44ème Session à huis clos de l'Assemblée mondiale sur la vie privée

Octobre 2022

Projet de résolution sur le renforcement des capacités de coopération internationale pour améliorer la réglementation en matière de cybersécurité et comprendre les dommages causés par les cyberincidents (v1.9 final)

Cette résolution est soumise par :

SPONSORS:

- Le Bureau du commissaire à l'information (ICO), Royaume-Uni

CO-SPONSORS :

- Bureau du commissaire australien à l'information, Australie
- Commissariat à la protection de la vie privée du Canada
- Surintendance de l'industrie et du commerce (SIC) de Colombie
- Inspection estonienne de la protection des données, Estonie
- Contrôleur européen de la protection des données (CEPD), Union européenne
- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- Commissaire à la protection des données du Ghana (GDPC), Ghana
- Autorité réglementaire de Gibraltar (GRA), Gibraltar
- Bureau du commissaire à la protection de la vie privée pour les données personnelles, Hong Kong, Chine
- Autorité israélienne de protection de la vie privée (PPA), Israël
- Bureau du commissaire à l'information de Jersey (JOIC), Jersey
- Commission nationale de la vie privée, Philippines
- Commission de protection des informations personnelles (PIPC), République de Corée
- Autorité catalane de protection des données (APDCAT), Catalogne, Espagne
- Préposé fédéral à la protection des données et à la transparence (PFPDT), Suisse
- Autorité turque de protection des données personnelles (KVKK), Turquie

- Unité de régulation et de contrôle des données personnelles, Uruguay.

La 44ème *Global Privacy Assembly* (Assemblée Mondiale sur la Protection de la Vie Privée) 2022 :

SOULIGNANT qu'une économie et une société mondiales apportent toute une série d'avantages tels que le commerce mondial, la diffusion mondiale de la technologie et de l'innovation ; la communication, la collaboration et le partage des connaissances et des ressources pour faire face aux problèmes mondiaux, ainsi que les échanges interculturels. Ces avantages ne peuvent être correctement réalisés que si les données à caractère personnel sont protégées de manière adéquate ;

PRÉOCCUPÉS par le fait que la numérisation croissante de l'économie et de la société mondiales entraîne, parallèlement à ses avantages, des risques croissants et importants pour les données personnelles des individus détenues par des organisations publiques et privées ;

NOTANT QUE le risque peut inclure des menaces même accidentelles que délibérées, telles que des tentatives de surveillance et d'accès aux données qui proviennent de sources comme des acteurs étatiques et des entités criminelles non étatiques dans de nombreuses juridictions, opérant souvent par-delà les frontières ;

RECONNAISSANT QUE la confidentialité, l'intégrité et la disponibilité, les trois éléments clés de la sécurité de l'information, sont en péril à cause de ces menaces ; si l'un de ces trois éléments est compromis, il peut y avoir de graves conséquences pour les responsables du traitement des données et aussi des préjudices importants pour les personnes dont les données personnelles sont touchées ;

*SOULIGNANT qu'*un principe commun aux lois sur la vie privée et la protection des données dans le monde entier est que les données à caractère personnel doivent être protégées par des mesures de sécurité appropriées contre des risques tels que la perte ou l'accès non autorisé, la destruction, l'utilisation, la modification, la divulgation ou la non-disponibilité ;

SOULIGNANT À NOUVEAU l'importance de préserver la confiance du public dans les réseaux et les systèmes informatiques par lesquels les données à caractère personnel sont traitées. Aussi, le rôle important que jouent des garanties solides en matière de protection des données et de la vie privée contre les cybermenaces ;

NOTANT QUE la cyber-résilience des systèmes de traitement des données est mise à rude épreuve et que les médias et les analystes de sécurité ont signalé une augmentation des cyber-attaques dans le monde entier, qui peuvent inclure des attaques de la chaîne d'approvisionnement, des accès non autorisés, des rançongiciels, des fraudes d'identité ou de l'hameçonnage ;

PRÉOCCUPÉ PAR LE FAIT que les incidents de cybersécurité ont désormais des conséquences économiques importantes pour la société, car ils sont considérés comme la principale menace pour la réussite financière des organisations[1] et les possibles barrières commerciales qui sont risqués d'être créés ; et que ces conséquences impactent également

[1] Selon une enquête mondiale réalisée par PriceWaterHouse Coopers en janvier 2022 (25th Annual Global CEO Survey - PwC), la cybersécurité est la première menace qui préoccupe les PDG. Les PDG s'inquiètent surtout de la possibilité qu'une cyberattaque ou un choc macroéconomique compromette la réalisation des objectifs financiers de leur entreprise.

les organisations plus petites et moins bien dotées en ressources qui traitent des données à caractère personnel ;

