PROJET DE RÉSOLUTION SUR LE RÔLE DES ERREURS D'ORIGINE HUMAINE DANS LES ATTEINTES À LA SÉCURITÉ DES DONNÉES PERSONNELLES

41e Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC)
Octobre 2019, Tirana, Albanie

PARRAINEUR :

- Office of the Australian Information Commissioner, Australie

COPARRAINEURS :

- Autoriteit Persoonsgegevens, Pays-Bas;
- Comissão Nacional de Protecção de Dados, Portugal;
- Commission nationale de l'informatique et des libertés, France;
- Data Protection Commission, Irlande;
- Information Commissioner's Office, Royaume-Uni;
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Mexique;
- National Privacy Commission, Philippines;
- Office of the Privacy Commissioner, Nouvelle-Zélande;
- Commissariat à la protection de la vie privée du Canada, Canada.

CONSTATANT que, afin de protéger la vie privée des personnes et d'instaurer la confiance dans l'économie des données, une réponse mondiale des autorités et des organisations chargées de la protection des données et de la vie privée est nécessaire en raison de l'augmentation du nombre, de l'ampleur et de la gravité des atteintes à la sécurité des données personnelles, du caractère commun de leurs causes, de la nature internationale des conséquences qui en découlent et des dommages qui peuvent en résulter;

RECONNAISSANT que la mise en œuvre de systèmes de notification des atteintes à la sécurité des données personnelles dans certaines juridictions membres a entraîné une augmentation significative du signalement des atteintes à la sécurité des données personnelles, ce qui a permis de mieux comprendre leurs causes et de mieux comprendre comment elles pourraient être évitées ainsi que de définir des stratégies de prévention potentielles;

SOULIGNANT que les notifications d'atteintes à la sécurité des données personnelles et les mesures réglementaires dans certaines juridictions membres ainsi que les études nationales et internationales montrent que les atteintes à la sécurité des données personnelles impliquent souvent une erreur d'origine humaine, en particulier lorsque les employés divulguent involontairement des données personnelles à des destinataires non autorisés ou que des personnes sont amenées par tromperie à compromettre les informations d'identification des utilisateurs qui donnent accès aux systèmes et informations (« erreur d'origine humaine »);

RECONNAISSANT qu'un principe commun aux lois sur la protection de la vie privée et des données dans le monde entier est que les données personnelles devraient être protégées par des garanties de sécurité adéquates contre des risques tels que la perte ou l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation;

AFFIRMANT que la prédominance de l'erreur d'origine humaine dans les atteintes à la sécurité des données personnelles souligne l'importance de créer des cultures de travail où la protection de la vie privée et la sécurité sont des priorités organisationnelles, notamment par la mise en œuvre périodique de programmes de formation, d'éducation et de sensibilisation, par la prise en compte de la vie privée dans la conception, le fonctionnement et la gestion des systèmes et des pratiques, et la mise en œuvre de solutions technologiques;

NOTANT que la Conférence internationale des commissaires à la protection des données et de la vie privée a déjà reconnu la nécessité d'œuvrer à l'élaboration de politiques, de normes et de modèles mondiaux et de renforcer la coopération en matière de réglementation pour améliorer la prévention, la détection, la dissuasion et les recours efficaces en matière de protection des données et de vie privée, et pour garantir la cohérence et la prévisibilité du système de contrôle dans l'économie des données;

CONSCIENT des travaux en cours de l'Organisation de coopération et de développement économiques (OCDE) pour faire en sorte que la sécurité numérique et la protection de la vie privée favorisent le développement de l'économie numérique, et pour améliorer la base de données probantes pour l'élaboration de politiques de sécurité et de protection de la vie privée, y compris la comparabilité des rapports de notification des atteintes à la protection des données personnelles;

NOTANT que l'enquête de 2017 de la Conférence internationale des commissaires à la protection des données et de la vie privée a montré que les systèmes de notification des atteintes à la sécurité des données personnelles varient d'une juridiction membre à l'autre et comprennent l'absence d'un système de notification des atteintes à la sécurité des données personnelles, un système volontaire de notification des atteintes à la sécurité des données personnelles et l'obligation de notifier les atteintes à la sécurité des données personnelles qui s'applique de manière générale ou à certains secteurs particuliers[1];

SOULIGNANT que la collecte, la classification, l'analyse et la publication de statistiques sur les atteintes à la sécurité des données personnelles notifiées aux autorités responsables de la protection des données et de la vie privée, y compris sur leurs causes, sont essentielles pour l'élaboration d'une politique mondiale et d'une réponse aux causes des atteintes à la sécurité des données personnelles;

