il y avait un intérêt international à enquêter sur cette affaire.

Compte tenu de l'ampleur de l'atteinte à la sécurité des données (environ 36 millions de comptes d'utilisateurs d'Ashley Madison), de la nature délicate des renseignements en cause, de l'incidence sur les personnes touchées et de la nature internationale des activités, le Commissariat à la protection de la vie privée de l'Australie (OAIC) et le Commissariat à la protection de la vie privée du Canada (CPVP) ont mené conjointement une enquête sur les pratiques de protection de la vie privée d'ALM. De plus, les deux autorités ont collaboré et partagé de l'information avec la Commission fédérale du commerce des États-Unis (FTC), qui a mené une enquête parallèle. Nous discuterons de ce cas en détail au fur et à mesure que nous progresserons dans les étapes pertinentes de coopération, ci-après.

Étude de cas – Enquête conjointe sur Clearview AI : En janvier 2020, Clearview AI inc. (Clearview), une entreprise spécialisée dans la technologie de reconnaissance faciale, a attiré l'attention du public mondial. Clearview a obtenu de l'information pour sa base de données en recueillant des images accessibles au public à partir d'un certain nombre de sources sur Internet, y compris des profils dans les médias sociaux. Elle a ensuite offert un service permettant d'effectuer une recherche dans cette base de données à l'aide des données biométriques pour identifier des personnes.

Étant donné la collecte et l'utilisation apparemment aveugles des renseignements personnels des Canadiens, le Commissariat à la protection de la vie privée du Canada et ses homologues provinciaux (le Commissariat à la protection de la vie privée de l'Alberta, BPIC-AB; le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, BPIC-BC; et la Commission d'accès à l'information du Québec, CAI) ont discuté de la question lors d'une réunion spéciale des responsables des autorités.

Les autorités ont déterminé qu'une enquête conjointe serait la meilleure utilisation des ressources, étant donné que chaque autorité entendait mener une enquête indépendante. Ce cas fera également l'objet d'une discussion détaillée à mesure que nous progresserons dans les étapes pertinentes de la coopération.

Questions préliminaires

Avant d'amorcer une enquête menée en collaboration, il est généralement important que les autorités concernées se penchent sur certaines questions préliminaires[22].

Les autorités sont-elles parties à une entente d'échange de renseignements ou la loi leur permet-elle d'échanger des renseignements confidentiels ou des données personnelles? Dans la négative, elles peuvent choisir d'adhérer à une entente existante (comme l'entente de l'AMVP) ou conclure une nouvelle entente spéciale bilatérale ou multilatérale.

Remarque : Si plus de deux autorités coordonnent leurs activités, même si elles sont toutes signataires d'une entente d'échange de renseignements, les parties devraient s'entendre sur la mesure dans laquelle les autorités peuvent s'échanger les renseignements. (À titre d'exemple, les **autorités A et B** coordonnent leurs activités. « **A** » n'a qu'un mandat en matière de protection de la vie privée, tandis que « **B** » est responsable de la protection de la vie privée et des consommateurs et de la concurrence. Lorsque « **A** » partage des renseignements confidentiels avec « **B** », est-ce que « **B** » devrait divulguer ces renseignements à l'interne à ses unités de concurrence et de protection des consommateurs, qui ne seraient autrement pas impliquées?) Comme il a déjà été indiqué, si les renseignements communiqués renferment des données personnelles, les autorités peuvent s'entendre ou prendre des dispositions pour que ces données fassent l'objet de restrictions ou d'un traitement particuliers.

[22] Les **autorités** pourraient juger utile le modèle présenté à l'annexe E pour documenter ces questions.

Exemple d'Ashley Madison : Pour échanger de l'information et coopérer dans ce dossier, les autorités se sont fondées sur un certain nombre d'ententes et de textes législatifs existants. Pour favoriser la coopération au moyen d'une enquête conjointe, le CPVP et l'OAIC ont partagé de l'information en vertu de leurs lois applicables et de l'Accord de coopération sur la protection transfrontière des données (CPEA) de la Coopération économique Asie-Pacifique (APEC). Comme nous l'avons déjà mentionné dans le présent guide, l'APEC crée un cadre permettant à ses membres de collaborer à l'application des lois sur la protection de la vie privée. Pendant ce temps, pour appuyer la coopération avec le CPVP et l'OAIC, la FTC s'est appuyée sur des dispositions clés de la loi américaine SAFE WEB Act, qui lui a permis de partager de l'information avec ses homologues étrangers afin de lutter contre les pratiques trompeuses et injustes qui traversent les frontières nationales.

Exemple de Clearview AI : Les lois directrices des quatre autorités permettent des activités d'application concertées. Le CPVP, le BPIC-AB et le BPIC-BC ont un protocole d'entente collectif sur la collaboration fédérale-provinciale en matière d'application des lois sur la protection de la vie privée dans le secteur privé. Cet accord écrit énonce les modalités selon lesquelles les bureaux peuvent échanger efficacement de l'information et collaborer sur des questions d'intérêt commun. Après avoir confirmé un intérêt commun à enquêter sur Clearview, les autorités ont également signé un protocole d'entente spécifique avec la CAI pour échanger des renseignements et mener une enquête conjointe.

Approche stratégique et modalités de la collaboration

Les autorités peuvent aussi envisager de créer un document présentant une « approche stratégique »[23] globale pour énoncer clairement leur compréhension commune des questions importantes telles que les enjeux à examiner; le rôle et les responsabilités de chaque participant; le délai d'exécution et les jalons; ainsi que les points de contact. Compte tenu des nouveaux développements qui surviennent constamment dans les enquêtes (dont bon nombre peuvent être imprévus), on pourrait faire référence à ce document évolutif, et le mettre à jour au besoin, tout au long de l'enquête afin d'assurer une compréhension commune en tout temps.

[23] Pour voir un exemple d'outil qui pourrait être utile dans ce processus, veuillez consulter le modèle de plan d'enquête conjoint ou coordonné à l'annexe E. Ce modèle a été élaboré par le Commissariat à la protection de la vie privée du Canada, le Commissariat à l'information et à la protection de la vie privée de l'Alberta et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, sur la base du présent guide.

Établissement d’une compréhension commune

Les autorités devraient prendre le temps de discuter très attentivement de la possibilité de coordination pour parvenir à une compréhension commune des capacités (p. ex., savoir-faire, pouvoirs d’application de la loi ou sanctions en cas de non-conformité) et les attentes de chacune. En établissant une compréhension commune avant d’amorcer une enquête conjointe ou coordonnée, les autorités pourront i) s’assurer qu’une enquête menée en collaboration constitue en fait la stratégie optimale; et ii) s’entendre sur une stratégie de collaboration qui donnera le résultat le plus efficient et efficace. Dans le cadre d’une initiative menée en collaboration, établir des objectifs simples donne souvent plus de flexibilité pour tracer la voie en vue de les atteindre.

En particulier, les autorités qui envisagent de collaborer sur une enquête devraient s’assurer qu’elles comprennent bien les similitudes et les différences importantes entre leurs lois respectives. Cela devient encore plus important lorsqu’on collabore avec des autorités de différents régimes de réglementation. Par exemple, les autorités devront probablement s’assurer qu’elles « parlent la même langue », étant donné la possibilité que des termes communs aient des significations différentes d’un régime à l’autre. Les différences n’empêchent pas nécessairement une collaboration, mais l’identification de ces différences aidera à régler de nombreuses questions mentionnées ci-après. Une autorité peut notamment juger utile d’examiner si les éléments de preuve recueillis et communiqués avec elle par une autre autorité, possiblement pour les besoins d’une forme d’enquête différente (p. ex., enquête administrative ou civile plutôt que criminelle), seraient admissibles à ses propres fins.

Détermination de la portée d’une enquête

Dans le cas d’une enquête conjointe, les autorités s’entendent généralement sur un ensemble d’enjeux communs. Idéalement, ces enjeux seraient établis en fonction du cadre de compétence de chaque autorité.

Les autorités peuvent également s’entendre pour que l’une d’entre elles fasse enquête sur un ou plusieurs enjeux supplémentaires dépassant la portée commune.

Entente sur le délai d’exécution

Comme les autorités assurent généralement une coordination en ce qui a trait aux questions d’importance stratégique pour leurs organisations respectives, le succès de cette coordination repose généralement sur l’établissement d’un consensus concernant le délai d’exécution. Les autorités devraient prendre en compte l’établissement de jalons clés, comme : i) un avis à l’organisation; ii) la fin de l’analyse; et iii) la formulation et la publication des conclusions. Ces jalons peuvent être saisis et revus au besoin dans un document d’approche stratégique.

Certaines autorités sont tenues par la loi de conclure certaines étapes de leur enquête, ou d’en publier les conclusions, dans des délais prescrits. Dans ce cas, il faudrait faire connaître ces exigences à toutes les autorités visées afin qu’elles puissent les prendre en compte au moment d’établir les jalons.

Recensement des points de contact

Une coordination efficace requiert une étroite communication entre les autorités. Chaque autorité peut donc choisir d'établir :

a. un ou plusieurs points de contact sur le plan opérationnel en vue d'une communication régulière (p. ex. avec un enquêteur ou un analyste technique);
b. des contacts substituts afin que l'enquête ne soit pas paralysée en cas d'absence inévitable;
c. un contact avec un membre de la haute direction ou un cadre pour avoir des discussions stratégiques et donner un nouvel élan au besoin.

En raison des différents fuseaux horaires et des horaires chargés, il est parfois difficile d'organiser des téléconférences ponctuelles et la correspondance par courriel peut entraîner des retards (en particulier lorsque le décalage horaire entre les autorités est important). Il peut donc être utile de prévoir des téléconférences régulières pour permettre aux autorités de se tenir mutuellement informées de leurs progrès et des développements importants dans le dossier.

Dans la mesure du possible, chaque autorité devrait désigner des interlocuteurs en mesure de communiquer dans une langue que les autres autorités comprennent. Il est possible de recourir à des services de traduction ou d'interprétation, mais cette option pourrait entraîner des retards importants.

Exemple d'Ashley Madison : Dès le début, les autorités ont mis par écrit, au moyen d'un échange de courriels, le fondement juridique de la coopération et de l'échange d'information et ont discuté de l'ampleur des questions qu'elles s'attendraient à examiner. Au cours des phases initiales, les autorités ont établi un calendrier officiel de réunions régulières pour discuter fréquemment des étapes, des échéanciers, des rôles et des responsabilités. Au fil du temps, une fois que les liens entre les membres des équipes d'enquête étaient bien établis, les autorités ont adopté une approche plus ponctuelle – fondée sur une compréhension commune des produits finaux cibles et du calendrier prévu.

Exemple de Clearview AI : Les autorités ont produit un plan de travail d'enquête conjoint à l'aide d'un modèle que les bureaux ont élaboré à partir du guide sur la coopération dans l'application des lois. Ils ont utilisé le document pour planifier l'enquête et assurer une compréhension commune des principaux aspects de la collaboration, notamment pour définir la portée de l'enquête, s'entendre sur le rôle de chaque bureau, établir un échéancier d'achèvement et déterminer les personnes-ressources pour les membres de l'équipe d'enquête, et leurs remplaçants. Le plan de travail était un document évolutif qui a servi de pierre angulaire tout au long de l'enquête.

Stratification de la participation

La stratification du degré de participation des autorités à une démarche en collaboration permet de réaliser des gains d'efficience. Par exemple, les autorités peuvent s'entendre pour que les participants à l'enquête jouent l'un des trois rôles suivants :

i. **Autorité responsable :** Les autorités peuvent convenir que l'une d'entre elles sera l'autorité responsable. Celle-ci peut : i) mener sa propre enquête, au lieu que plusieurs autorités mènent chacune la leur; ou ii) dans le cas d'enquêtes distinctes, mais coordonnées, assurer la liaison entre les autorités pour coordonner divers aspects de la procédure d'enquête (p. ex., collecte et communication de renseignements ou communications publiques).

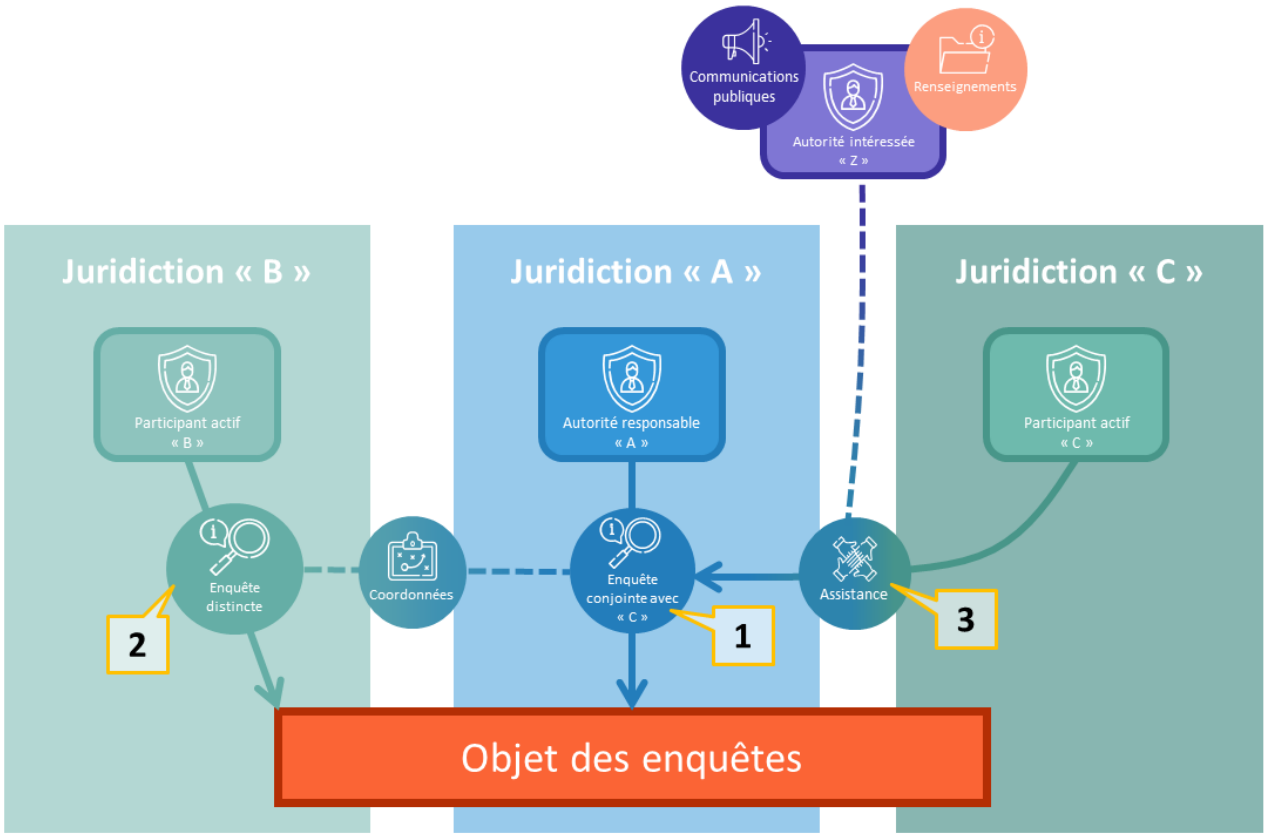
   Plusieurs critères sont pertinents pour déterminer quelle autorité, le cas échéant, devrait être l'autorité responsable, par exemple :

   - le lieu où l'organisation est établie et le pays visé;
   - le pays où un grand nombre de personnes sont touchées;
   - une question constituant une priorité stratégique pour une autorité;
   - une autorité est dotée des ressources techniques pertinentes permettant de mener une enquête.

ii. **Participants actifs :** Certaines autorités peuvent juger utile i) de mener leur propre enquête « conjointe » ou « distincte, mais coordonnée » ou ii) d'aider une autorité responsable concernant certains aspects de sa procédure d'enquête. Les autorités qui collaborent s'entendent généralement au départ sur une répartition des activités d'enquête entre l'autorité responsable et les participants actifs, après quoi elles réévaluent la situation tout au long du processus d'enquête.

iii. **Autorités intéressées :** Une autorité peut choisir de ne pas faire enquête ou de s'en remettre aux interventions d'autres autorités pour s'assurer que la question sera réglée sans qu'elle ait à consacrer des ressources à une procédure susceptible de faire double emploi. Selon ce type d'approche, une autorité intéressée pourrait apporter son soutien aux autorités qui font enquête en diffusant des communications publiques ou en communiquant des renseignements dans son territoire.

Figure 6 : Scénario de participation stratifiée



Dans cette situation, l'autorité « A » collabore avec trois autres autorités pour mener une enquête sur une organisation.

(1) L'autorité « A » a lancé une enquête conjointe avec « C » dans laquelle les deux ont convenu que « A » sera l'autorité principale. À titre de responsable, « A » est le point de contact unique avec l'organisation et le principal analyste technologique. Les deux sont des participants actifs qui coordonnent chaque étape de l'enquête dans le but de rédiger un seul rapport final et de prendre des mesures conjointes au besoin.

(2) L'autorité « B » enquête sur la même organisation visée, mais a choisi de mener sa propre enquête distincte en raison de ses exigences législatives. Bien que « B » soit aussi un participant actif et qu'il partage l'information avec « A » et « C », il se concentre sur différentes questions et envoie sa propre correspondance dans l'intention de produire son propre rapport distinct.

(3) L'autorité « Z » s'intéresse au cas, mais elle a déterminé que, compte tenu du travail effectué par les trois autres autorités, sa participation active ne constituerait pas une utilisation efficace de ses ressources. Au lieu de cela, l'autorité « Z » communique l'information contextuelle dont elle dispose et publie une lettre ouverte indiquant ses préoccupations et son intérêt à l'égard de la question.