ÉGALEMENT PRÉOCCUPÉ par le fait que les organisations ne prennent pas toujours les précautions opportunes requises pour mettre à jour les mesures techniques et organisationnelles, telles que la *pseudonymisation* ou le cryptage, au sein des systèmes existants afin d'être efficacement équipées contre les cyberattaques croissantes, ce qui génère des risques que les autorités chargées de la protection des données et de la vie privée ont pour rôle de traiter, en collaboration avec d'autres, et que ces risques sont amplifiés si les organisations ne signalent pas ces attaques, les violations de données et autres incidents lorsqu'ils se produisent ou quand ils sont découverts ;

EN OUTRE, CONCERNÉ par le fait qu'une seule cyberattaque peut avoir de graves conséquences pour de nombreuses victimes dans différentes juridictions ; et *SOULIGNANT* qu'il importe par conséquent d'éviter la duplication des travaux de réglementation, ce qui démontre à son tour l'intérêt d'une coopération sur les menaces communes, tant entre les autorités membres de la GPA qu'avec les organismes de cybersécurité, le cas échéant et si les lois locales le permettent ;

SOULIGNANT les prochaines recommandations de l'OCDE sur la sécurité numérique des produits et services et sur le traitement des vulnérabilités, basées sur les travaux existants menés en 2021 par le Comité de la politique de l'économie numérique de l'OCDE avec des experts externes, même qui promeuve la sécurité par conception et par défaut dans les produits et services ; le recours à l'expertise des chercheurs en sécurité pour identifier, signaler et divulguer les vulnérabilités en matière de sécurité numérique ; ainsi que des stratégies de conformité alignées sur les exigences de la législation sur la protection des données ;

NOTANT QUE les politiques publiques ont commencé à évoluer au niveau national pour renforcer les protections des infrastructures nationales critiques, notamment la protection des services publics et essentiels et la garantie d'un signalement précis des incidents et des violations de données. Ce faisant, les gouvernements ont reconnu le lien étroit qui doit exister entre la législation/réglementation relative à la protection des données et la législation relative aux systèmes d'information et à la sécurité des réseaux, afin de concevoir des solutions efficaces en matière de prévention des incidents, de réaction et d'application de la loi ; notamment en ce qui concerne la protection des infrastructures nationales critiques;

RECONNAISSANT que les autorités chargées de la protection des données et de la vie privée dans les différentes juridictions ont des responsabilités, des compétences et des pouvoirs très différents en matière de cybersécurité, mais *NOTANT* le lien étroit entre la cybersécurité et les exigences de nombreuses lois sur la protection des données et la vie privée relatives à la sécurité, la confidentialité, l'intégrité et la disponibilité des données personnelles ;

RÉAFFIRMANT la mission de la GPA, qui consiste notamment à relier et à soutenir les efforts déployés aux niveaux national et régional, ainsi que dans d'autres forums internationaux, pour permettre aux autorités de mieux protéger et promouvoir la vie privée et la protection des données ; et l'importance du renforcement des capacités, de la coopération, du partage des informations et des connaissances dans la poursuite de la mission ;

RAPPELANT QUE la première priorité stratégique de la GPA est de faire progresser la protection de la vie privée à l'ère de la numérisation accélérée et aussi la pertinence de la cybersécurité dans la poursuite de cette priorité ; et *RAPPELANT EN OUTRE* que le plan

stratégique 2021-23 de la GPA[2] exige que la GPA surveille les possibilités de coopération, en notant les risques numériques nouveaux et émergents posés à la vie privée des individus ;

RAPPELANT QUE la GPA a déjà reconnu[3] que la convergence vers des principes clés et des normes élevées pour l'accès des pouvoirs publics aux données à caractère personnel détenues par le secteur privé peuvent contribuer à la sécurité juridique et à la facilitation des flux de données dans l'économie numérique mondiale. Aussi, qu'il a souligné l'importance de la cybersécurité dans et entre tous les systèmes ;

SOULIGNANT l'importance de la cybersécurité pour la protection des données et de la vie privée, et préoccupé par le fait que les cyberattaques peuvent causer des damages importants aux personnes, en particulier celles appartenant à des groupes vulnérables. Entre eux, l'obtention, l'appariement et la vente de données personnelles à des fins frauduleuses ;

NOTANT que certaines autorités chargées de la protection des données et de la vie privée ont déjà commencé à planifier les préjudices liés à la cybersécurité par rapport à d'autres préjudices et à identifier les préjudices sociétaux et individuels causés par les cyberincidents ; mais qu'il reste encore beaucoup à faire pour comparer, d'une juridiction à l'autre : les préjudices plutôt que les abus identifiés (par exemple, les préjudices physiques, psychologiques, culturels, politiques, économiques et de réputation au niveau individuel et sociétal) ; les modèles utilisés pour évaluer ou classer ces préjudices ; l'analyse des lacunes ; et les conséquences réglementaires à prévoir ;