RAPPELANT qu'en 2009, la 31e Conférence internationale des commissaires à la protection des données et de la vie privée a adopté les normes internationales sur la protection des données personnelles et de la vie privée (« la résolution de Madrid »), qui comprennent des principes visant à protéger les données personnelles par la mise en œuvre de mesures techniques et organisationnelles adéquates (Principe 20 – Mesures de sécurité) et des mesures proactives, notamment la mise en œuvre de programmes et de vérifications réguliers par des parties indépendantes (Principe 22 – Mesures proactives) de formation, d'éducation et de sensibilisation;

RAPPELANT qu'en 2010, la 32e Conférence internationale des commissaires à la protection des données et de la vie privée a décidé d'encourager l'adoption des Principes fondamentaux de la prise en compte du respect de la vie privée dès la conception comme guide pour faire de la protection de la vie privée le mode de fonctionnement par défaut des organisations;

La 41e CONFÉRENCE INTERNATIONALE DES COMMISSAIRES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE se propose de faire appel :

1) AUX MEMBRES DE l'ICDPPC qui recueillent, analysent et publient des statistiques sur les atteintes à la sécurité des données personnelles qui leur sont signalées dans le cadre d'un système de notification volontaire ou obligatoire des atteintes à la sécurité des données personnelles afin qu'ils :

i) classent les causes des atteintes à la sécurité des données personnelles et en fassent rapport, et envisagent d'inclure des classifications pour celles qui sont le résultat d'une erreur d'origine humaine;

ii) poursuivent l'examen de toute recommandation relative à la mesure des atteintes à la sécurité des données personnelles formulée par des organes d'experts tels

[1]Groupe de travail sur les indicateurs de protection des données de la Conférence internationale des commissaires à la protection des données et de la vie privée, *Counting on Commissioners: High level results of the ICDPPC Census 2017* (2017) https://icdppc.org/wp-content/uploads/2017/09/ICDPPC-Census-Report-1.pdf.

que l'OCDE et le Groupe de travail de l'ICDPPC sur les indicateurs de protection des données.

2) À TOUS LES MEMBRES DE l'ICDPPC afin qu'ils promeuvent des garanties de sécurité adéquates pour prévenir les erreurs d'origine humaine pouvant entraîner des atteintes à la sécurité des données personnelles, notamment les suivantes :

i) établir des cultures de travail où la protection de la vie privée et la sécurité des données personnelles sont des priorités organisationnelles, notamment par la mise en œuvre de programmes réguliers de formation, d'éducation et de sensibilisation pour les employés sur leurs obligations en matière de protection de la vie privée et de sécurité et par la détection et la déclaration des menaces à la sécurité des données personnelles;

ii) établir des pratiques, des procédures et des systèmes robustes et efficaces en matière de protection des données et de protection de la vie privée, notamment en :

   a. intégrant la protection de la vie privée dans la conception, l'exploitation et la gestion des systèmes et des pratiques et en investissant dans l'amélioration de la situation concernant la sécurité mondiale en fonction des risques connus en matière de sécurité;

   b. au niveau de l'utilisateur, mettant en œuvre des technologies pour compléter l'éducation de l'utilisateur sur l'atténuation du risque de compromission des justificatifs d'identité et de divulgation non intentionnelle de données personnelles à des destinataires non autorisés;

iii) évaluer les pratiques, les procédures et les systèmes de protection de la vie privée afin d'assurer leur efficacité continue, notamment en mettant en œuvre un programme d'examen proactif, y compris la surveillance et la vérification du système.

3) À TOUS LES MEMBRES DE L'ICDPPC afin qu'ils assurent la liaison avec les réseaux internationaux et régionaux pertinents pour promouvoir cette résolution.

4) AUX ORGANISATIONS (Y COMPRIS LE GOUVERNEMENT ET LES ENTREPRISES) afin qu'elles comprennent et reconnaissent que les atteintes à la sécurité des données personnelles impliquent souvent une erreur d'origine humaine et mettent en œuvre des garanties de sécurité adéquates, qui peuvent inclure celles décrites au paragraphe 2) ci-dessus.

NOTE EXPLICATIVE

Ce projet de résolution constitue une nouvelle étape vers une politique globale de l'ICDPPC en matière de prévention des atteintes à la sécurité des données personnelles, en mettant l'accent sur les garanties de sécurité qu'il convient de prendre contre la cause de nombreuses atteintes à la sécurité des données personnelles – l'erreur d'origine humaine.

Le projet de résolution arrive à point nommé étant donné que l'augmentation importante du nombre de notifications dans les juridictions membres de l'ICDPPC avec des systèmes obligatoires de notification des atteintes à la sécurité des données confirme ce que l'on sait depuis un certain temps – que de nombreuses atteintes à la sécurité des données personnelles sont causées ou provoquées par des erreurs d'origine humaine[2].