Attribution d’activités d’enquête particulières

Pour bénéficier des avantages d’une enquête menée en collaboration, les autorités devraient dans la mesure du possible tenter de répartir les tâches de l’enquête de manière à tirer parti des points forts de chacune et des ressources disponibles pour obtenir les résultats les plus efficaces et efficients.

Collecte de renseignements et communication avec la personne visée par l’enquête

i. **Contact avec la personne visée par l’enquête :** Dans le cas d’une enquête conjointe, les autorités peuvent choisir de désigner l’une d’entre elles comme principal point de contact pour la communication ou la correspondance régulière ou administrative avec l’organisation visée par l’enquête afin i) de limiter les dédoublements ou le risque de confusion associé à l’existence de plusieurs points de contact; ii) de résoudre un problème de différences linguistiques ou de décalage horaire; ou iii) de simplement répartir les responsabilités et la charge de travail connexe entre les autorités qui coordonnent leurs activités. Chaque autorité communique généralement avec ses propres plaignants au besoin.

ii. **Correspondance :** Les autorités pourraient s’entendre pour que toute la correspondance importante (notification d’enquête, demandes initiales ou détaillées d’information, etc.) soit rédigée par une autorité qui intégrera les commentaires des autres avant de l’envoyer.

Les autorités devraient déterminer si la correspondance sera envoyée par l’une d’entre elles au nom de toutes les autorités qui coordonnent leurs activités ou séparément par chaque autorité. Si un document doit porter plusieurs signatures, il serait utile pour faciliter le processus que chaque autorité i) convienne de la méthode d’approbation de la documentation (p. ex., par courriel) et ii) fournisse une version PDF de la signature et du logo de l’autorité appropriés, ainsi que du libellé du bloc de signature.

iii. **Collecte de renseignements :** Même si le principal point de contact doit transmettre, au nom du groupe, les questions à l’organisation qui fait l’objet de l’enquête, les autorités se concertent généralement pour formuler ces questions de manière à s’assurer qu’elles permettront d’obtenir les renseignements nécessaires à chaque autorité en fonction de son cadre législatif particulier.

Lorsque la collecte de renseignements se fait au cours d’une téléconférence ou d’une réunion, les autorités peuvent envisager de participer conjointement à la démarche au lieu de tenir plusieurs discussions unilatérales. Les interactions en direct entraînent souvent les discussions dans une direction imprévue et la présence de chaque autorité lui permet i) de s’assurer qu’elle comprend bien le matériel présenté de vive voix ou par écrit; ii) de poser toute question supplémentaire qui peut en découler; et iii) d’éviter la création d’exposés de preuve différents/conflictuels si l’objet de l’enquête donne à chaque autorité des réponses différentes aux mêmes questions.

Même si plusieurs autorités participent à la réunion, elles peuvent s’entendre à l’avance sur une liste préliminaire de questions à poser au cours de la réunion ou sur la personne qui animera la

réunion (généralement, le principal point de contact). Cette façon de procéder aide parfois à éviter le dédoublement des questions et à s'assurer qu'il sera possible de répondre aux questions de chaque autorité dans le temps dont on dispose.

Les autorités devraient envisager de tirer parti de leurs points forts respectifs en matière de collecte d'éléments de preuve au moment de définir les responsabilités de chacune — p., ex., certaines autorités pourraient avoir le pouvoir :

- d'interroger des témoins sous serment;
- d'ordonner la production de déclarations sous serment, de documents ou de dossiers;
- d'entrer dans un lieu ou d'y effectuer une perquisition et de saisir des éléments de preuve;
- d'effectuer des enquêtes en ligne (p. ex., recherche de dispositifs ou de stockage électroniques); ou
- de prendre des mesures si l'organisation visée par l'enquête fait de l'obstruction.

Lorsqu'on recueille des éléments de preuve, il est important de tenir compte de toute exigence des différents partenaires en matière de preuve afin de s'assurer que chaque autorité qui pourrait vouloir exercer ses pouvoirs d'exécution serait en mesure d'utiliser l'information communiquée. Par exemple, certaines autorités pourraient exiger des détails sur la façon dont l'information a été recueillie ou exiger que certaines méthodes ne soient pas utilisées (p. ex., pour se conformer aux exigences d'équité procédurale).

Remarque : Même si les autorités choisissent de mener des enquêtes distinctes simultanées, elles peuvent se concerter pour élaborer leurs demandes de renseignements respectives afin que chacune puisse obtenir des renseignements pouvant être utiles à l'autre. Par ailleurs, lorsqu'une autorité sait qu'une organisation a déjà fourni des réponses à une autre autorité, elle peut envisager de demander une copie de ces réponses directement à l'organisation. Cette approche permettrait d'éviter certaines complications liées à la communication de cette information en vertu d'une entente d'échange de renseignements (p. ex., transmission de documents volumineux et limites imposées à l'utilisation des renseignements fournis par une autre autorité).

Analyse

Lorsque la prise d'une décision concernant un enjeu nécessite une analyse en fonction de dispositions législatives sensiblement similaires (p. ex., sur la base des principes de l'OCDE relatifs à l'équité dans le traitement de l'information, de la Résolution de Madrid ou de la Convention 108 du Conseil de l'Europe) ou des normes techniques applicables à l'évaluation des mesures de sécurité adéquates (p. ex., normes de sécurité sur les données de l'industrie des cartes de paiement), les autorités pourraient partager la responsabilité de certains aspects de l'analyse.

i. **Analyse technique :** Des enquêtes portant sur des atteintes à la sécurité des données touchant plusieurs pays ou d'autres enquêtes en lien avec la technologie pourraient offrir à une autorité la possibilité d'effectuer une analyse technique au nom d'un groupe. Une analyse

technique nécessite souvent l'utilisation de matériel spécialisé ou de logiciels ou un savoir-faire que certaines autorités ne possèdent pas.

Si les autorités souhaitent s'entendre pour que l'une d'entre elles effectue des analyses techniques particulières, elles peuvent choisir de se concerter à l'avance afin de déterminer la portée des analyses (y compris les questions techniques auxquelles l'organisation devra répondre) ainsi que toute exigence particulière en matière de preuve (p., ex., documentation du processus d'analyse ou des résultats).

Encore une fois, si une autorité effectue des analyses au nom de plusieurs autorités, elle doit s'assurer qu'elle comprend bien le cadre législatif de ses partenaires.

ii. **Rédaction du rapport (analyse des politiques ou analyse juridique) :** Les autorités de coordination conserveront toujours la capacité de mener leurs propres analyses et, en fin de compte, de tirer des conclusions différentes. En général, cependant, il est peu probable que les autorités chargées de la coordination en arrivent à des conclusions radicalement différentes, étant donné qu'elles auraient discuté de la question en fonction de leurs cadres législatifs respectifs. De plus, des communications régulières tout au long de l'enquête permettront de s'assurer que les autorités se coordonnent au fur et à mesure que de nouvelles décisions sont prises à partir d'éléments de preuves. Dans le cas d'une enquête conjointe, les autorités qui coordonnent leurs activités ont généralement deux options :

- **Rapport conjoint** : Si les décisions sont fondées sur une analyse en vertu de lois sensiblement similaires et que les autorités peuvent dégager un consensus concernant leurs conclusions respectives, elles peuvent choisir de produire un rapport conjoint. Il est parfois difficile de s'entendre sur la formulation, mais on peut rédiger le rapport de manière à faire état des différences entre les lois des autorités et les analyses en découlant. Un rapport conjoint offre aussi la possibilité de faire connaître une position unique et d'en tirer parti de manière à obtenir une plus grande coopération de la part de l'organisation et un résultat qui a plus de chances de contribuer à protéger la vie privée.

- **Rapports distincts, mais coordonnés** : Si une autorité doit produire son propre rapport indépendant ou que les analyses peuvent ne pas être uniformes d'un pays à l'autre (même s'il est possible que les conclusions finales soient très similaires), les autorités qui coordonnent leurs activités peuvent choisir de rédiger des rapports distincts. Lorsque leurs conclusions sont similaires, elles devraient envisager de tirer parti de la force d'un message unique en publiant simultanément des rapports distincts, peut-être accompagnés d'une lettre conjointe résumant leurs conclusions ou leurs attentes à l'égard de l'organisation pour la suite des choses.

Remarque : Possibilité d'échange de renseignements – Si les autorités choisissent de ne pas coordonner leur analyse ou la rédaction de leur(s) rapport(s), elles peuvent néanmoins bénéficier de l'échange des détails issus de leurs analyses respectives pour améliorer leur efficience et valider leurs conclusions. Cette stratégie permet parfois aux autorités i) de tirer des conclusions plus uniformes, car elles ont une compréhension commune des faits et bénéficient du point de vue de chacune ou ii) d'être mieux préparées à expliquer les différences entre les conclusions d'un pays à l'autre.

Exemple d'Ashley Madison : Dans le contexte de l'enquête conjointe menée par le CPVP et l'OAIC, les autorités ont convenu mutuellement que le CPVP serait le point de contact unique avec Ashley Madison puisque l'entreprise est établie au Canada. Toutes les communications officielles ont fait l'objet de discussions et ont été approuvées à l'avance par les deux autorités. Le CPVP et l'OAIC ont rédigé et publié conjointement le rapport final sur les conclusions en étroite consultation, et c'est l'OAIC qui a dirigé le processus.

Simultanément, le CPVP/OAIC et la FTC ont partagé la correspondance et les réponses d'Ashley Madison, mais n'ont pas eu de communications conjointes, étant donné la démarcation entre les enquêtes. Cela s'est révélé utile, car le recoupement des réponses d'Ashley Madison dans le cadre des deux processus d'enquête a permis d'obtenir des renseignements précieux. Les trois autorités ont également effectué une visite conjointe sur place, ce qui a permis aux enquêteurs des trois autorités de se coordonner et de mettre en commun leur expertise. Les trois autorités ont également échangé des renseignements généraux sur leurs constatations et les prochaines étapes prévues.

Exemple de Clearview AI : L'une des premières étapes de la planification de l'enquête conjointe a été d'établir quel bureau assumerait le rôle principal ou le rôle de coordonnateur, compte tenu du nombre d'autorités en cause. Les autorités ont convenu que le CPVP était le mieux placé pour remplir ce rôle, compte tenu de sa capacité et du fait que Clearview fournissait ses services dans toutes les provinces. Le CPVP a collaboré étroitement avec les trois autres autorités pour obtenir de la rétroaction, une entente et des approbations à chaque étape de l'enquête. Le rapport final des conclusions a été rédigé et publié conjointement.

Communications publiques

Les communications publiques offrent aux autorités la possibilité d'amplifier les résultats et les leçons tirées de leurs activités coordonnées et de bâtir la confiance entre les partenaires en s'assurant que les autres autorités sont pleinement informées et préparées à réagir à la réponse et aux demandes d'information du public qui s'ensuivront.

Le cadre législatif (ou l'approche stratégique) de chaque autorité dictera la mesure dans laquelle elle peut faire connaître au public sa participation à une enquête en cours ou les résultats d'une enquête complétée. Il importe que toutes les autorités qui coordonnent leurs activités i) comprennent, avant même d'amorcer une enquête, toutes les limites concernant la publication et ii) respectent les exigences de chaque autorité au moment de publier leurs propres déclarations publiques (p. ex., l'**autorité A** ne peut pas annoncer publiquement qu'elle fait enquête sur une question, mais l'**autorité B** le peut. Si l'autorité **B** veut annoncer qu'elle fait enquête sur la question, il est possible qu'elle doive éviter de mentionner l'implication de l'autorité **A**.)

Sous réserve des restrictions susmentionnées, les autorités pourront à leur choix avoir recours à l'une des approches suivantes :

i. Communications conjointes : Les autorités peuvent diffuser des communications publiques conjointes. Il faut parfois du temps et des efforts pour s'entendre sur la formulation exacte, ou sur la production des traductions nécessaires, mais les communications conjointes témoignent d'un esprit d'unité et de solidarité entre les pays et peuvent par conséquent avoir davantage d'impact.

ii. Communications coordonnées : Si une autorité qui coordonne les activités décide de diffuser des communications publiques distinctes de façon indépendante, il est généralement utile de transmettre le message à ses partenaires avant de le diffuser. De cette façon, i) les autres autorités pourront envoyer en même temps des messages coordonnés, qui auront ainsi davantage d'impact, ii) on pourra s'assurer que les messages ne révèlent aucun renseignement contre le gré d'un autre partenaire; ou iii) les autorités seront mieux préparées à expliquer toute différence importante entre leurs messages respectifs.

> Même si la contribution d'une autorité à une enquête indépendante est limitée (communication de renseignements, consultations sur une approche, etc.), une simple déclaration publique indiquant que « l'enquête a bénéficié de l'assistance de l'autorité X » peut véhiculer un message positif concernant la collaboration internationale.

Exemple d'Ashley Madison : Dans le cadre de l'enquête conjointe menée entre le CPVP et l'OAIC, les autorités ont mis en œuvre une stratégie de communication coordonnée. Les autorités ont publié des communications publiques distinctes et indépendantes, mais ont discuté des messages et de la stratégie dans le contexte de l'enquête conjointe.

Des communications indépendantes de la FTC ont également contribué à attirer l'attention et à amplifier l'impact des résultats des enquêtes.

La conclusion de l'enquête conjointe a reçu beaucoup d'attention du public dans les trois juridictions et à l'échelle internationale. Selon une analyse médiatique, environ 128 millions de personnes ont été rejointes par des reportages publiés sur l'enquête. Cela a permis d'informer un public mondial de personnes et d'organisations axées sur les données de l'importance de la protection de la vie privée à l'ère numérique et de la valeur de la coopération et de l'application de la loi transfrontalières, ainsi que de fournir un effet dissuasif puissant et mondial.

Exemple de Clearview AI : Les autorités dans l'enquête de Clearview ont utilisé un amalgame de communications publiques conjointes et coordonnées pour sensibiliser le public. Plus particulièrement, les autorités ont conjointement lancé l'enquête et communiqué les résultats. Les autorités ont convenu à l'avance du contenu de ces communiqués et les ont publiés simultanément. Les quatre autorités ont également tenu une conférence de presse conjointe au cours de laquelle les commissaires et le président de la CAI ont fait des déclarations et répondu aux questions des médias. Cette stratégie de communication a contribué à la couverture mondiale de l'enquête et du rapport des conclusions par les médias nationaux et internationaux et a amplifié l'impact de l'affaire. L'analyse des médias a permis de déterminer que les articles publiés sur l'enquête ont permis de rejoindre environ 33 millions de personnes à l'échelle mondiale.

Pouvoirs d'application de la loi

Les pouvoirs d'application de la loi conférés aux autorités varient grandement d'un pays à l'autre. Entre autres, celles-ci peuvent être habilitées à :

- imposer des amendes ou des sanctions administratives pécuniaires;
- rendre des ordonnances;
- conclure des ententes exécutoires qui peuvent parfois offrir de la souplesse pour obtenir des recours plus holistiques;

- prendre des mesures administratives ou obtenir une ordonnance d'injonction;
- assurer la conformité au moyen de procédures judiciaires;
- rendre public le nom d'une organisation.

Avant d'amorcer une enquête menée en collaboration, les autorités devraient s'assurer qu'elles connaissent bien les pouvoirs de leurs partenaires en matière d'application des lois (ou les limites de ces pouvoirs). Chaque pouvoir peut s'avérer un moyen efficace pour atteindre la conformité, particulièrement lorsque chaque autorité est en mesure de tirer parti de l'ensemble unique d'outils d'application de la loi dont elle dispose. Des pouvoirs complémentaires à cet égard peuvent offrir la possibilité d'exercer des pressions plus fortes sur une organisation pour l'inciter à se conformer. C'est pourquoi il est parfois important de prendre en compte les pouvoirs d'application de la loi respectifs au moment de choisir des partenaires aux fins d'une coordination des activités.

Par exemple, les partenaires pourraient adopter une approche en plusieurs étapes pour tirer le maximum de leurs pouvoirs respectifs. Une autorité peut commencer par rendre public le nom de l'organisation dans le but d'accélérer une conformité volontaire et de sensibiliser les intervenants. Si cette approche ne porte pas ses fruits, une deuxième autorité pourrait alors prendre le relais et intenter des poursuites judiciaires.

Exemple d'Ashley Madison : À la suite de l'enquête, Ruby Corp a pris des engagements juridiquement contraignants envers les trois autorités, ainsi que plusieurs États américains, afin d'améliorer ses pratiques en matière de sécurité de l'information et d'être plus transparent avec les utilisateurs au sujet de ses pratiques de traitement de l'information. En vertu d'un engagement exécutoire avec l'Australie et d'un accord de conformité avec le Canada, Ruby Corporation devait également réduire les périodes de conservation des données sur ses clients et améliorer l'exactitude des renseignements qu'elle recueillait, alors que, à la suite d'un règlement avec la FTC et plusieurs États américains, la société a également été contrainte de payer environ 1,6 million de dollars américains.