SOULIGNANT que les préjudices consécutifs aux incidents de cybersécurité sont divers et mériteraient une analyse plus approfondie sur la meilleure façon de protéger les individus contre ces préjudices ;

NOTANT QUE les gouvernements de nombreuses juridictions collaborent pour protéger la sécurité nationale et les infrastructures nationales essentielles ;

SOULIGNANT les régulateurs de la protection des données et de la vie privée doivent également être prêtes à collaborer, le cas échéant, à des stratégies internationales et nationales visant à protéger les données des particuliers des individus en cas de cyberincidents ; et également, que la GPA est bien placée pour promouvoir un partage efficace des données réglementaires entre les membres de la GPA sur les vulnérabilités et les menaces en matière de cybersécurité ;

La 44ème Assemblée mondiale de la protection de la vie privée prend donc la résolution suivante :

1. **Prendre des mesures pour mieux comprendre les attributions et les responsabilités des autorités membres de la GPA en matière de cybersécurité ;**
2. **Explorer les possibilités de coopération internationale, de partage des connaissances et des informations entre les membres de la GPA, ce qui devrait inclure l'expertise technique et les meilleures pratiques, afin d'éviter les doubles emplois dans les enquêtes ou autres activités réglementaires concernant les**

[2] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)
[3] 20211025-GPA-Resolution-Government-Access-Final-Adopted .pdf (globalprivacyassembly.org)

questions de cybersécurité et les approches réglementaires en matière de protection des données et de la vie privée ;

3. **Demander au Groupe de travail sur la coopération internationale en matière d'application de la loi de la GPA de réaliser des travaux exploratoires d'ici l'automne 2023, en tenant compte des travaux réalisés par d'autres groupes de travail de la GPA, le cas échéant, et en consultant le Panel de Référence de la GPA si nécessaire. La GPA devrait également déterminer s'il convient de poursuivre ces travaux dans le cadre de son prochain plan stratégique à partir de 2023.**
4. **Demander au Groupe de travail sur la coopération internationale en matière d'application de la loi de convenir d'un plan de travail pour réaliser les étapes ci-dessus, en se concentrant sur des résultats clairs et pratiques qui devraient inclure la tenue d'une session fermée sur les questions de cybersécurité en 2023.**

Note explicative

La prévalence croissante des cyberattaques dans les régions du monde exige une réponse réglementaire solide et coordonnée pour protéger les données personnelles des individus. Les acteurs étatiques et les entités criminelles non étatiques posent de plus en plus facilement des menaces dans le cyberespace, en partie en raison de l'accélération rapide de l'interconnexion numérique de la société depuis l'apparition de la pandémie de COVID-19[4] , mais aussi en raison des vulnérabilités de la chaîne d'approvisionnement dans les produits finaux. Cette résolution se concentre sur l'atténuation et la remédiation des cyberattaques. Les membres de la GPA ont mené un grand nombre d'enquêtes sur des cyberincidents qui ont mis en évidence de graves erreurs de manipulation des catégories de données les plus sensibles, notamment le changement de sexe, les données relatives à la santé et l'identité physique (qui peut inclure la race ou l'origine ethnique, entre autres.). Le manque de sensibilisation à la sécurité dans les organisations, l'absence de responsabilité en matière de sécurité de l'information, la gestion efficace des risques et les contrôles réguliers tout au long de la chaîne d'approvisionnement sont souvent en cause.

Des écosystèmes complexes de fournisseurs pour la prestation de services peuvent signifier un plus grand risque de vulnérabilité ; par exemple, une attaque de la chaîne d'approvisionnement sur un seul point faible générée par une mauvaise gestion des risques de la chaîne d'approvisionnement peut permettre aux cyber-attaquants d'accéder de manière persistante à de nombreux autres serveurs dans le monde entier sur une période prolongée. L'argent, les données personnelles et les informations des personnes sont en danger et leur accès aux services et aux connaissances des secteurs public et privé est fortement compromis par ces cybermenaces.

[4] Par exemple, le Centre national de cybersécurité (NCSC) du Royaume-Uni a signalé en 2021 une multiplication par trois des incidents liés aux ransomwares, le gouvernement, les entreprises et les particuliers étant ciblés de manière plus agressive que précédemment : ISC-Annual-Report-2019-2021.pdf (independent.gov.uk)Et pour les sources commerciales : 2021_NCC_Group_Annual_Threat_Report.pdf Page 19.