Le premier appel à l'action vise à constituer la base de données probantes fournie par les notifications des atteintes à la sécurité des données. Une enquête menée en 2017 sur les pratiques statistiques relatives à la notification des atteintes à la vie privée, en collaboration avec le Groupe de travail sur les indicateurs de protection des données de l'ICDPPC, a démontré qu'il y a peu de points communs dans la façon dont les personnes sondées ont classifié les atteintes à la sécurité des données personnelles dont elles ont été informées, et a laissé entendre qu'il y avait une bonne marge de travail pour aider les autorités à élaborer des pratiques communes pour classifier la nature des atteintes[3].

L'Organisation de coopération et de développement économiques (OCDE) a déterminé des questions semblables dans le cadre de ses travaux en cours pour améliorer la base de données probantes pour l'élaboration de politiques de sécurité et de protection de la vie privée. Les travaux de l'OCDE dans ce domaine comprennent l'élaboration d'un questionnaire, avec le soutien de l'ICDPPC, pour nourrir une étude de faisabilité sur les données que les autorités de protection des données et de la vie privée devraient collecter et dont elles devraient rendre copter afin d'améliorer la comparabilité dans la notification des atteintes à la protection des données personnelles. Le questionnaire concerne entre autres la classification des types d'atteintes à la protection des données. En particulier, est-ce que les données devraient être classifiées en fonction de « classifications de haut niveau » ou de sous-catégories d' « incidents types » plus précis[4].

---

[2]La détermination d'erreur d'origine humaine comme cause de nombreuses atteintes à la sécurité des données personnelles est antérieure à la mise en œuvre des systèmes obligatoires de notification des atteintes à la sécurité des données et a été signalée comme une cause connue d'atteintes à la sécurité des données personnelles par les juridictions membres qui ont un système volontaire de notification des atteintes à la sécurité des données ou aucun système de notification, ainsi que dans les rapports du secteur privé et des organismes de recherche.

[3] Blair Stewart, *Improving the measurement of digital security incidents (Privacy authority perspectives): Taking stock and priorities for action* (18 avril 2017) https://icdppc.org/wp-content/uploads/2017/04/Breach-notification-statistics-survey-report-18-April-2017.pdf.

[4]Voir, par exemple, OCDE, *Measuring digital security risk management practices in businesses*, Documents de travail de l'OCDE sur l'économie numérique, n° 283 (2009) https://doi.org/10.1787/7b93c1f1-en et Groupe de travail de l'OCDE sur la sécurité et la vie privée dans l'économie numérique (WPSPDE), *OECD Workshop « Improving the Measurement of Digital Security Incidents and Risk Management »: Draft Summary and Main Points* (30 et 31 octobre 2017, Paris) http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP/SPDE(2017)19&docLanguage=En.

L'appel à l'action s'adresse uniquement aux membres qui recueillent, analysent et publient des statistiques sur les atteintes à la sécurité des données personnelles qui leur sont signalées, tout en reconnaissant que les systèmes de notification varient d'une juridiction membre à l'autre, certaines juridictions membres ne disposant pas de système de notification ou ayant pour pratique de communiquer des statistiques sur les atteintes à la sécurité des données personnelles signalées.

Le deuxième appel à l'action s'adresse à tous les membres de l'ICDPPC, individuellement. Il reconnaît la prédominance de l'erreur d'origine humaine et demande aux membres de l'ICDPPC de promouvoir la mise en œuvre de garanties de sécurité TIC efficaces auprès des organisations en plus de prendre des mesures pour traiter l'erreur d'origine humaine afin d'assurer l'efficacité continue des mesures de TIC et de traiter le facteur humain.

L'appel à l'action approuve une liste non exhaustive de garanties de sécurité et d'approches bien connues des membres de l'ICDPPC[5] et communément reconnues comme des garanties de sécurité adéquates dans certaines circonstances contre des risques tels que la perte ou l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation des données personnelles[6].

Le troisième appel à l'action s'adresse à tous les membres de l'ICDPPC et vise à ce que la résolution soit promue par les réseaux internationaux et régionaux pertinents.

Le quatrième appel à l'action s'adresse aux organisations (gouvernements et entreprises). Il vise à mettre en lumière le rôle de l'erreur d'origine humaine dans les atteintes à la sécurité des données personnelles et les garanties de sécurité qu'il peut être approprié de prendre à cet égard.

Bien qu'aucune des garanties de sécurité énoncées dans le projet de résolution ne soit nouvelle pour les membres de l'ICDPPC, leur inclusion constitue un pas supplémentaire vers une politique globale et une réponse aux causes connues des atteintes à la sécurité des données personnelles.

[5] Voir la 31e Conférence internationale des commissaires à la protection des données et de la vie privée, *Normes internationales sur la protection des données personnelles et de la vie privée* (« la résolution de Madrid »), Principe 20 – Mesures de sécurité et Principe 22 – Mesures proactives.

[6] Le principe des garanties de sécurité est un principe fondamental de la protection de la vie privée énoncé dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'OCDE de 1980 ainsi que dans les Lignes directrices révisées de ces Lignes directrices de 2013. Le Principe se rapporte comme suit : « Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés. »