Conclusion

De plus en plus, les organisations ont tendance à établir une présence à l'échelle mondiale et elles disposent d'une technologie leur permettant de traiter un volume croissant de données personnelles. La coopération offre à l'ensemble des autorités chargées de l'application des lois sur la protection de la vie privée la possibilité de régler un problème mondial en adoptant une solution mondiale. Lorsque vous envisagez de coopérer dans l'application des lois, gardez à l'esprit quelques points clés importants :

i. Établissez et entretenez des relations à la fois formelles et informelles avec d'autres autorités, au niveau de la haute direction et sur le plan opérationnel – ces relations jetteront les bases de la coopération. À mesure que le nombre de questions d'interréglementation augmente, des efforts doivent également être déployés pour établir et maintenir de nouvelles relations avec des autorités extérieures à la sphère de la protection de la vie privée.

ii. Dotez-vous à l'interne des capacités voulues pour détecter les possibilités de coopération dans l'application des lois et y donner suite – p. ex. en élaborant des protocoles, en instaurant une formation sur la coopération dans l'application des lois ou en proposant des détachements ou des échanges d'employés.

iii. Comme il faut généralement conclure une entente d'échange de renseignements afin de coopérer dans l'application des lois, soyez proactifs et concluez à l'avance ce type d'entente pour être prêts à saisir par la suite les possibilités de coopération qui se présenteront.

iv. La forme de coopération appropriée varie d'une situation à l'autre. Les autorités peuvent obtenir des résultats concrets rien qu'en échangeant des renseignements ou en envoyant une lettre conjointe.

v. À notre époque caractérisée par l'augmentation de la circulation transfrontière, la coopération dans l'application des lois, sous toutes ses formes, permet d'obtenir de façon plus efficiente de meilleurs résultats en matière de conformité. Au moment de choisir vos partenaires, envisagez les points forts des autorités qui sont complémentaires aux vôtres. En même temps, les APD doivent déterminer si leur expertise en matière de protection de la vie privée peut aider les autorités d'autres régimes de réglementation (et inversement) lorsqu'ils examinent les possibilités de coopération interréglementaires.

vi. Pour éviter le double emploi et tirer le maximum d'avantages d'une enquête conjointe ou coordonnée, dégagez un consensus sur un plan stratégique qui tire parti des points forts de chaque partenaire (p. ex., l'emplacement, la capacité, un savoir-faire spécial ou des pouvoirs particuliers).

vii. Le succès de la coopération repose sur la confiance. Dans la mesure du possible, les partenaires devraient s'efforcer de se tenir mutuellement pleinement informés des activités coordonnées, de respecter leurs engagements respectifs et de faire preuve de souplesse dans le but d'en arriver à un consensus.

ANNEXE A

Entente mondiale de coopération transfrontière dans l’application des lois

Table des matières

Préambule

Rappelant qu'une résolution adoptée par la Conférence de Varsovie prévoyait l'élargissement du mandat du Groupe de travail sur la coopération internationale dans l'application des lois en vue d'élaborer une approche commune pour le traitement des dossiers transfrontières et la coordination de l'application des lois, et de présenter cette approche dans un cadre multilatéral portant sur la communication d'information liée à l'application des lois, notamment sur la façon dont cette information doit être traitée par ceux qui la reçoivent;

Prenant acte qu'un phénomène mondial nécessite une intervention mondiale et que la création de stratégies et d'outils efficaces pour éviter les doubles emplois, faire une utilisation plus efficace des ressources limitées et améliorer l'efficacité de l'application de la loi dans les situations où les atteintes à la vie privée et à la sécurité des données transcendent les frontières nationales est dans l'intérêt des autorités[1], des individus, des gouvernements et des entreprises;

Conscients qu'il est de plus en plus apparent que l'augmentation de la circulation transfrontière des données et que les pratiques des organisations nationales et multinationales associées à cette circulation peuvent rapidement porter atteinte à la vie privée et à la protection des données personnelles d'un très grand nombre de personnes dans le monde et que, par conséquent, cette augmentation de la circulation transfrontière de données devrait s'accompagner d'une meilleure communication de l'information entre autorités d'exécution des lois sur la protection des données et de la vie privée et d'une coopération internationale accrue dans l'application des lois, et que cette communication et cette coopération sont essentielles pour protéger la vie privée et les données et servir ainsi un intérêt public important;

Tenant compte du fait que plusieurs autorités ont à plusieurs occasions fait enquête en même temps sur les mêmes pratiques ou atteintes;

Rappelant les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108 du Conseil de l'Europe), en particulier les dispositions sur l'entraide énoncées au chapitre IV;

Rappelant que la *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée* (2007) conseille aux pays membres de coopérer au niveau international pour faire appliquer les lois sur la protection des données et de la vie privée et de prendre les mesures voulues afin :

- d'améliorer leurs cadres nationaux d'application des lois sur la protection des données et de la vie privée afin de faciliter la coopération transfrontière dans le respect des lois nationales;

- d'avoir recours à l'assistance mutuelle pour assurer l'application des lois sur la protection des données et de la vie privée, notamment par la notification, la transmission des plaintes, l'aide aux enquêtes et la communication d'information sous réserve des mesures de sécurité appropriées;

- d’engager les intervenants pertinents aux discussions et activités visant à renforcer la coopération dans l’application des lois sur la protection des données et de la vie privée;

Rappelant que les résolutions adoptées lors des Conférences internationales des commissaires à la protection des données et de la vie privée précédentes et la Déclaration de Montreux encourageaient notamment les autorités à redoubler d’efforts pour appuyer la coopération internationale dans l’application des lois et à travailler avec les organisations internationales afin de renforcer la protection des données à l’échelle mondiale;

Faisant fond sur les progrès considérables accomplis au cours des dernières années aux niveaux régional et international pour améliorer les accords portant notamment sur la coopération transfrontière dans l’application des lois sur la protection des données et de la vie privée;

Reconnaissant que la coopération transfrontière dans l’application des lois peut prendre différentes formes; elle peut avoir lieu à différents niveaux (national, régional ou international), être de différents types (coordonnée ou non) et porter sur plusieurs activités (communication de pratiques exemplaires, ratissages d’Internet, enquêtes coordonnées ou mesures concertées d’application des lois menant à des peines ou à des sanctions); toutefois, quelle que soit la forme de cette coopération, son succès repose sur l’instauration d’une culture de communication proactive et pertinente de l’information, qui peut être confidentielle ou non et renfermer ou non des données personnelles, et sur une coordination appropriée des activités d’application des lois;

Encourageant toutes les autorités à utiliser et à perfectionner les plateformes de coopération et les mécanismes d’application de la loi connexes et à aider à optimiser l’efficacité de la coopération transnationale dans l’application de la loi;

Concluant qu’il faut adopter une approche multilatérale pour intervenir efficacement à la suite d’atteintes à la sécurité des données et à la vie privée qui touchent plusieurs territoires de ressort et que l’on a donc grand besoin, pour contrer ces atteintes, de mécanismes appropriés facilitant la communication d’information confidentielle concernant l’application de la loi et la coordination entre les autorités chargées de son application;

Conséquemment, les autorités sont fortement encouragées à adhérer à la présente entente et à s’engager à respecter ses dispositions, notamment celles régissant la confidentialité et la protection des données, quand elles participent à des activités transfrontières d’application des lois.

1. Définitions

Les définitions suivantes s’appliquent pour les besoins de la présente entente :

Coopération dans l’application des lois – Expression générale faisant référence à des autorités qui collaborent pour appliquer les lois sur la protection des données et de la vie privée.

Application concertée des lois – Type particulier de coopération dans l'application des lois en vertu de laquelle deux ou plusieurs autorités concertent leurs activités en vue de faire respecter les lois sur la protection des données et de la vie privée sur leurs territoires respectifs.

Lois sur la protection des données et de la vie privée – Ensemble des lois d'un territoire de ressort dont l'application a pour effet de protéger les données personnelles.

Autorité d'exécution de la loi sur la protection des données et de la vie privée (« autorité[2] ») – Tout organisme public ayant la responsabilité d'appliquer les lois sur la protection de la vie privée ou des données et détenant le pouvoir de faire enquête ou de prendre des mesures d'application des lois.

Demande d'assistance – Requête adressée par une partie à une ou plusieurs autres parties en vue de coopérer et de coordonner l'application d'une loi sur la protection des données et de la vie privée, entre autres :

i. le renvoi d'une question liée à l'application d'une loi sur la protection des données et de la vie privée;

ii. une demande de coopération dans l'application d'une loi sur la protection des données et de la vie privée;

iii. une demande de coopération dans une enquête au sujet d'un manquement allégué à une loi sur la protection des données et de la vie privée;

iv. le transfert d'une plainte alléguant un manquement à une loi sur la protection des données et de la vie privée.

Partie – Autorité signataire de la présente entente.

Comité – Comité de direction de la Conférence internationale des commissaires à la protection des données et de la vie privée.

Plaignant – Toute personne ayant déposé auprès de l'autorité une plainte alléguant un manquement à une loi sur la protection des données et de la vie privée.

2. Objet

La présente entente a pour objet de favoriser la protection des données par les organisations qui traitent des données personnelles dans plusieurs territoires de ressort. Elle encourage et facilite la coopération entre toutes les autorités grâce à la communication d'information, en particulier de l'information confidentielle concernant l'application des lois en lien avec des enquêtes éventuelles ou en cours, et s'il y a lieu, l'entente régit en outre la coordination des activités d'application de la loi par ces autorités pour leur permettre d'utiliser leurs ressources limitées de façon aussi efficiente et efficace que possible.

3. Finalité

La présente entente vise à réaliser sa finalité en atteignant les objectifs suivants :

i. énoncer les principales dispositions à appliquer pour communiquer l'information concernant l'application des lois, notamment l'utilisation de cette information par les parties qui la reçoivent;

ii. énoncer les principales dispositions à appliquer pour communiquer l'information concernant l'application des lois, notamment l'utilisation de cette information par les parties qui la reçoivent;

iii. encourager les parties à s'engager dans une coopération transfrontière en faisant appel à la communication d'information concernant l'application de la loi et, s'il y a lieu, à la mise en commun de leur savoir, leur expertise et leur expérience susceptibles d'aider d'autres parties à aborder les questions d'intérêt commun;

iv. encourager les parties à appuyer la création de plateformes sécurisées pour la communication électronique de l'information et à s'en servir pour s'échanger l'information concernant l'application des lois, en particulier l'information confidentielle concernant les activités éventuelles ou en cours d'application des lois.

4. Nature de l'entente

La présente entente énonce les engagements des parties à l'égard de la coopération transfrontière dans l'application des lois, en particulier au chapitre de la réciprocité, de la confidentialité, de la protection des données et de la coordination.

L'entente NE VISE PAS :

i. à remplacer les conditions ou mécanismes nationaux et régionaux existants régissant la communication de l'information ni à contrecarrer les accords similaires conclus par l'entremise d'autres réseaux;

ii. à créer des obligations juridiquement contraignantes ni à modifier des obligations existantes découlant d'autres ententes ou du droit international ou national;

iii. à empêcher une partie de coopérer avec d'autres parties, ou avec des autorités qui ne sont pas parties à la présente, en vertu d'autres lois, accords, traités ou ententes (juridiquement contraignants ou non);

iv. à créer des obligations ou des attentes de coopération qui vont au-delà de l'autorité ou de la compétence d'une partie;

v. à contraindre les parties à collaborer dans le cadre d'activités d'application de la loi, notamment à fournir de l'information confidentielle ou non qui renferme ou non des données personnelles.

5. Principe de réciprocité

Toutes les parties coopéreront dans la mesure du possible avec les autres parties et leur viendront en aide dans le cadre des activités d'application transfrontière des lois, notamment en répondant aux demandes d'assistance dans les meilleurs délais possible.

Quand ils communiquent des données et de l'information concernant l'application des lois en vertu de la présente entente, les parties devraient indiquer par écrit qu'elles le font conformément aux modalités de cette entente. Les parties qui reçoivent une demande d'assistance devraient en accuser réception dans les meilleurs délais, de préférence dans les deux semaines suivant réception de la demande.

Avant d'effectuer une demande d'assistance auprès d'une autre partie, la partie demanderesse devrait effectuer une vérification préliminaire interne pour s'assurer que la demande s'inscrit dans le champ d'application et l'objet de la présente entente et qu'elle n'impose aucun fardeau excessif à l'autre partie. Si elle le souhaite, une partie peut limiter sa coopération dans l'application transfrontière de la loi, notamment dans les situations suivantes :

i. la question ne relève pas de son autorité ou de sa compétence;

ii. la question ne constitue pas un acte ou une pratique au sujet de laquelle elle peut faire enquête ou au sujet de laquelle ses lois nationales peuvent être appliquées;

iii. les ressources sont limitées;

iv. la question est incompatible avec d'autres priorités ou obligations juridiques;

v. la question ne présente pas un intérêt mutuel;

vi. la question n'entre pas dans le champ d'application de la présente;

vii. un autre organisme serait mieux désigné pour s'occuper de la question;

viii. toute autre situation qui empêcherait une partie de coopérer.

Si une partie refuse ou limite sa coopération, elle devrait en indiquer les raisons par écrit à la partie qui l'a sollicitée, dans la mesure du possible dans les quatre semaines suivant réception de la demande d'assistance.

6. Principe de confidentialité

6.1 Sous réserve du paragraphe 6.2, les parties assurent la confidentialité de toute information reçue d'autres parties en vertu de la présente entente :

i. en respectant le caractère confidentiel de toute information reçue ou de toute demande d'assistance au titre de la présente entente, y compris le fait qu'une autre partie envisage de faire enquête, a entrepris une enquête ou mène actuellement une enquête et au besoin, en prenant des arrangements supplémentaires pour se conformer aux exigences légales nationales de la partie qui envoie des renseignements;

ii. en ne communiquant pas à un tiers l'information obtenue d'autres parties, notamment à d'autres autorités nationales ou à d'autres parties sans le consentement écrit de la partie ayant fourni l'information en vertu de la présente entente;

iii. en limitant l'utilisation de cette information aux fins pour lesquelles elle a été communiquée au départ;

iv. si une partie reçoit d'un tiers (par exemple un individu, un organisme judiciaire ou un autre organisme d'exécution de la loi) une demande de communication d'information confidentielle reçue d'une autre partie en vertu de la présente entente, elle doit :

    a. s'opposer à la demande, ou s'efforcer de la limiter le plus possible;
    b. respecter le caractère confidentiel de l'information en question;
    c. informer sans délai la partie ayant fourni l'information et à chercher à obtenir son consentement à la communication de l'information en question;
    d. informer la partie ayant fourni l'information de l'existence de lois nationales qui exigent néanmoins la communication, si la partie ayant fourni l'information refuse de consentir à la communication;

v. en cas de retrait de l'entente, en respectant le caractère de toute information confidentielle communiquée par une autre partie en vertu de la présente entente ou encore, avec l'accord mutuel des autres parties, en retournant l'information, en la détruisant ou en l'effaçant;

vi. en veillant à ce que toutes les mesures techniques et organisationnelles voulues soient prises pour protéger toute information fournie en vertu de la présente entente, notamment en retournant ou en traitant l'information (conformément à la législation nationale dans la mesure du possible) dans le respect des conditions de consentement de la partie ayant fourni l'information.

6.2 S'il est possible que des obligations juridiques nationales empêchent une partie de respecter l'un des points des alinéas 6.1i) à vi), il doit en informer au préalable les parties ayant fourni l'information.

7. Principes de protection des données et de la vie privée

Selon les parties ou l'activité d'application de la loi en question, il pourrait être nécessaire de communiquer des renseignements personnels. Toutefois, pour respecter les principes reconnus en matière de protection des données et de la vie privée, la communication de renseignements personnels devrait se limiter le plus possible aux situations où cette communication est nécessaire pour garantir une application efficace de la loi sur la protection de la vie privée et des données. Toutes les parties à l'entente qui communiquent ou reçoivent des données personnelles feront de leur mieux pour respecter leurs mesures de sécurité mutuelles visant à protéger les données. Les autorités reconnaissent cependant que ces efforts ne suffisent pas toujours pour permettre la communication de renseignements personnels.

Dans ce cas, si la partie qui communique des renseignements personnels a besoin de mesures de sécurité particulières visant à protéger les données, elle devrait :

- demander aux autres parties de lui donner l'assurance qu'elles se conformeront aux exigences énoncées à l'annexe I;

ou prévoir d'autres ententes entre la partie qui communique les données personnelles et la partie qui les reçoit de manière à assurer le respect intégral des exigences de chaque partie concernant la protection des données et de la vie privée. Les parties doivent indiquer au Comité si elles s'engagent à respecter les exigences énoncées à l'annexe I ou lui faire part d'autres arrangements tel qu'il est susmentionné. En principe, cet avis devrait être donné au moment de présenter un avis d'intention de participer conformément à l'article 13 ou, en tout état de cause, avant de recevoir des données personnelles d'une autre partie en vertu de la présente entente. Une liste des parties, y compris leurs avis initiaux et mis à jour concernant l'annexe I et tout autre arrangement tel qu'il est susmentionné, sera mise à la disposition de toutes les parties.

8. Principes de coordination

Les parties feront de leur mieux pour coordonner leurs activités d'application transfrontière des lois. Les principes qui suivent ont été établis en vue de coordonner l'application transfrontière des lois sur la protection de la vie privée ou des données :

i. Détermination des activités qui se prêteraient à une coordination

    a. Les autorités devraient cerner les questions ou les incidents qui se prêteraient à une coordination et rechercher activement les possibilités de coordonner leurs activités lorsque c'est possible et bénéfique.

ii. Évaluation des possibilités de participation

    a. Les autorités devraient évaluer attentivement, au cas par cas, la pertinence de participer à une application de la loi coordonnée et communiquer clairement leur décision aux autres autorités.

iii. Participation à des actions coordonnées

    a. Les autorités devraient évaluer attentivement, au cas par cas, la pertinence de participer à une application de la loi coordonnée et communiquer clairement leur décision aux autres autorités.

iv. Facilitation de la coordination

    a. Les autorités devraient se préparer à l'avance à participer à des actions coordonnées.

v. Direction d'une action coordonnée

    a. Les autorités qui dirigent une action coordonnée devraient conclure des ententes pratiques qui simplifient la coopération et appuient ces principes.

Les parties peuvent se reporter au Cadre de coordination internationale de l'application des lois pour un complément d'information au sujet de ces principes.

9. Résolution des problèmes

Tout différend entre les parties en lien avec la présente entente devrait de préférence être réglé par voie de discussion entre leurs personnes-ressources désignées et, à défaut d'un règlement dans un délai raisonnable, entre les premiers dirigeants des parties.

10. Répartition des coûts

Chaque partie prend à sa charge ses propres coûts associés à la coopération, conformément à la présente entente.

Les parties peuvent convenir de partager ou de transférer les coûts d'une coopération en particulier.

11. Restitution des éléments de preuve

Les parties renvoient les éléments dont ils n'ont plus besoin si la partie qui les a fournis a demandé par écrit au moment de leur communication qu'ils lui soient renvoyés. Si la partie ayant fourni les éléments ne demande pas qu'ils lui soient renvoyés, l'autre partie en dispose selon une méthode prescrite par la

partie qui les a fournis ou, si cette dernière n'a précisé aucune méthode, selon une méthode sécuritaire, dans les meilleurs délais possible après que les éléments ne sont plus nécessaires.

12. Critères d'admissibilité

Toute autorité peut présenter au Comité un avis d'intention indiquant qu'elle s'engage à participer à la présente entente :

i. en tant que membre, si elle est un membre agréé de la Conférence internationale des commissaires à la protection des données et de la vie privée (la Conférence) et donc répond aux exigences d'admissibilité énoncées à l'article 5.1 des règles et procédures de la Conférence, notamment l'exigence concernant une autonomie et une indépendance appropriées;

ii. ou en tant que partenaire, même si elle n'est pas un membre accrédité de la Conférence, si
   a. elle représente un État signataire de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108);
   b. ou elle est membre du Global Privacy Enforcement Network (GPEN);
   c. ou elle participe à l'Accord de coopération de l'APEC sur la protection transfrontière des données (Cross-border Privacy Enforcement Arrangement ou CPEA);
   d. ou elle est membre du Groupe de travail Article 29.

Le Comité conservera une liste actualisée de toutes les autorités qui se sont engagées à participer à la présente entente et de toutes celles qui se seront engagées à respecter l'annexe I. Toutes les parties devraient avoir facilement accès à cette liste.

13. Rôle du comité de direction de la conférence internationale

Le Comité :

a. reçoit les avis d'intention de participer à l'entente ou de s'en retirer;

b. reçoit les avis d'engagement à l'annexe I ou autres arrangements comme il est mentionné à l'article 7;

c. examine ces avis pour vérifier que l'autorité peut être partie à l'entente;

d. examine la mise en œuvre de l'entente trois ans après son entrée en vigueur et présente ses conclusions à la Conférence internationale;

e. fait connaître l'entente;

f. recommande à la Conférence internationale, après avoir dûment tenu compte des renseignements, que la participation d'une partie soit suspendue ou encore, dans les cas les plus graves de non-conformité aux exigences énoncées dans l'entente — et donc de bris du lien de confiance que l'entente a instauré entre les parties — recommande à la Conférence internationale que la partie soit exclue de l'entente.

14. Retrait de l'entente

Une partie peut se retirer de l'entente en donnant au Comité un préavis écrit d'un mois.

Dans les plus brefs délais après avoir informé le Comité de son intention de se retirer de l'entente, une partie prendra toutes mesures raisonnables pour informer les autres parties de son retrait. Elle devrait afficher cette information sur son propre site Web pendant qu'elle participe encore à l'entente et durant une période raisonnable après son retrait.

Une partie qui participe activement à une activité d'application transfrontière de la loi en vertu de la présente entente devrait s'efforcer de s'acquitter de ses obligations en lien avec cette activité avant de se retirer.

Indépendamment du retrait d'une partie, toute information reçue en vertu de la présente entente demeure assujettie au principe de confidentialité énoncé à l'article 6, aux principes de protection des données énoncés à l'article 7 et, s'il y a lieu, à l'annexe I de l'entente.

15. Entrée en vigueur

Le Comité acceptera les avis d'intention à partir de la date de la 37e Conférence, et l'entente entrera en vigueur dès qu'elle comptera au moins deux parties.

Les autorités deviendront des parties à l'entente lorsque le Comité leur aura signifié qu'elles sont acceptées.

Annexe I

1) En vertu de l'article 7 de la présente entente, les engagements prévus dans la présente annexe pourraient être appropriés pour permettre l'échange de données personnelles.

Toutefois, la présente annexe n'écarte pas les situations où les lois sur la protection des données et de la vie privée d'une partie exigent des mesures de sécurité supplémentaires dont doivent convenir les parties avant toute communication de renseignements personnels.

Les parties qui communiquent des données personnelles et qui se sont engagées à respecter la présente annexe doivent respecter les conditions suivantes dans la mesure où elles sont en mesure de le faire :

i. limiter la communication de données personnelles aux situations qui l'exigent absolument et, quoi qu'il en soit, communiquer uniquement des données personnelles pertinentes et non excessives compte tenu de la fin précise pour laquelle elles sont communiquées. En tout état de cause, les données personnelles ne doivent pas être communiquées à grande échelle ni d'une façon structurelle ou répétitive;

ii. veiller à ce que les données personnelles communiquées d'une partie à une autre ne soient pas utilisées par la suite à des fins incompatibles avec la fin pour laquelle elles ont été communiquées au départ;

iii. veiller à ce que les données personnelles communiquées d'une partie à une autre soient exactes et, au besoin, tenues à jour;

iv. n'adresser aucune une demande d'assistance à une autre partie au nom d'un plaignant sans le consentement explicite de ce dernier;

v. informer l'intéressé : a) de l'objet de la communication; b) de la possibilité que la partie ayant reçu les données personnelles les stocke ou les traite ultérieurement; c) de l'identité de la partie qui reçoit les données personnelles; d) des catégories de données visées; e) du droit de consulter et de corriger les données; f) de toute autre information nécessaire pour assurer un traitement équitable. Ce droit peut être limité au besoin pour protéger l'intéressé ou les droits et libertés d'autres personnes;

vi. veiller à ce que l'intéressé ait le droit de consulter ses données personnelles, de les corriger s'ils se révèlent inexacts et de s'opposer à la communication, au stockage ou à tout autre traitement des données personnelles qui le concernent. Ces droits peuvent être limités au besoin pour protéger l'intéressé ou les droits et libertés d'autres personnes; le droit de s'opposer peut être davantage limité si l'exercice de ce droit risque de porter préjudice à l'intégrité de la mesure d'application entre les participants, ou s'il compromet d'autres obligations juridiques nationales; si des données personnelles sensibles sont communiquées et font l'objet de tout autre traitement, veiller à ce que des mesures de sécurité supplémentaires soient mises en place, par exemple, exiger le consentement explicite de l'intéressé;

vii. sur réception de données personnelles, prendre toutes les mesures de sécurité techniques et organisationnelles adaptées aux risques que posent la communication, l'utilisation ultérieure ou le stockage de ces données. Les parties doivent également veiller à ce que toute organisation traitant des données en leur nom prenne des mesures de sécurité et que cette organisation n'utilise pas ou ne stocke pas de renseignements personnels sauf si la partie qui les a reçus lui en donne l'instruction;

viii. veiller à ce que toute entité à laquelle la partie ayant reçu les données les lui transfère par la suite soit également assujettie aux mesures de sécurité énoncées ci-dessus;

ix. si un tiers (par exemple un individu, un organisme judiciaire ou une autre autorité de la loi) demande à une partie de lui communiquer des données personnelles reçues d'une autre partie en vertu de la présente entente, veiller à ce que la partie ayant reçu la demande :

    a. s'oppose à la demande, ou s'efforce de la limiter le plus possible;
    b. informe sans délai la partie ayant fourni les données et cherche à obtenir son consentement à la communication de l'information en question;
    c. si la partie ayant fourni ces données refuse de consentir à la communication, l'informer si des lois nationales exigent la communication.

x. s'assurer que des mécanismes sont en place pour surveiller la conformité à ces mesures de sécurité et offrir à l'intéressé un recours approprié en cas de non-conformité.

2) Dans la présente annexe, « données personnelles sensibles » désigne :

a. des données qui concernent l'intimité du plaignant; ou

b. des renseignements susceptibles de donner lieu, en cas d'utilisation abusive :

    i. à une discrimination illicite ou arbitraire; ou
    ii. à de graves risques pour l'intéressé.

En particulier, les données personnelles qui peuvent révéler des aspects tels l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ainsi que les données relatives à la santé ou à la vie sexuelle sont considérées comme des données sensibles. Les lois nationales applicables peuvent prévoir d'autres catégories de données sensibles répondant aux conditions énoncées dans le paragraphe précédent.

---

[1] Afin d'éviter toute ambiguïté, l'expression « autorités » ou « autorités d'exécution des lois sur la protection des données et de la vie privée » englobe pour les besoins du présent document les autorités de protection des données personnelles.

[2] Afin d'éviter toute ambiguïté, l'expression « autorités » ou « autorités d'exécution des lois sur la protection des données et de la vie privée » englobe pour les besoins du présent document les autorités de protection des données personnelles.

ANNEXE B

Original disponible en anglais seulement.

PROTOCOLE D'ENTENTE ENTRE LA FEDERAL TRADE COMMISSION ET L'AUTORITÉ DE PROTECTION DES DONNÉES DES PAYS-BAS SUR L'ENTRAIDE DANS LE CADRE DE L'APPLICATION DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ

La Federal Trade Commission (FTC) des États-Unis et l'autorité de protection des données des Pays-Bas (College bescherming persoonsgegevens ou CBP) (collectivement, « les participants »),

RECONNAISSANT la nature de l'économie mondiale moderne, la circulation accrue des renseignements personnels d'un pays à l'autre, la complexité croissante et le caractère envahissant des technologies de l'information et le besoin connexe de renforcer la coopération en matière d'application transfrontalière des lois;

RECONNAISSANT que la recommandation de l'OCDE fixant un cadre pour la coopération dans l'application transfrontalière des lois sur la vie privée, le plan d'action du Global Privacy Enforcement Network, les résolutions du groupe de travail sur l'éducation au numérique de la Conférence internationale des commissaires à la protection des données et de la vie privée et le cadre de protection de la vie privée de l'APEC demandent l'élaboration de mécanismes de communication des renseignements transfrontaliers et des ententes de coopération en matière d'application des lois et qu'une telle coopération est essentielle pour garantir la conformité en matière de protection des renseignements personnels et des données, servant un intérêt important du public;

RECONNAISSANT que la Federal Trade Commission Act des États-Unis, 15 U.S.C. § 41 et suivants, modifiée par la U.S. SAFE WEB Act, autorise la FCC à divulguer de l'information aux organismes d'application de la loi d'autres pays dans les circonstances qui le justifient;

RECONNAISSANT que les paragraphes 1 et 2 de l'article 2:5 de la Loi sur le droit général administratif (de Algemene wet bestuursrecht) des Pays-Bas prévoient qu'un organisme public néerlandais peut fournir des renseignements confidentiels à des personnes ou des organisations participant à ses tâches si cette communication est nécessaire pour réaliser ses tâches de supervision et si la confidentialité des renseignements est maintenue;

RECONNAISSANT que la CBP est l'autorité désignée aux Pays-Bas pour ce qui est de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (laquelle a été ouverte à la signature le 28 janvier 1981) et est l'autorité de surveillance aux Pays-Bas aux fins de la Directive 95/46/CE 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;

RECONNAISSANT que les participants ont des attributions en matière de protection des renseignements personnels dans leurs pays respectifs;

RECONNAISSANT que les participants ont collaboré relativement à plusieurs initiatives internationales liées à la protection des renseignements personnels;

RECONNAISSANT que les participants ont coopéré dans le contexte de plusieurs réseaux internationaux, y compris le Global Privacy Enforcement Network et la Conférence internationale des commissaires à la protection des données et de la vie privée;

RECONNAISSANT que les participants ne pourraient offrir une aide à l'autre partie si une telle aide est interdite par leurs lois respectives en matière,

notamment en matière de protection des renseignements personnels, de sécurité des données ou de confidentialité, ou leurs politiques en matière d'application de la loi.

SONT PARVENUS À L'ENTENTE SUIVANTE

I. **Définitions**

Dans le cadre du présent protocole,

A. « lois applicables sur la protection des renseignements personnels » signifie les lois désignées à l'Annexe 1, laquelle peut être modifiée par accord mutuel des participants, y compris tout règlement d'application de ces lois, l'application desquelles a pour effet de protéger les renseignements personnels.

B. « Violation visée » signifie des pratiques qui violeraient les lois relatives à la vie privée applicables du pays d'un participant et qui sont identiques ou essentiellement similaires aux pratiques interdites par n'importe quelle disposition des lois relatives à la vie privée du pays de l'autre participant.

C. « Personne » signifie toute personne physique ou morale, y compris les sociétés par actions, les associations sans personnalité morale et les sociétés de personnes, établis, existants ou autorisés en vertu des lois des États-Unis, de ses États ou de ses Territoires, ou des lois des Pays-Bas.

D. « Demande » signifie une demande d'aide en vertu du présent protocole.

E. « Participant répondant » désigne le participant à qui on demande de l'aide en vertu du présent protocole, ou qui a fourni une telle aide.

F. « Participant demandant » désigne le participant qui demande de l'aide en vertu du présent protocole, ou qui a reçu une telle aide.

II. **Objectifs et portée**

A. Ce protocole d'entente énonce l'intention des participants, en présence de violations visées, de s'aider mutuellement et d'échanger de l'information dans le but d'enquêter et d'appliquer et de faire observer les lois. Les participants n'entendent pas créer des obligations contraignantes en droit national ou international avec les dispositions du présent protocole d'entente.

B. Les participants reconnaissent qu'il est dans leur intérêt commun de faire ce qui suit :

1. coopérer dans le cadre du contrôle de l'exécution des lois applicables sur la protection des renseignements personnels, y compris en communiquant des plaintes et d'autres informations pertinentes et en offrant une aide en matière d'enquête;

2. faciliter les activités de recherche et de sensibilisation concernant la protection des renseignements personnels;

3. favoriser l'échange mutuel de connaissances et d'expertise au moyen de programmes de formation et d'échanges de personnel;

4. promouvoir une compréhension réciproque améliorée des conditions et des théories économiques et juridiques relatives à l'exécution des lois applicables sur la protection des renseignements personnels;

5. s'informer mutuellement des nouveaux événements dans leur pays respectif qui ont des répercussions sur le présent protocole.

C. Pour servir ces intérêts communs et conformément à la section IV, les participants s'engagent à faire de leur mieux pour :

1. communiquer de l’information, y compris des plaintes et d’autres renseignements permettant d’identifier une personne – qui, selon un participant, pourraient se révéler utiles à une enquête ou à une poursuite relative à une violation visée par les lois applicables en matière de protection des renseignements personnels du pays de l’autre participant;

2. fournir de l’aide pour des enquêtes, lorsqu’approprié, y compris en obtenant des preuves en vertu des pouvoirs juridiques respectifs de chacun au nom de l’autre participant;

3. échanger et fournir toute autre information pertinente sur des questions visées par le présent protocole, comme des renseignements utiles pour la sensibilisation des consommateurs et des entreprises, des solutions en matière d’application qui relèvent du gouvernement ou de l’autoréglementation, des modifications aux textes législatifs pertinents et des problèmes relatifs à la dotation et à d’autres ressources, de l’expertise, des outils ou des techniques technologiques, de la recherche portant sur la sécurité des données et la vie privée et des renseignements sur les problèmes relatifs à la dotation et aux ressources;

4. évaluer les possibilités d’échange de personnel et de programmes de formation conjoints;

5. coordonner les mesures d’exécution de la loi concernant des violations visées transfrontalières en matière de protection des renseignements personnels qui sont prioritaires pour les deux participants;

6. participer à des téléconférences périodiques afin de discuter des efforts de coopération en cours et des possibilités de coopération éventuelles;

7. fournir toute autre aide appropriée qui favoriserait l’application de la loi contre les violations visées en matière de protection des renseignements personnels.

III. **Procédures d’entraide**

A. Chaque participant nommera une personne-ressource principale qui traitera les demandes d’aide et les autres communications entre les parties du protocole d’entente.

B. Si un participant demande de l’aide relativement à l’exécution des lois applicables sur la protection des renseignements personnels, les participants conviennent que :

1. les demandes d’aide contiennent suffisamment de renseignements pour que le participant répondant puisse déterminer si elles sont liées à une violation visée en matière de protection des renseignements personnels et s’il doit intervenir dans les circonstances appropriées. De tels renseignements peuvent inclure une description des faits sous-jacents à la demande et le type d’aide demandée ainsi qu’une indication de toute précaution spéciale à prendre pour donner suite à la demande;

2. les demandes d’aide précisent à quelle fin les renseignements demandés seront utilisés;

3. conformément à la section V (A), une demande d’aide certifie que, sous réserve de toute restriction légale pertinente applicable dans sa propre administration quant à sa capacité de le faire, le participant répondant traitera à titre confidentiel :

- chaque demande d’aide;
- l’existence de toute enquête liée à la demande;
- les documents associés à la demande;
- l’ensemble des informations et documents fournis en réponse à la demande, à moins d’entente contraire entre les participants.

4. Avant de demander de l’aide, les participants doivent réaliser une enquête préliminaire pour confirmer que la demande est conforme à la portée du présent protocole d’entente.

C. Les participants feront de leur mieux pour régler tout désaccord concernant la coopération dans le cadre du présent protocole d’entente par le truchement des personnes-ressources désignées à la section III (A). Si celles-ci sont incapables de régler le problème après un délai raisonnable, les responsables des participants en discuteront.

IV. **Limites liées à l’aide**

A. Le participant répondant peut exercer son pouvoir discrétionnaire et refuser de répondre à une demande d’aide, limiter sa coopération ou imposer des conditions connexes, particulièrement lorsque la demande n’est pas visée par le présent protocole d’entente ou, plus généralement, lorsque cela est contraire à ses lois ou à des intérêts et priorités importants.

B. Les participants reconnaissent qu’il ne leur est pas toujours possible de se venir en aide dans le cas d’une violation visée en matière de protection des renseignements personnels.

Par conséquent, comme il est mentionné à la section II, les participants entendent faire de leur mieux pour solliciter la coopération de l’autre et offrir la leur dans le cas des violations visées les plus graves, par exemple, celles qui portent ou sont susceptibles de porter atteinte à un nombre important de personnes, ou celles qui causent des préjudices importants, en particulier si ceux-ci touchent les deux pays.

C. Si le participant répondant n’est pas en mesure d’offrir une aide complète ou refuse de l’offrir, il doit en expliquer les raisons.

D. Les participants ont l’intention, dans la mesure où ils le peuvent et sont autorisés à le faire en vertu de leurs lois nationales, de communiquer des

renseignements confidentiels selon le présent protocole d'entente uniquement dans la mesure où cela est nécessaire pour atteindre les objectifs énoncés à la section II.

V. **Confidentialité, protection des renseignements personnels et limites quant à l'utilisation**

A. Dans la mesure du possible et sous réserve de toute restriction imposée par leurs lois nationales respectives, chaque participant s'engage à traiter de manière confidentielle les renseignements communiqués dans le cadre du présent protocole d'entente, ce qui s'applique également à l'existence d'une enquête à laquelle les renseignements se rapportent. Les participants s'engagent à traiter sous le sceau de la confidentialité les renseignements communiqués, l'existence d'une enquête à laquelle ces renseignements se rapportent et toute demande faite dans la cadre du présent protocole d'entente et, dans la mesure du possible, à ne pas communiquer ou utiliser ces renseignements à d'autres fins que celles pour lesquelles ils ont été communiqués à l'origine, sans avoir obtenu au préalable l'autorisation écrite du participant répondant.

B. Nonobstant le paragraphe A de la section V, il est entendu :

1. qu'un participant peut communiquer des renseignements fournis aux termes du présent protocole d'entente en réponse à une demande officielle d'un organe législatif de son pays ou à une ordonnance prise par un tribunal compétent dans une action intentée par le participant ou son gouvernement;

2. que les documents obtenus dans le cadre d'enquêtes ou de l'application des lois pénales soient utilisés aux fins d'enquête, de poursuite ou de prévention d'infractions aux lois pénales du pays de l'un ou de l'autre participant.

C. Chaque participant doit s'efforcer de protéger la sécurité de tout renseignement reçu dans le cadre du présent protocole d'entente et de respecter les mesures de protection convenues par les participants. En cas d'un accès non autorisé aux renseignements communiqués par un participant ou de

communication non autorisée de ceux-ci, les participants doivent prendre toutes les mesures raisonnables pour éviter qu'une telle situation ne se reproduise et doivent en informer l'autre participant.

D. Lorsqu'un participant reçoit d'une tierce partie une demande de communication de renseignements ou de documents confidentiels fournis par le participant répondant, le participant demandant doit rapidement informer le participant répondant et obtenir son consentement pour divulguer les renseignements ou – si le participant répondant ne consent pas à la divulgation des renseignements – tout faire en son pouvoir, dans les limites des lois applicables de son pays, pour s'opposer à toute demande de divulgation. Lorsque le participant ayant reçu une demande de divulgation par une tierce partie n'est pas en mesure d'obtenir le consentement de divulgation du participant répondant, si le participant demandant est néanmoins tenu compte selon ses lois de divulguer les renseignements, il doit en informer le participant répondant dès que possible de sa décision de divulguer les renseignements, ainsi que de la procédure générale concernant la divulgation de renseignements.

E. Les participants reconnaissent que l'information échangée dans le cadre d'enquêtes et de mesures d'exécution de la loi contient souvent des renseignements permettant d'identifier une personne. Si le participant demandant souhaite obtenir des renseignements confidentiels susceptibles de permettre d'identifier une personne, le participant reconnaît qu'il doit prendre des mesures supplémentaires appropriées pour transmettre ces renseignements de manière sécuritaire et pour les protéger. Les mesures suivantes et les mesures équivalentes raisonnables sont des exemples des mesures de protection pouvant être prises séparément ou de manière combinée, selon les circonstances :

1. transmettre les documents en format chiffré;

2. expédier les documents directement au participant en ayant recours à une entreprise de messagerie capable de faire le suivi de l'envoi;

3. envoyer les documents par télécopie plutôt que par courriel non chiffré;

4. conserver les documents dans des endroits sûrs dont l'accès est limité (p. ex., protection par mot de passe pour les fichiers électroniques, rangement sous clé pour les documents papier);

5. si les renseignements sont utilisés dans le cadre d'une procédure qui pourrait entraîner une divulgation publique, caviarder les renseignements permettant d'identifier une personne ou les mettre sous scellé.

VI. **Modifications des lois applicables**

En cas de modification importante des lois du pays d'un participant qui sont applicables au présent protocole, les participants entendent se consulter rapidement et, si possible, avant l'entrée en vigueur desdites modifications, pour déterminer s'il y a lieu de modifier le présent protocole d'entente.

VII. **Conservation des renseignements**

A. Si les participants souhaitent conserver les renseignements reçus de l'autre participant dans le cadre du présent protocole, les participants comprennent qu'ils ne pourront conserver les renseignements plus longtemps qu'il est raisonnablement nécessaire pour réaliser l'objectif à l'origine de la communication ou plus longtemps que ne l'autorisent les lois du pays du participant demandant.

B. Les participants reconnaissent que, pour réaliser l'objectif à l'origine de la communication, ils doivent normalement conserver les documents communiqués jusqu'à la fin de l'enquête pour laquelle les documents ont été demandés et de toute procédure connexe, ce qui comprend la date où un jugement devient définitif.

C. Les participants doivent faire de leur mieux pour renvoyer tous les documents qui ne sont plus requis si le participant répondant a demandé par écrit le renvoi des documents au moment de la communication. Si le participant répondant ne demande pas le renvoi des documents, le participant demandant en disposera à

l’aide des méthodes définies par le participant répondant ou, si ce dernier n’a pas précisé les méthodes, grâce à des méthodes sécuritaires, le plus rapidement possible une fois que les documents ne sont plus nécessaires.

VIII. **Coûts**

Sauf si les participants en décident autrement, le participant répondant engage tous les coûts nécessaires pour répondre à la demande. Lorsque les coûts sont importants, le participant répondant peut demander au participant demandant de les payer en tant que condition au traitement de la demande. Dans une telle situation, les participants procéderont à des consultations sur la question à la demande d’un des participants.

IX. **Durée de la coopération**

A. Les participants veulent pouvoir faire appel à la coopération aux termes du présent protocole à partir de la date de la signature du protocole.

B. L’aide prévue au titre du protocole d’entente s’applique aux violations visées qui se sont produites avant et après la signature du protocole.

C. Les participants doivent s’efforcer de fournir un préavis de 30 jours aux autres participants lorsqu’ils comptent se retirer du présent protocole d’entente. Cependant, avant de donner un tel avis, chaque participant fera de son mieux pour consulter l’autre participant.

D. Après résiliation du présent protocole, les participants continueront d'assurer la confidentialité des renseignements communiqués par l'autre participant dans le cadre du présent protocole conformément à la section V, et renverront ou détruiront ces renseignements conformément aux dispositions de la section VII.

X. **Portée juridique**

Aucune disposition du présent protocole d'entente ne vise à :

A. créer des obligations contraignantes en droit international ou national ou avoir une incidence sur des obligations existantes;

B. empêcher un participant de demander l'aide à l'autre participant ou de lui en fournir dans le cadre d'autres ententes, arrangements ou pratiques;

C. avoir une incidence sur le droit d'un participant à chercher à obtenir des renseignements de façon légale d'une personne située dans le pays de l'autre participant ni à empêcher une telle personne de fournir volontairement à un participant des renseignements obtenus légalement;

D. créer des obligations contraires aux lois nationales ou aux ordonnances d'un tribunal du pays de l'un ou de l'autre participant ou aux instruments juridiques internationaux applicables;

E. créer des attentes de coopération qui dépassent la compétence des participants.

Signé à Washington, D.C.

Le 6 mars 2015, en double exemplaire.

_____	_____
Edith Ramirez	Jacob Kohnstamm
Présidente	Président
Federal Trade Commission des États-Unis	Autorité de protection des données des Pays-Bas

PROTOCOLE D'ENTENTE

ENTRE

LA COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA ET L'INFORMATION COMMISSONER DU ROYAUME-UNI

SUR

L'ENTRAIDE DANS LE CADRE DE L'APPLICATION DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ

La commissaire à la protection de la vie privée du Canada (la commissaire) et le Information Commissioner du Royaume-Uni (le « IC ») (« les participants ») :

RECONNAISSANT la nature de l'économie mondiale moderne, la circulation et la communication accrues des renseignements personnels d'un pays à l'autre, la complexité et le caractère envahissant des technologies de l'information et le besoin connexe de renforcer la coopération en matière d'application transfrontalière des lois;

RECONNAISSANT que la Recommandation de l'OCDE fixant un cadre pour la coopération dans l'application transfrontalière des lois sur la vie privée et le cadre de protection de la vie privée de l'APEC exhortent les pays et les économies membres à élaborer des mécanismes de communication des renseignements transfrontaliers et des ententes de coopération bilatérales ou multilatérales en matière d'application des lois;

RECONNAISSANT que l'article 23.1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5, autorise la commissaire à communiquer des renseignements à des autorités responsables de la protection des renseignements personnels dans le secteur privé d'autres pays;

RECONNAISSANT que le IC est l'autorité désignée au Royaume-Uni pour les fins de l'article 13 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ouverte à la signature à Strasbourg, le 28 janvier 1981, et est l'autorité de contrôle au Royaume-Uni pour les fins de la Directive 95/46/CE 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;

RECONNAISSANT que les participants ont chacun des attributions semblables en matière de protection des renseignements personnels dans le secteur privé dans leurs pays respectifs; et
RECONNAISSANT que rien dans ce protocole n'exige aux participants à offrir quelconque assistance en matière d'application des lois de protection des renseignements personnels dans le secteur privé si une telle assistance serait interdit par leur lois domestiques ou politiques d'application respectives.

SE SONT ENTENDUS SUR CE QUI SUIT :

I. **Définitions**

Dans le cadre du présent protocole,

A. « lois applicables sur la protection des renseignements personnels » Lois et règlements du pays participant dont l'application permet de protéger les renseignements personnels. Dans le cas de la commissaire, la « loi applicable sur la protection des renseignements personnels » est la partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5 (LPRPDE) et, dans le cas du IC, la Data Protection Act 1998; ainsi que toute modification apportée aux lois applicables sur la protection des renseignements personnels des participants et d'autres lois et règlements que les participants peuvent décider conjointement, au fil du temps et par écrit, d'inclure dans la catégorie des lois applicables sur la protection des renseignements personnels du présent protocole d'entente.
B. « personne » Personne physique ou morale, y compris les sociétés par actions, les associations sans personnalité morale et les sociétés de personnes.
C. « demande » Demande d'aide aux termes du présent protocole d'entente.
D. « participant répondant » Participant à qui une aide est demandée aux termes du présent protocole d'entente ou qui fournit une telle aide.
E. « participant demandant » Participant qui demande l'aide aux termes du présent protocole d'entente ou qui la reçoit.
F. « contravention visée en matière de protection des renseignements personnels » Tout comportement qui contreviendrait aux lois applicables sur la protection des renseignements personnels du pays de l'un des participants qui est identique ou essentiellement semblable à un comportement qui constitue une contravention aux lois applicables sur la protection des renseignements personnels du pays de l'autre participant.

II. **Objectifs et portée**

A. Les participants reconnaissent qu'il est dans leur intérêt commun de faire ce qui suit :

1. coopérer dans le cadre du contrôle de l'application des lois applicables sur la protection des renseignements personnels, y compris en communiquant des renseignements pertinents et dans le cadre de l'instruction des plaintes dans lesquelles ils ont un intérêt mutuel;
2. faciliter les activités de recherche et de sensibilisation concernant la protection des renseignements personnels;
3. promouvoir une meilleure compréhension des conditions et des théories économiques et juridiques relatives à l'application des lois applicables sur la protection des renseignements personnels; et
4. se tenir informés des nouveaux événements dans leurs pays respectifs qui ont des répercussions sur le présent protocole d'entente.

B. Pour servir ces intérêts communs et conformément à la section IV, les participants feront de leur mieux pour réaliser ce qui suit :

1. communiquer des renseignements qui, selon eux, pourraient être utiles à une enquête ou à une poursuite en cours ou éventuelle relative à une contravention visée en matière de protection des renseignements personnels par les lois applicables sur la protection des renseignements personnels du pays de l'autre participant;
2. échanger et fournir des renseignements liés à des affaires visées par le protocole d'entente, comme des renseignements utiles pour la sensibilisation des consommateurs et des entreprises, des solutions en matière d'application de la loi issues du gouvernement ou de l'autoréglementation, des modifications aux textes législatifs connexes et des problèmes relatifs à la dotation et aux ressources; et
3. organiser des échanges de personnel à court terme et, éventuellement, à long terme, pour favoriser et renforcer la collaboration des participants dans le cadre d'activités d'application.

C. Pour servir ces intérêts communs et conformément à la section IV, les participants reconnaissent que l'élément suivant est un enjeu prioritaire exigeant une éventuelle coopération :

1. éventuelle enquête ou mesure d'application parallèle ou conjointe des participants.

III. **Procédures d'entraide**

A. Chaque participant nommera une personne-ressource principale qui traitera les demandes d'aide et les autres communications entre les parties du protocole d'entente.

B. Lorsqu'ils demandent de l'aide relativement à des procédures ou à des enquêtes ou pour d'autres motifs touchant l'application transfrontalière des lois applicables sur la protection des renseignements personnels, les participants s'assureront que :
1. les demandes d'aide contiennent suffisamment de renseignements pour que le participant répondant puisse déterminer si elles sont liées à une contravention visées en matière de protection des renseignements personnels et s'il doit intervenir dans les circonstances appropriées. De tels renseignements peuvent inclure une description des faits sous-jacents à la demande et le type d'aide demandée ainsi qu'une indication de toute précaution spéciale à prendre pour donner suite à la demande;
2. les demandes d'aide précisent à quelle fin les renseignements demandés seront utilisés; et
3. avant de demander de l'aide, les participants réalisent une enquête préliminaire pour confirmer que la demande est conforme à la portée du présent protocole d'entente et ne constitue pas un fardeau excessif pour le participant répondant.

C. Les participants prévoient communiquer et collaborer entre eux, s'il y a lieu, quand cela peut contribuer aux enquêtes en cours.

D. Les participants informeront les autres sans délai s'ils constatent que certains renseignements communiqués dans le cadre du présent protocole d'entente sont inexacts, incomplets ou périmés.

E. Sous réserve de la section IV, les participants peuvent, si cela est approprié et conforme à leurs lois applicables sur la protection des renseignements personnels, se renvoyer des plaintes ou s'informer de possibles contraventions visées en matière de protection des renseignements personnels par les lois applicables sur la protection des renseignements personnels du pays de l'autre participant.

F. Les participants feront de leur mieux pour régler tout désaccord concernant la coopération dans le cadre du présent protocole d'entente par le truchement des personnes-ressources désignées à la section III (A). Si celles-ci sont incapables de régler le problème après un délai raisonnable, les responsables des participants en discuteront.

IV. Limites liées à l'aide et à l'utilisation

A. Le participant répondant peut exercer son pouvoir discrétionnaire et refuser de répondre à une demande d'aide, limiter sa coopération ou imposer des conditions connexes, particulièrement lorsque la demande n'est pas visée par le présent protocole d'entente ou, plus généralement, lorsque cela est contraire à ses lois ou à des intérêts et priorités importants. Le participant demandant peut demander les motifs pour lesquels le participant répondant a refusé de l'aider ou a limité son aide.

B. Les participants communiqueront uniquement des renseignements personnels dans le cadre du présent protocole d'entente dans la mesure où cela est nécessaire à la réalisation des objectifs du protocole. En outre, quand cela est possible, ils feront de leur mieux pour obtenir au préalable le consentement des personnes concernées.

C. Pour plus de certitude, la commissaire ne communiquera pas de renseignements confidentiels sauf :

   a. aux fins établies à la section II (B.1);
   b. s'il est nécessaire de le faire pour présenter une demande d'aide à l'autre participant concernant les renseignements pouvant être utiles dans le cadre d'une enquête ou d'une vérification en cours ou éventuelle aux termes de la partie 1 de la LPRPDE. Les participants n'utiliseront pas les renseignements fournis par le participant répondant à d'autres fins que celles auxquelles ils ont été communiqués.

V. Confidentialité

A. Les renseignements communiqués dans le cadre du présent protocole d'entente seront traités de manière confidentielle et ne seront pas autrement communiqués sans le consentement de l'autre participant.

B. Chaque participant fera de son mieux pour protéger les renseignements fournis aux termes du présent protocole d'entente et respecter toutes les mesures de protection établies par les participants. En cas de consultation ou de communication non autorisée des renseignements, les participants mettront en place toutes les mesures nécessaires pour empêcher que cela se reproduise et informeront rapidement l'autre participant de la situation.

C. Les participants feront tout en leur pouvoir, dans les limites des lois de leur pays, pour s'opposer à toute demande par une tierce partie de communication de renseignements ou de documents confidentiels fournis par le participant répondant, sauf si celui-ci consent à la communication. Les participants qui recevront une telle demande en informeront rapidement le participant qui a fourni les renseignements confidentiels.

VI. Modification des lois applicables sur la protection des renseignements personnels

En cas de modification des lois applicables sur la protection des renseignements personnels du pays d'un participant qui sont visées par le présent protocole d'entente, les participants feront de leur mieux pour se consulter rapidement et, si possible, avant l'entrée en vigueur desdites modifications, pour déterminer s'il faut modifier le présent protocole d'entente.

VII. Conservation des renseignements

Les renseignements reçus dans le cadre du présent protocole d'entente ne seront pas conservés plus longtemps que nécessaire pour la réalisation de l'objectif à l'origine de la communication ou plus longtemps que l'exigent les lois du pays du participant demandant. Les participants feront de leur mieux pour renvoyer tous les renseignements qui ne sont plus requis si le participant

répondant a demandé par écrit le renvoi des renseignements au moment de la communication. Si le participant répondant ne demande pas le renvoi des renseignements, le participant demandant en disposera à l'aide des méthodes définies par le participant répondant ou, si ce dernier n'a pas précisé les méthodes, grâce à des méthodes sécuritaires, le plus rapidement possible une fois que les renseignements ne seront plus nécessaires.

VIII. **Coûts**

Sauf si les participants en décident autrement, le participant répondant engagera tous les coûts nécessaires pour répondre à la demande. Lorsque les coûts liés à la communication ou l'obtention de renseignements dans le cadre du présent protocole d'entente sont importants, le participant répondant peut demander au participant demandant de les payer en tant que condition au traitement de la demande. Dans une telle situation, les participants procéderont à des consultations sur la question à la demande d'un des participants.

IX. **Durée de la coopération**

A. Le présent protocole d'entente entre en vigueur à la date de signature.
B. L'aide prévue dans le présent protocole d'entente sera fournie relativement à des contraventions visées qui se sont produites avant et après la signature du protocole d'entente.
C. Les participants peuvent mettre fin au présent protocole d'entente en envoyant un avis écrit de 30 jours à l'autre participant. Cependant, avant de donner un tel avis, chaque participant fera de son mieux pour consulter l'autre participant.
D. Ce protocole peut être modifié, ou complété, tel que convenu par les participants par écrit.
E. Lorsque le protocole d'entente ne sera plus en vigueur, les participants continueront à assurer la confidentialité des renseignements communiqués par l'autre participant dans le cadre du présent protocole d'entente conformément à la section V, et renverront ou détruiront les renseignements fournis par l'autre participant dans le cadre du présent protocole d'entente conformément aux dispositions de la section VII.

X. **Conséquences juridiques**

Aucune disposition du présent protocole d'entente ne vise :

A. à créer des obligations contraignantes ou à influer sur des obligations existantes aux termes du droit international, ou à créer des obligations aux termes des lois des pays des participants;
B. à empêcher un participant de demander l'aide de l'autre participant ou de lui en fournir dans le cadre d'autres ententes, traités, arrangements ou pratiques;
C. à avoir un impact sur le droit d'un participant à tenter d'obtenir des renseignements de façon légale d'une personne située dans le pays de l'autre participant ni à empêcher une telle personne de fournir volontairement des renseignements obtenus légalement à un participant; ou
D. à créer des obligations ou des attentes de coopération qui dépassent la compétence des participants.

Signé le 14 mai 2012 à Montréal, Québec, Canada en deux exemplaires, en français et en anglais, toutes les versions étant également valides.

La version originale est signée par

Christopher Graham
Information Commissioner du Royaume-Uni

Date : 2012-05-14
À : Montréal, Québec, Canada

La version originale est signée par

Jennifer Stoddart
Commissaire à la protection de la vie privée du Canada

Date : 2012-05-14
À : Montréal, Québec, Canada

MEMORANDO DE ENTENDIMIENTO ENTRE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA Y LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DEL REINO DE ESPAÑA

REUNIDOS

De una parte, Mar España Martí, Directora de la Agencia Española de Protección de Datos, cargo para el que fue nombrada por Real Decreto 715/2015 de 24 de julio, en nombre y representación de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (en adelante, la "AEPD"), y

De otra parte, Andrés Barreto González, Superintendente de Industria y Comercio, cargo para el que fue nombrado mediante el decreto 1806 del 20 de septiembre de 2018[1], en nombre y representación de la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA (en adelante, la "SIC").

Reconociendo la necesidad garantizar el debido tratamiento de los datos personales y los riesgos en la circulación e intercambio de información personal transfronteriza, la creciente complejidad de las tecnologías de la información y la consiguiente necesidad de incrementar la cooperación internacional;

Reconociendo la importancia de la protección de los datos personales para promover un desarrollo nacional sólido y la confianza en los flujos internacionales de información;

Deseando fomentar una cooperación más estrecha entre ambas partes en el campo de la protección de datos a fin de promover la creación, protección y aplicación de la normativa de protección de datos;

DECLARAN

I. Que la AEPD es una autoridad administrativa independiente, con personalidad jurídica propia y plena capacidad pública y privada, que ostenta las competencias atribuidas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento General de Protección de Datos o RGPD), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Corresponde a la AEPD ejercer las funciones establecidas en el artículo 57 del RGPD, entre las que se encuentran controlar la aplicación del propio Reglamento y hacerlo aplicar; promover la sensibilización del público y su comprensión de los riesgos; normas, garantías y derechos en relación con el tratamiento de los mismos; promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben, así como cualquier otra función relacionada con la protección de los datos personales.

II.- Que, de conformidad con lo dispuesto en el artículo 71 de la Ley 1151 de 2007 y el Decreto 4886 de 2011, la SIC es un organismo de carácter técnico con personería jurídica, que goza de

[1] Cfr. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201806%20DEL%2020%20DE%20SEPTIEMBRE%20DE%202018.pdf

autonomía administrativa, financiera, presupuestal y cuenta con patrimonio propio, denominada entidad estatal para efectos contractuales de acuerdo con lo señalado ene I literal b) del numeral 1 del artículo 2 de la Ley 80 de 1993.

III.- Que la SIC funge como Autoridad Nacional en materia de Protección de Datos Personales, y en sus acciones vela por garantizar que, en la recolección, el uso, la circulación y el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la Constitución y en la Ley y además exige el respeto del "habeas data" previsto en el artículo 15 de la Constitución Política Nacional.

De la misma manera, el artículo 3 del Decreto 4886 de 2011 establece que, dentro de las funciones del Despacho del Superintendente de Industria y Comercio, está la de asesorar al Gobierno Nacional y participar en la formulación de las políticas relacionadas con la promoción a la protección de datos personales. A su vez, de acuerdo con el artículo 16 del Decreto 4886 de 2011, dentro de las funciones del Despacho del Superintendente Delegado para la Protección de Datos Personales, está la de velar por el cumplimiento de las normas y leyes vigentes en materia de protección de datos personales, y proponer nuevas disposiciones.

IV.- Que la Superintendencia de Industria y Comercio aprobó o acordó la suscripción del presente Memorando.

V.- Que la AEPD y la SIC forman parte, en condición de Miembros, de la Red Iberoamericana de Protección de Datos (en adelante, RIPD), foro creado como respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los Países Iberoamericanos, a través del diálogo y la colaboración en materia de protección de datos de carácter personal.

VI. Que uno de los logros más destacados en el ámbito de la cooperación promovida en el marco de la RIPD ha sido la aprobación de los "Estándares en materia de Protección de Datos para los Estados Iberoamericanos" (en adelante, "los Estándares"), fruto de un importante esfuerzo por dotar a la Comunidad Iberoamericana de un marco común que sirva de referencia a la hora de aprobar las respectivas normativas de protección de datos, o para adaptar las vigentes.

VII. Que, entre los objetivos prioritarios de los Estándares, está el de "Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia". En particular, su numeral 45 establece que: "Los Estados Iberoamericanos podrán adoptar mecanismos de cooperación internacional que faciliten la aplicación de las legislaciones nacionales aplicables en la materia, los cuales podrán comprender, de manera enunciativa más no limitativa: a) El establecimiento de mecanismos que permitan reforzar la asistencia y cooperación internacional en la aplicación de las respectivas legislaciones nacionales en la materia; b) La asistencia entre las autoridades de control a través de la notificación y remisión de reclamaciones, la asistencia en investigaciones y el intercambio de Información, y c) La adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en

materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países".

VIII. Que ambas instituciones, conscientes de la importancia de proteger de manera adecuada el derecho fundamental a la protección de los datos personales, quieren dejar constancia de su interés en desarrollar una estrecha colaboración que sirva de marco general para la realización de actividades conjuntas de cooperación, formación, desarrollo de programas y proyectos específicos en las áreas que ambas partes determinen de mutuo acuerdo.

IX. Que, en consideración a la voluntad de los firmantes de colaborar en las acciones descritas a continuación, la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS y la SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO de Colombia, acuerdan suscribir el presente MEMORANDO DE ENTENDIMIENTO (en adelante, el Memorando), que se regirá por las siguientes

CLÁUSULAS

PRIMERA.- OBJETO.

El presente Memorando tiene por objeto establecer las bases de la colaboración institucional entre sus firmantes, con la finalidad de promover la difusión del derecho a la protección de datos de carácter personal; velar por la cooperación conjunta en materia de protección de datos personales y brindar un marco para el intercambio de conocimientos técnicos y mejores prácticas, que permitan fortalecer las capacidades técnicas de ambas partes relacionadas con la aplicación de la ley en materia de protección de datos personales.

SEGUNDA. ALCANCE DE LA COOPERACIÓN.

Para el cumplimiento de los objetivos del presente Memorando, los firmantes asumen los siguientes compromisos generales:

a. Impulsar mecanismos específicos de cooperación técnica que permitan, de manera enunciativa más no limitativa, intercambiar conocimientos y experiencias, e identificar las mejores prácticas en materia de protección de datos personales;

b. Fomentar y contribuir a la realización de investigaciones, estudios, análisis e informes en materia de protección de datos personales;

c. Colaborar en la elaboración y difusión de guías, herramientas y otros materiales orientados a facilitar el cumplimiento de la legislación de protección de datos por parte de los sujetos obligados;

d. Favorecer los mecanismos de asistencia jurídica y cooperación técnica para la aplicación efectiva de sus legislaciones nacionales y, en especial, en el marco de las potestades de investigación conferidas por sus respectivas legislaciones nacionales;

e. Impulsar el desarrollo de iniciativas conjuntas, prioritariamente en el marco de programas y proyectos internacionales, que contribuyan a reforzar las respectivas competencias en sectores y ámbitos con un importante impacto social, ambiental e institucional, en especial en materia de igualdad de género, menores e innovación y emprendimiento, y

f. En general, impulsar cualquier actuación que consideren necesario para el más adecuado cumplimiento de sus respectivas competencias, dentro de los límites de sus legislaciones nacionales y, en su caso, del derecho internacional que pudiera resultar aplicable en la materia.

TERCERA. COMPROMISO CON LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS (RIPD).

1. Los firmantes reafirman su compromiso con la Red Iberoamericana de Protección de Datos, destacando el papel relevante que dicha Red desempeña actualmente en la Región y coincidiendo en la necesidad de impulsar, en el estado actual de la misma, nuevos espacios e instrumentos de cooperación entre sus miembros, específicamente, a partir de la aprobación de los Estándares que se constituyen en un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes, así como al desarrollo de mecanismos de cooperación internacional entre las autoridades de control.

2. En este sentido, la SIC, que desempeña en la actualidad la Presidencia de la RIPD, y la AEPD, en su condición de Secretaría Permanente de la RIPD, advierten sobre la necesidad imperiosa de impulsar mecanismos y acciones de colaboración concretas para que los Estándares impacten en las iniciativas y proyectos en la materia de la región y, en su caso, de otras regiones y organismos internacionales, con la finalidad de lograr su trascendencia más allá de su aprobación.

3. En especial, de conformidad con el Plan Estratégico de la RIPD 2021-2025, aprobado en la sesión cerrada (online) del XVIII Encuentro Iberoamericano de Protección de Datos, celebrada el 4 de diciembre de 2020, las instituciones firmantes trabajarán, en el marco de la RIPD, en favor de la creación de un nuevo espacio que promueva la cooperación efectiva entre las Autoridades Iberoamericanas de Protección de Datos, y en particular en el impulso de las siguientes acciones:

- Potenciar el papel del Grupo Permanente de Autoridades Nacionales de Protección de Datos (GPAN) creado en el marco del XVII Encuentro Iberoamericano de Protección de Datos como foro específico para que las Autoridades Iberoamericanas puedan establecer criterios o directrices comunes en ámbitos de especial impacto para la privacidad, especialmente los relacionados con el desarrollo de las nuevas tecnologías de tratamiento masivo de los datos personales (Big Data, Internet de las Cosas, Inteligencia Artificial ....). En tal sentido, se contemplará el establecimiento de un mecanismo para que esos criterios o directrices queden plasmados, por ejemplo, mediante la adopción de resoluciones específicas o la implementación de grupos de trabajo que puedan llevar a cabo el seguimiento de los temas.

- Identificar casos reales que afecten a ciudadanos de varios países de la red con miras a que todas las autoridades de la red o la mayoría de ellas actúen de oficio y desde sus países frente a dichas situaciones y dentro del marco de sus competencias legales.

- Difundir entre los países integrantes de la Red las resoluciones sobre casos relacionados al tratamiento ilícito de datos personales por parte de empresas transnacionales con la finalidad de promover experiencias que sirvan como antecedentes en la materia.

- Impulsar fórmulas e instrumentos de cooperación efectiva (enforcement) entre las Autoridades, especialmente de asistencia jurídica mutua en el ámbito de la investigación y evaluación tecnológica, así como en otros ámbitos (intercambio de información de guías y herramientas, planificación estratégica, etc.).

- Promover el desarrollo de unidades o divisiones de innovación para que las Autoridades puedan estar atentas a las últimas novedades y tendencias en el ámbito tecnológico.

- Fomentar el intercambio de buenas prácticas y la adopción de iniciativas concretas, incluso a título experimental, de experiencias de cooperación efectiva entre las Autoridades Iberoamericanas de Control.

- Apoyar la generación de estudios e investigaciones, y, en general, de cuantas iniciativas tengan por objeto un mejor conocimiento del estado de situación de la protección de datos en Iberoamérica.

- Desarrollar programas de capacitación y formación online del personal directivo y empleados de las Autoridades, tanto para reforzar la cultura de la protección de datos en estas organizaciones públicas, como para promover una formación especializada en la materia, necesaria en ámbitos tecnológicos cada vez más complejos y exigentes.

- Fomentar programas de estancias temporales entre empleados y directivos de las Autoridades Iberoamericanas de Protección de Datos, para mejorar el conocimiento y el intercambio de experiencias entre las distintas culturas administrativas que integran la RIPD.

CUARTA. MEMORANDOS ESPECÍFICOS DE COLABORACIÓN.

1. El desarrollo de las actividades conjuntas se realizará mediante la celebración y ejecución de Memorandos Específicos de Colaboración que se integrarán como anexos al presente instrumento, donde se deberá precisar lo siguiente:

a) Objetivos y actividades a realizar o ejecutar;
b) Compromisos asumidos por cada una de las partes;
c) En su caso, presupuesto disponible y fuentes de financiamiento;
d) Personal designado, instalaciones y equipo a utilizar;
e) Calendario de trabajo y mecanismos de evaluación, y

f) En general, todo aquello que resulte necesario para determinar con exactitud los fines y alcances aprobados por los firmantes en cada uno de los memorandos.

2. Cada uno de los Memorandos específicos serán sometidos previamente a su aprobación a informe jurídico de los respectivos firmantes, a efectos de determinar si contienen compromisos específicos de hacer o de financiar.

QUINTA.- FINANCIAMIENTO.

1. El presente Memorando no conlleva gasto alguno. Las aportaciones financieras para la realización de las actividades de cooperación a implementarse en el marco del mismo, serán acordadas por los firmantes en cada uno de los Memorandos Específicos de Colaboración.

2. La firma de cualquier Memorando Específico de Colaboración estará supeditada a su viabilidad y a la disponibilidad presupuestaria de cada uno de los firmantes.

3. Los firmantes promoverán la búsqueda de fuentes de financiación complementaria para los fines del presente Memorando.

SEXTA.- AUTONOMÍA.

Las acciones encaminadas a lograr el cumplimiento del presente Memorando se harán bajo el absoluto respeto y sin perjuicio de la autonomía o naturaleza propia de cada uno de los firmantes, así como de las determinaciones que corresponda a cada uno de ellos.

SÉPTIMA.- PROPIEDAD INTELECTUAL.

1. Los firmantes preservarán la titularidad de los derechos de aquellas obras que sean producto de su trabajo respectivo, de conformidad con lo que establecen las leyes en materia de propiedad intelectual de las respectivas legislaciones.

2. En el caso de aquellas obras, materiales y trabajos que sean producto de un trabajo conjunto, los firmantes convienen compartir la titularidad de los derechos, de conformidad con lo que establezcan sus respectivas leyes en materia de propiedad intelectual.

3. En el supuesto de que alguno de los firmantes desee utilizar en una publicación propia información o resultados de una investigación proporcionada por el otro firmante, deberá solicitar previamente autorización escrita a ésta, y ajustarse a las disposiciones legales que correspondan en la materia.

4. Una parte no podrá utilizar la marca, logotipo o emblema de la otra en publicaciones ni programas sin el previo consentimiento por escrito de ésta.

OCTAVA. MECANISMO DE SEGUIMIENTO.

1. Para el adecuado desarrollo de las actividades que se generarán con motivo de la ejecución del presente Memorando, cada uno de los firmantes designarán como contacto a un representante, quien podrá ser sustituido en cualquier momento, previa notificación al otro firmante.

2. Los representantes designados como puntos de contacto tendrán las siguientes funciones:

a) Promover la celebración de Memorandos específicos;
b) Determinar y apoyar las acciones a ejecutar con el fin de dar cumplimiento al objeto del presente Memorando y de los Memorandos Específicos de Colaboración;
c) Coordinar la realización de actividades señaladas en el presente Memorando;
d) Dar seguimiento a las actividades que se desprendan del presente Memorando e informar periódicamente a los firmantes sobre los resultados obtenidos;
e) Las demás que acuerden los firmantes.

3. Los criterios para la coordinación, seguimiento y ejecución del objeto de este Memorando que se consideren necesario instrumentar, serán determinados por los representantes que al efecto se designen.

4. La representación estará conformada por las siguientes personas:

POR LA "SIC"	POR LA "AEPD"
Nelson Remolina Angarita. Superintendente-Delegado para la Protección de Datos Personales. Domicilio: Carrera 13 No. 27-00, Bogotá D.C., Colombia Teléfono: +571 5870000	Jesús Rubí Navarrete. Coordinador de la Unidad de Apoyo y Relaciones Institucionales. Domicilio: Calle Jorge Juán, 6. 28001. Madrid. Teléfono: +34913996921

NOVENA. RELACIÓN LABORAL.

Los firmantes convienen que el personal asignado por cada uno para la realización de las actividades previstas en el presente Memorando, continuará bajo la dirección y dependencia de la Institución a la que pertenezca, por lo que no se crearán relaciones de carácter laboral con la otra, a la que no se considerará patrón sustituto o solidario.

DÉCIMA. ENTRADA Y SALIDA DE PERSONAL.

Los firmantes se apoyarán en sus autoridades correspondientes, a efecto de que se otorguen todas las facilidades necesarias para la entrada, estancia y salida de los participantes que en forma oficial intervengan en las actividades de cooperación que se deriven del presente Memorando. Estos participantes se someterán a las disposiciones migratorias, fiscales, aduaneras, sanitarias y de seguridad nacional vigentes en el país receptor y no podrán dedicarse a ninguna actividad ajena a sus funciones sin la previa autorización de las autoridades competentes en esta materia. Los participantes dejarán el país receptor, de conformidad con las leyes y disposiciones del mismo.

UNDÉCIMA. TRANSPARENCIA DE LA INFORMACIÓN.

Los firmantes llevarán a cabo las acciones necesarias para poner a disposición de la ciudadanía la información relacionada con el trabajo realizado con motivo de la ejecución del presente Memorando, así como la relativa al ejercicio de recursos públicos, siempre que dicha actuación no vulnere el deber de sigilo y secreto profesional exigible, así como la legislación nacional aplicable a cada uno de los firmantes en materia de protección de datos personales.

DUODÉCIMA. SOLUCION DE CONTROVERSIAS.

1. Cualquier diferencia derivada de la interpretación o aplicación del presente Memorando, será resuelto por los firmantes de común acuerdo.

2. El presente Memorando no es jurídicamente vinculante ni está sometido al Derecho internacional.

DECIMOTERCERA. DISPOSICIONES FINALES.

1. El presente Memorando será de aplicación a partir de la fecha de su firma y continuará siéndolo por un período de cuatro años contado a partir de esa fecha, pudiendo renovarse, por igual periodo, mediante el acuerdo expreso y escrito de los firmantes.

2. El presente Memorando podrá ser modificado por mutuo consentimiento de los firmantes, formalizado por medio de comunicaciones escritas, en las que se especifique la fecha de inicio de aplicación de dichas modificaciones.

3. Cualquiera de los firmantes podrá dar por terminado el presente Memorando, siempre que lo notifique por escrito a la otra parte, con un mínimo de tres (3) meses de anticipación a la fecha de terminación. La terminación anticipada del presente Memorando no afectará la conclusión de los proyectos iniciados en el marco del mismo.

Firmado el día ___ del año dos mil veintiuno, en dos ejemplares originales en idioma español, siendo ambos textos igualmente auténticos.

POR LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE LA REPÚBLICA DE COLOMBIA	POR LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DEL REINO DE ESPAÑA
	ESPAÑA MARTI MAR - DNI 05259618R Firmado digitalmente por ESPAÑA MARTI MAR - DNI 05259618R Fecha: 2021.03.25 10:14:30 +01'00'
Fdo: D. Andrés Barreto González Superintendente de Industria y Comercio 14 Abril 2021.	Fdo: Dª. Mar España Martí Directora

ANNEXE C

Lettre aux opérateurs du site diffusant des images de caméras Web

Le 21 novembre 2014

Mesdames,
Messieurs,

Nous vous écrivons en tant qu'autorités chargées de l'application des lois sur la protection des renseignements personnels pour faire le point sur un important problème qui a été porté à notre attention.

Nous avons de sérieuses préoccupations concernant votre site Web et les séquences vidéo que vous diffusez en direct à partir de caméras Web dont les propriétaires ont conservé le nom d'utilisateur et le mot de passe par défaut fournis par le fabricant. Ces caméras se trouvent dans des lieux privés ou des espaces publics et commerciaux, y compris des lieux de travail, et ce partout dans le monde.

Sur votre site Web, il est indiqué que cette pratique vise à démontrer l'importance de régler les paramètres de sécurité des caméras de surveillance. Nous reconnaissons en principe l'importance de mettre en lumière les problèmes potentiels liés à la sécurité, mais nous estimons que cela devrait se faire d'une façon qui ne porte pas atteinte aux gens.

Compte tenu de la nature délicate des renseignements personnels recueillis au moyen de ces caméras, particulièrement celles se trouvant dans les maisons, et du fait que votre site Web communique ces renseignements personnels sans que les individus filmés en soient conscients, cela constitue une grave menace pour la vie privée des gens du monde entier. Cette menace est accentuée par l'inclusion d'information sur l'emplacement géographique précis des caméras.

De plus, comme vous le savez sans doute, cette question a beaucoup retenu l'attention des médias. L'intérêt accru du public entraînera un risque encore plus important que les caméras accessibles à distance portent atteinte à la vie privée des personnes.

Par conséquent, nous vous demandons de prendre des mesures immédiates afin de fermer ce site Web. Nous vous demandons en outre d'éviter de recréer ce site à l'avenir, que ce soit sous son nom actuel ou tout autre nom, s'il continue de diffuser toute séquence vidéo montrant des individus et que ces derniers ne savent pas que la séquence vidéo en question fait l'objet d'une communication. Si vous ne vous conformez pas à cette demande d'ici au 26 novembre 2014 (00:00 UTC), nous envisagerons de prendre des mesures supplémentaires d'application de la loi.

Veuillez agréer, Mesdames, Messieurs, nos salutations distinguées.

Le commissaire à la protection de la vie privée de l'Australie,

Original signé par

Timothy Pilgrim

Le commissaire à la protection de la vie privée du Canada,

Original signé par

Daniel Therrien

La coordonnatrice, Office for Personal Data Protection of Macao – Chine,

Original signé par

Chan Hoi Fan

Le commissaire adjoint à l'information du Royaume-Uni,

Original signé par

David Smith

Le président de la Commission d'accès à l'information du Québec,

Original signé par

M^{e} Jean Chartier

La commissaire à l'information et à la protection de la vie privée de l'Alberta,

Original signé par

Jill Clayton

La commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique,

Original signé par

Elizabeth Denham

Les autorités chargées de la protection des données exhortent Google à donner suite aux préoccupations concernant Google Glass

Ottawa, le 18 juin 2013

Monsieur Larry Page
Chef de la direction
Google Inc.
1600 Amphitheatre Parkway
Mountain View, California
USA 94043

Monsieur,

Nous vous écrivons à titre d'autorités de protection des données personnelles afin de soulever, du point de vue du droit à la vie privée, des questions entourant le développement de Google Glass, un type d'ordinateur vêtement sous forme de lunettes[1], présentement en phase de test bêta et n'étant pas encore disponible au grand public.

Vous avez constaté bien entendu que Google Glass a fait l'objet de nombre d'articles qui soulèvent des préoccupations au sujet des répercussions évidentes, et peut-être moins évidentes, sur le plan de la vie privée découlant d'un appareil qui peut être porté par une personne et qui peut servir à produire des enregistrements audio et vidéo d'autres personnes. Des craintes ont été soulevées quant à la surveillance ubiquiste d'individus par d'autres individus, que ce soit par l'entremise de tels enregistrements ou d'autres applications présentement en développement. Des questions quant à la collecte de telles données par Google et quant à leur utilisation se posent également au regard de la nouvelle politique de confidentialité de Google.

Comme vous le savez sans doute, les autorités de protection des données insistent depuis longtemps sur la nécessité pour les organisations de tenir compte des principes de protection des données personnelles dès l'étape de la conception des produits et services, avant le lancement de ceux-ci. En outre, plusieurs d'entre nous enjoignons les organisations à consulter de manière significative nos autorités respectives.

À ce jour, tout ce que nous savons au sujet de Google Glass, de son mode d'opération, de ses usages potentiels et de l'utilisation que Google pourrait faire des données recueillies par l'entremise de Glass provient en grande partie d'articles de presse, largement fondés sur des hypothèses, et de la publicité effectuée par Google elle-même au sujet de l'appareil.

Par exemple, nous avons cru comprendre que pendant la phase de test bêta du produit, Google a mis en place des lignes directrices détaillées à l'intention des développeurs d'applications qui conçoivent des programmes destinés à Glass[2]. Les limites qui leur sont imposées semblent porter en grande partie sur la publicité à l'intérieur de Glass. Si c'est effectivement le cas, nous y verrions une première étape positive dans le repérage des enjeux de vie privée, mais il ne s'agirait que d'une première étape et de la seule dont nous serions au courant.

Nous savons que d'autres entreprises développent également des produits semblables, mais la vôtre est un chef de file en la matière, la première à faire l'essai d'un produit in situ, et la première à envisager les enjeux éthiques soulevés par un tel produit. Jusqu'à présent, toutefois, votre entreprise n'a toujours pas communiqué avec la majorité des autorités de protection des données personnelles signataires de la présente pour discuter de l'un ou l'autre des enjeux en cause.

Pour notre part, nous exhortons Google à entamer un dialogue significatif avec les autorités de protection des données au sujet de Glass.

Nous voudrions soulever entre autres les questions suivantes :

- Comment Google Glass se conforme-t-il aux lois sur la protection des données?
- Quelles mesures de protection des données personnelles Google et les développeurs d'application mettent-ils en place?
- Quels renseignements Google recueille-t-elle par l'entremise de Glass et quels renseignements sont transmis à des tiers, y compris des développeurs d'applications?
- Comment Google compte-t-elle utiliser cette information?
- Bien que nous croyions comprendre que Google a choisi de ne pas intégrer la reconnaissance faciale à Glass, comment Google prévoit-elle aborder les enjeux liés à la reconnaissance faciale à l'avenir?
- Google fait-elle quoi que ce soit au sujet des grands enjeux sociétaux et éthiques soulevés par un tel produit, en outre, au sujet de la collecte subreptice d'information au sujet d'autres individus?
- Google a-t-elle déjà entrepris des évaluations des risques à la vie privée dont elle serait disposée à partager les conclusions avec nous?
- Google serait-elle disposée à faire une démonstration de l'appareil à l'intention de nos organisations, et de permettre à toute autorité de protection des données qui en fait la demande de soumettre l'appareil à des tests?

Nous sommes conscients que ces questions portent sur des enjeux qui sont de notre ressort en tant qu'autorité de protection des données, de même que sur des enjeux éthiques plus vastes soulevés par les ordinateurs vêtements. Nous serions très intéressés à en savoir davantage au sujet de l'incidence sur la vie privée de ce nouveau produit, et des mesures que vous envisagez adopter afin de vous assurer que le droit à la vie privée des personnes est respecté partout dans le monde, alors que vous allez de l'avant avec Google Glass. Nous attendons de vos nouvelles à ce sujet et nous espérons avoir l'occasion de prendre part à une rencontre afin de discuter des enjeux de vie privée soulevés par Google Glass.

Veuillez agréer, Monsieur, l'expression de nos sentiments distingués,

La commissaire à la protection de la vie privée du Canada,

Original signé par

Jennifer Stoddart

Le président du Groupe de travail de l'Article 29, au nom des membres du Groupe de travail de l'Article 29,

Original signé par

Jacob Kohnstamm

Le commissaire à la protection de vie privée de l'Australie,

Original signé par

Timothy Pilgrim

La commissaire de la protection de la vie privée de la Nouvelle-Zélande,

Original signé par

Marie Shroff

Le secrétaire à la protection des données de l'Institut fédéral de l'Accès à l'information et la Protection des données du Mexique,

Original signé par

Alfonso Oñate Laborde

Le chef de la Israeli Law, Information and Technology Authority (Israël),

Original signé par

Rivki Dvash

Le préposé fédéral à la protection des données et à la transparence (Suisse),

Original signé par

Hanspeter Thür

La commissaire à la protection de la vie privée de l'Alberta,

Original signé par

Jill Clayton

Le président de la Commission d'accès à l'information du Québec,

Original signé par

Jean Chartier

La commissaire à la protection de la vie privée de la Colombie-Britannique,

Original signé par

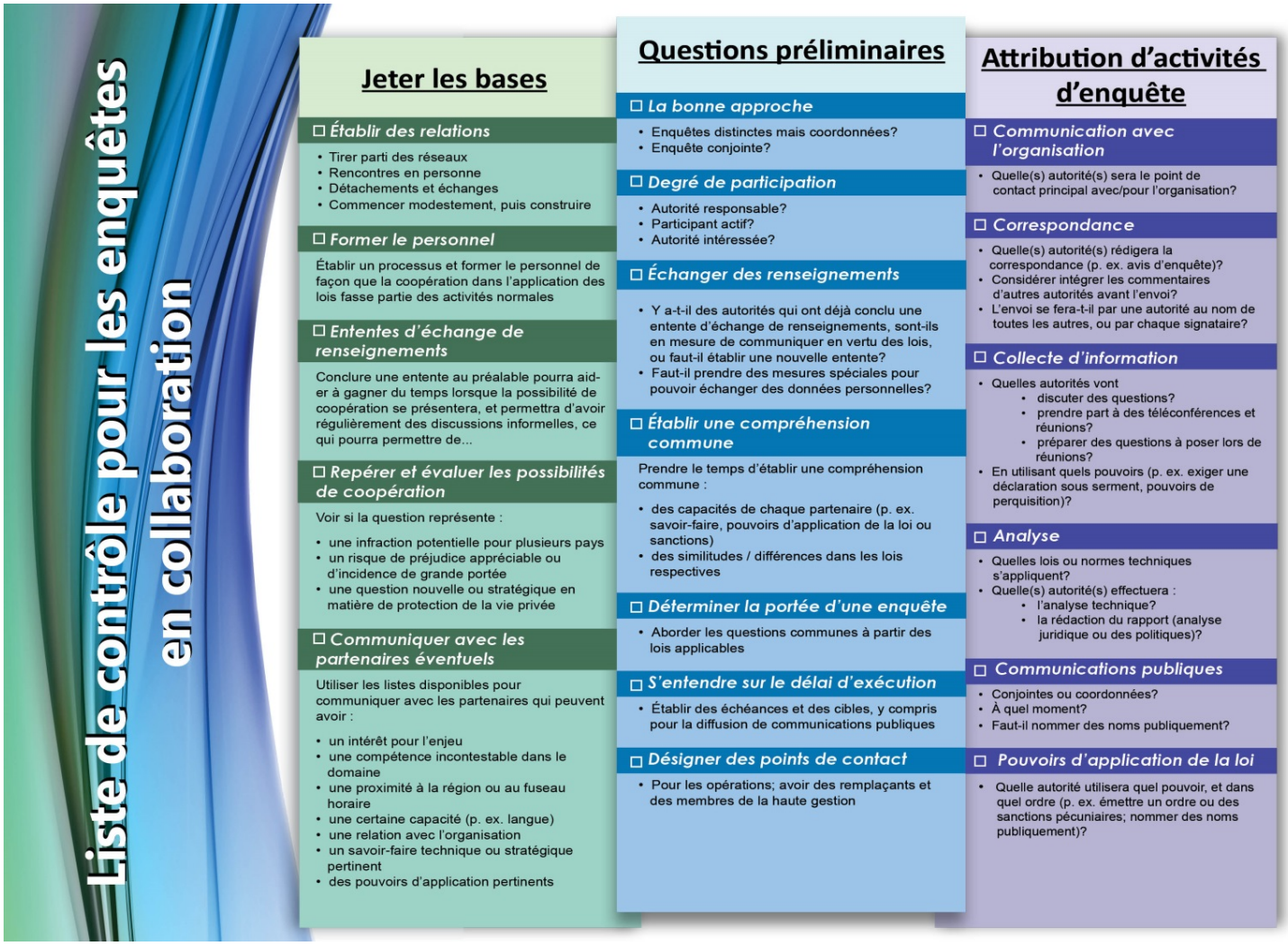
Elizabeth Denham

[1] Google Glass comprend une caméra, un micro et un GPS, avec connectivité Internet. Google Glass fonctionne à partir du système d'exploitation Android, et des tierces parties développent présentement des applications pour Glass. Pour accéder à Glass, l'utilisateur doit disposer d'un compte Google.

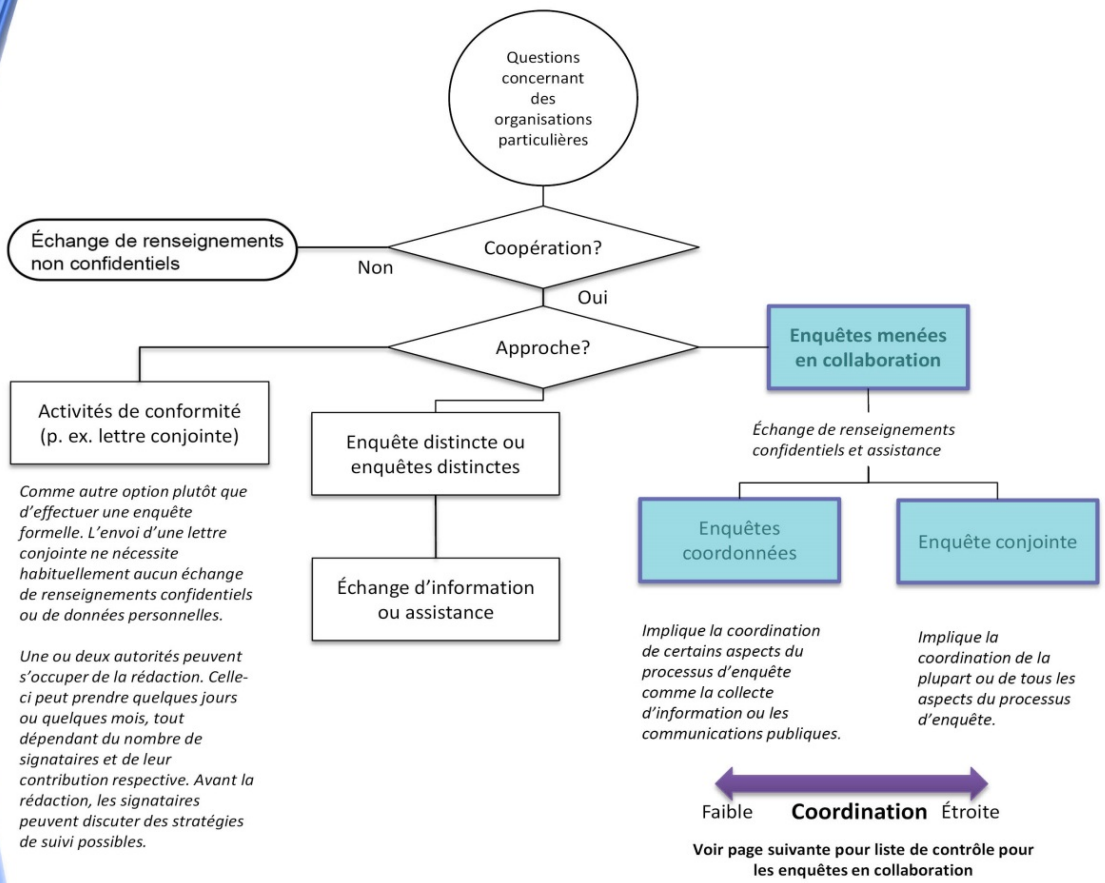
[2] https://developers.google.com/glass/overview

ANNEXE D

Aide-mémoire sur la coopération dans l'application des lois



Graphique de cheminement de la coopération dans l'application des lois



Voir page suivante pour liste de contrôle pour les enquêtes en collaboration

ANNEXE E

Exemple de modèle aux fins d'utilisation par les autorités lors de l'élaboration de leurs propres mécanismes de réflexion à l'égard de la coopération dans l'application transfrontière des lois

Liste de contrôle pour la coopération dans l'application des lois

Étape d'exploration

1. Organisation (nom et adresse, le cas échéant)

2. **Enjeu**

• Brève description de l'enjeu • Élément ayant permis de cerner l'enjeu (p. ex. plainte, médias ou autre autorité de protection des données personnelles) • Aspects internationaux

3. **L'enjeu relève-t-il de votre compétence?** Oui Non À déterminer

4. **Partenaires éventuels dans l'application de la loi**

Autorité	Fondements possibles pour la coopération
Nom et territoire	• Organisation exerçant ses activités sur le territoire de l'autorité • Intérêt exprimé par l'autorité

5. **Votre autorité a-t-elle le pouvoir d'échanger des renseignements personnels dans ce dossier?** Oui Non

Capacité d'échanger de l'information	• Fondements juridiques, restrictions (dans la négative, discussions de haut niveau uniquement)

6. **Premier contact avec l'autorité**

Autorisation (antérieure) donnée par :	• P. ex. directeur
Coordonnées	Nom, titre et coordonnées

Structure	**Information recherchée**

Intérêt ou enquête?	Oui ou non
Raison de l'intérêt pour l'enjeu	• Plaintes reçues • Enquête en cours ou nécessité de faire enquête • Enjeu grave ayant une incidence sur les individus
Intérêt pour la coopération ou l'échange d'information	Oui ou non
Partage des connaissances (lorsque la loi l'autorise)	• Résumé de la compréhension de l'autorité, des éléments de preuve déjà recueillis et des différences importantes par rapport à sa propre compréhension
Examen des bénéfices potentiels de la coopération ou de l'échange d'information	• Compétence et lien avec l'organisation • Proximité et langue • Capacité ou pouvoir d'accéder aux éléments de preuve pertinents • Savoir-faire particulier (stratégique ou technique)

7. Recommandations de l'enquêteur

- i) Aucune mesure requise de la part de votre autorité
- ii) Enquête menée par votre autorité ou par une autre autorité agissante seule, avec échange d'information
- iii) Enquête coordonnée par votre autorité ou par une autre autorité (certains aspects de l'enquête peuvent être coordonnés – voir 10b] ci-après)
- Justification : autre autorité intéressée; avantages et possibilités pour votre autorité

Étape d'enquête

8. Approbation de l'approche de coopération (cadre supérieur)

9. Compréhension et approbation des modalités de l'échange d'information

Organisations échangeant l'information	• Votre autorité, autre autorité ou les deux
Type d'information à échanger	• P. ex. mises à jour sur l'enquête et éléments de preuve
Fréquence	• P. ex. à la réception ou mensuellement
Restrictions et exigences	• Fondements juridiques, mesures de protection, traitement des données personnelles ou restrictions relatives à la publication

10. Enquête menée en collaboration

a. Questions préliminaires

Votre autorité mènera-t-elle l'enquête ou enquêtera-t-elle en collaboration?	• Volonté ou besoin des deux autorités de faire enquête • Possibilité de regrouper les ressources pour accroître l'efficience ou l'incidence
Compréhension de la législation régissant le partenaire	• Similitudes et différences importantes • Pouvoirs d'application des lois et pouvoirs de collecte des éléments de preuve • Restrictions relatives à la communication au public
Établissement de la portée de l'enquête	• Enjeux visés par l'enquête (y compris les différences entre les autorités)
Délai d'exécution ou jalons convenus	• Avis à l'organisation • Communication de mise à jour périodique • Achèvement de l'enquête et publication des conclusions
Contacts	Contact pour l'enquête
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées)
	Contact secondaire pour l'enquête
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées)
	Contact de la direction
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées
	Autre (p. ex. technologie)
	Votre autorité : (nom, titre et coordonnées) Autre autorité : (nom, titre et coordonnées)

b. Coordination des activités d'enquête et d'application des lois

Point de contact au sein de l'organisation	• Un contact au sein de chaque autorité
Correspondance avec l'organisation	• Correspondance conjointe ou distincte (mais généralement coordonnée)
Collecte d'information auprès de l'organisation	• Qui recueillera quelle information et en vertu de quelle compétence (généralement de façon coordonnée)?
Analyse des éléments de preuve	• P. ex. analyse technique ou juridique
Communications publiques	• Communications conjointes ou coordonnées (envoi de messages ou moment des communications)
Atteinte de la conformité ou application de la loi	• Quels pouvoirs seront utilisés et qui les utilisera (désignation, pénalités ou conformité obligatoire)?

11. Approbation de l'approche finale (p. ex. cadre supérieur ou directeur chargé de l'application des lois)

Exemple de modèle de plan d'enquête conjointe ou coordonnée

Données de base

N° de dossier - *Autorité A* - *Autorité B* - *Autorité C*	
Nom de l'intimé	
Adresse de l'intimé	
Date(s) de début de l'enquête	
Date initiale du plan	
Historique des versions	

Type de coopération

Enquêtes distinctes, mais coordonnées, ou enquête conjointe.

Échange d'information

Protocoles d'entente en vertu desquels il y aura échange d'information, et toute autre exigence ou limite que les autorités souhaitent mettre en évidence.

Questions devant faire l'objet d'une enquête

Établir la portée de l'enquête, y compris les questions qui feront l'objet d'une enquête conjointe et celles qui feront l'objet d'enquêtes distinctes. Les question devraient être abordées en fonction des lois applicables respectives, en précisant les dispositions des lois en question pour assurer une bonne compréhension de ce que chaque autorité doit examiner.

Jalons/calendrier

Un consensus doit être établit en ce qui concerne le calendrier et les jalons détaillés de l'enquête (p. ex. envoi de l'avis, réception des observations, visite des lieux, rapport provisoire, rapport définitif – sous réserve d'ajustements pour tenir compte des besoins opérationnels ou de circonstances imprévues). Le Modèle des jalons peut servir de document d'orientation.

Points of Contact

Chaque autorité doit désigner un point de contact principal pour les communications régulières, ainsi qu'un point de contact secondaire en cas d'absence. Un point de contact représentant la haute direction peut être désigné pour les discussions stratégiques.

Rôles et responsabilités

Identifier l'autorité responsable (ou les co-responsables), les participants actifs et les autorités intéressées.

Collecte de renseignements et communication avec l'organisation

Déterminer les éléments suivants :

- *Quelle autorité sera le principal point de contact des parties?*
- *Quelle correspondance sera envoyée arborant l'en-tête conjointe ou seulement celle de l'autorité responsable?*
- *Les discussions avec les parties seront-elles tenues conjointement ou seulement avec l'autorité responsable?*
- *De quelle manière les questions posées aux parties seront-elles déterminées : seront-elles rédigées par l'autorité responsable aux fins d'examen et d'approbation par les autres autorités?*
- *De quelle manière et par qui les renseignements seront-ils recueillis (p. ex. observations écrites, entrevues, recherche indépendante) et examinés?*

Visites des lieux/entrevues

Une visite des lieux est-elle anticipée? Dans l'affirmative, préciser l'objectif et les détails généraux de la visite des lieux. Quelles autorités participeront à la planification et lesquelles participeront à la visite des lieux. Des entrevues seront-elles réalisées sous serment?

Analyse

Indiquer les autorités qui seront responsables de l'analyse technique et de la rédaction du rapport (analyses juridique et des politiques).

Communications publiques

(Pourrait être établi durant l'enquête)
Établir le plan de communications publiques, déterminer si les communications sont conjointes ou coordonnées, afin d'amplifier l'incidence des leçons tirées, et si l'intimé devrait être nommé.

Application de la loi

(Pourrait être établi durant l'enquête)
Dans l'éventualité où il serait nécessaire de faire respecter les loi visées, quelles autorités prendront quelles mesures d'application de la loi?

Tâche	Autorité responsable	Date de début prévue	Date de fin cible	Date d'achèvement	État et notes
Lancement de l'enquête					
Réaliser la recherche préliminaire					
Cerner les preuves nécessaires					
Envoyer les avis et les demandes d'information					
Recevoir et analyser les réponses des parties aux questions préliminaires					
Acheminer les questions additionnelles à l'intimé					
Visite des lieux (s'il y a lieu)					
Établir un plan de visite des lieux					
Obtenir les approbations internes					
Aviser l'intimé de la visite des lieux					
Effectuer les visites des lieux					
Recevoir les documents demandés lors de la visite					
Analyse					
Effectuer une analyse technique					
Réaliser des analyses juridique et des politiques					
Rédiger un rapport des conclusions et obtenir un consensus à son égard					
Obtenir les approbations internes					

Communiquer les conclusions et les recommandations avec l'intimé, et obtenir des engagements					
Produire un rapport des conclusions					
Communications publiques					
Établir un plan de communications publiques					
Application de la loi					
À déterminer, le cas échéant					

Glossaire

Le présent glossaire a pour objet d'expliquer aux rédacteurs la signification de certains termes utilisés dans le guide. Il prend acte du fait que les autorités peuvent donner des définitions différentes mais tout aussi valables de ces termes conformément à leur cadre juridique. Les explications ne sont donc pas données dans le but d'obtenir, voire de suggérer leur acceptation générale. Le glossaire doit uniquement être utilisé pour interpréter et comprendre le présent guide. Les autorités de chaque pays sont les mieux placées pour évaluer dans quelle mesure cela concorde avec la terminologie locale.

1. **activité en matière d'application de la loi ou activité en matière de conformité**

    a. **activité en matière d'application de la loi :** Mesure(s) prise(s) par une autorité d'exécution des lois sur la protection de la vie privée dans le but soit : i) d'exiger qu'une organisation (ou un particulier) se conforme à la législation sur la vie privée ; ou ii) de pénaliser l'organisation ou le particulier en question qui ne se conforme pas.

    b. **activité en matière de conformité :** Mesure(s) prise(s) par une autorité d'application des lois sur la protection de la vie privée dépassant le cadre de ses pouvoirs d'exécution pour encourager la conformité volontaire des organisations ou des particuliers aux lois sur la protection de la vie privée ou à des pratiques exemplaires.

2. **autorité d'exécution des lois sur la protection de la vie privée (ou « autorité ») :** Autorité ayant la responsabilité de promouvoir la conformité aux lois sur protection de la vie privée ou d'obliger à la conformité sur un territoire donné. Aux fins du présent guide, le terme inclut les autorités assurant la protection des données.

3. **autorité responsable de la concurrence :** Autorité chargée de la promotion, de la réglementation ou de l'application de lois en matière de concurrence (dispositions relatives à la concurrence (ou de lois antitrust) énoncées dans les lois applicables relevant de sa compétence. Elle s'affaire généralement à assurer et à maintenir une concurrence équitable et efficace sur le marché, en évaluant les répercussions sur les concurrents des fusions proposées et en déterminant s'il s'agit d'un abus de position dominante ou d'une autre forme de comportement anticoncurrentiel.

4. **autorité responsable de la protection des consommateurs :** Autorité chargée de la faire la promotion et d'assurer le respect des dispositions relatives à la protection des consommateurs dans les lois applicables relevant de sa compétence. Le terme peut s'appliquer à un large éventail d'activités réglementaires liées à la protection des intérêts des consommateurs, allant des pratiques d'affaires injustes, trompeuses ou frauduleuses qui compromettent la sécurité des consommateurs. De telles autorités auront souvent un mandat double comprenant la sphère de la concurrence. Aux fins du présent guide, le terme s'applique à toute autorité visée par la présente définition.

5. **compétence (juridiction) :** Portée des responsabilités d'une autorité d'application des lois en matière de protection de la vie privée (c'est-à-dire les limites légales ou géographiques) ou région géographique au sein de laquelle une autorité est chargée de faire appliquer les lois en matière de protection de la vie privée.

6. **coopération :** Regroupement de plusieurs autorités pour favoriser l'application de mesures de protection de la vie privée, ayant les objectifs suivants : i) la communication d'une politique non confidentielle ou d'information pratique; ii) l'échange de renseignements confidentiels ou de données personnelles ; ou iii) la coordination des activités aux fins d'activités en matière d'application de la loi ou de conformité dans un autre domaine.

    a. **coordination :** Forme de coopération dans le cadre de laquelle plusieurs autorités établissent des liens entre leurs activités (ou les coordonnent) en relation avec des activités particulières d'application des lois (p. ex. enquête menée en collaboration ou initiative en matière de conformité dans un autre domaine – p. ex. lettre conjointe ou ratissage).

        i. **enquête menée en collaboration :** Forme de coordination dans le cadre de laquelle plusieurs autorités coordonnent leurs activités en relation avec des activités d'application des lois connexes dans leurs pays respectifs (p. ex., collecte de renseignements, analyse technique, communication publique de résultats). L'enquête requiert généralement la communication de renseignements confidentiels ou de données personnelles. Le niveau de collaboration (p. ex. le nombre d'activités que les autorités choisissent de coordonner) peut être restreint ou vaste.

7. **données personnelles (ou renseignements personnels) :** Information sur une personne qui est, dans de nombreux pays, visée par des exigences particulières en vertu des lois sur la protection de la vie privée ou des renseignements (p. ex. comme il est précisé à l'article 7 et à l'annexe I de l'Entente). Les données personnelles seront, dans la plupart des cas, des renseignements confidentiels. Pour les besoins exclusifs du présent guide, nous n'établirons pas de distinction entre les « données personnelles » et les « renseignements personnels ».

8. **entente (ou protocole d'entente) :** Document n'ayant pas force exécutoire signé par plusieurs autorités d'exécution des lois sur la protection de la vie privée, qui précise l'accord intervenu entre les signataires, les situations et les conditions en vertu desquelles ces autorités peuvent coopérer dans le cadre d'activités d'application de la loi et, en particulier, échanger des renseignements confidentiels ou des données personnelles. Rien dans ce type de document n'exige que les signataires se prêtent main-forte dans l'application des lois si cette assistance est interdite par des lois nationales ou applicables ou par les politiques en matière d'application de la loi. Aux fins du présent guide, nous n'établissons pas de distinction entre une entente et un protocole d'entente.

9. **renseignements confidentiels :** Renseignements qu'une « autorité qui communique » fournit à une « autorité qui reçoit » (ensemble, « les autorités coopérantes »), étant entendu que, sous réserve de toute autre entente entre les autorités coopérantes, l'autorité qui reçoit s'assurera que les renseignements ne sont accessibles qu'aux personnes relevant de sa compétence et devant avoir accès à ces renseignements aux fins où ils ont été communiqués (p. ex. en relation avec une enquête précisée). Les renseignements confidentiels sont souvent des renseignements se rapportant à une activité en matière d'application de la loi en cours ou éventuelle qui peut inclure ou non des données personnelles. Ils peuvent également comporter d'autres types de renseignements stratégiques non publics ou ayant trait à la politique.