Les gouvernements et les autorités régionales, ou les groupements de coopération gouvernementale, ont réagi en adoptant de nouvelles lois, politiques et en lançant des initiatives d'enquête afin de protéger leurs infrastructures nationales critiques, de préserver leur rôle dans le maintien de leurs fonctions publiques ainsi que les moyens de subsistance des entreprises qui sont essentiels à la santé des économies nationales. La cybersécurité n'implique pas qu'un seul facteur pour les organisations ; des facteurs clés tels que la sécurité des données, la sécurité des systèmes, la sécurité en ligne et la sécurité des dispositifs doivent tous être pris en compte pour éviter des préjudices.

Les gouvernements continuent de reconnaître la nécessité d'aligner la législation sur la protection des données, les systèmes d'information en réseau et la sécurité afin de fournir un effort de prévention et d'application plus complet.

Les développements en Europe et sur le continent américain ne sont que quelques-uns des récents ajouts au cadre général de la cybersécurité dans les règlements juridiques et les initiatives de coopération qui ont vu le jour au cours des deux dernières années pour renforcer la résilience, empêcher l'accès non autorisé aux réseaux et permettre des plans de récupération lorsque les attaques ont réussi. Il peut s'agir de solutions telles que des Équipes d'intervention en cas d'incident de sécurité informatique (CSIRT), ou de la création d'une autorité nationale compétente pour émettre des directives et gérer les informations ou les incidents de sécurité.

Les lois régionales, nationales et locales ont imposé aux municipalités et aux autres autorités publiques décisionnaires d'accroître considérablement leur résilience. Certaines autorités chargées de la protection des données et de la vie privée étudient déjà les moyens de contribuer à ces efforts.

Des entités intergouvernementales, telles que l'OCDE, ont reconnu[5] la nécessité de coordonner et de mieux informer les parties prenantes tout au long des chaînes d'approvisionnement afin de traiter efficacement les menaces liées aux vulnérabilités ; de mieux comprendre la position des chercheurs en sécurité, et de développer des moyens pour qu'une bonne gestion des vulnérabilités soit reconnue comme des indicateurs de conformité à la législation sur la protection de la vie privée, telle que le RGPD. Certains de ces besoins ont également été soulignés dans plusieurs rapports nationaux d'organisations régionales[6] comme l'Agence de l'Union européenne pour la cybersécurité (ENISA) ou l'Organisation des États américains (OEA).

Les autorités chargées de la protection des données et de la vie privée peuvent fournir des conseils sur la conformité juridique ainsi que sur les conséquences des nouvelles lois pour une meilleure protection des données personnelles en cas de cyberattaque. On commence à reconnaître les partenariats que les autorités chargées de la protection des données et de la vie privée doivent établir avec leurs homologues nationaux pour apporter une réponse coordonnée, solide et fondée sur les risques aux cybermenaces. Néanmoins, il faut également envisager des partenariats avec des entités situées dans d'autres parties du

[5] pdf (oecd.org) Groupe de travail sur la sécurité dans l'économie numérique - Rapport : Page 76, ENCOURAGER LE TRAITEMENT DES VULNÉRABILITÉS Gestion, traitement et divulgation responsables des vulnérabilités, février 2021

[6] Coordinated Vulnerability Disclosure Policies in the EU - ENISA (europa.eu) ENISA, avril 2022 et National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf (oas.org) OAS, juin 2022

monde pour lutter plus efficacement contre les menaces transfrontalières pesant sur les données personnelles des individus et pour maintenir la stabilité du cyberespace.

Depuis l'apparition de la pandémie COVID-19, l'Assemblée mondiale de la protection de la vie privée (GPA) a commencé à se pencher plus en détail sur les menaces isolées de cybersécurité. Elle s'est notamment intéressée à des sujets tels que le << credential stuffing >> (bourrage d'dentité) et à la manière dont les entreprises de vidéoconférence (VTC) peuvent protéger leurs utilisateurs contre les menaces pesant sur les réunions en ligne.

Mais la GPA peut agir de manière plus large en promouvant et en créant une meilleure compréhension parmi ses membres de l'éventail des préjudices liés à la cybersécurité, à la fois individuels et sociétaux, en s'appuyant sur des recherches récentes effectuées par des membres individuels de la GPA.

Le plan de mise en œuvre stratégique 2021-2023 de la GPA a clairement mandaté[7] ses membres pour qu'ils identifient et examinent les sujets d'intérêt liés à la surveillance des citoyens et des consommateurs dans l'économie numérique et pour que le Groupe de travail sur l'application internationale de la loi et le Groupe sur l'économie numérique dirigent ces travaux avec le soutien d'autres acteurs.

La GPA a également demandé[8] à son Groupe de travail international sur l'application de la loi de continuer à surveiller les possibilités de coopération en matière d'application de la loi, en notant les risques numériques nouveaux et émergents qui menacent la vie privée des personnes. Les défis décrits dans cette résolution s'inscrivent dans le cadre du mandat actuel de ce plan stratégique.

Les activités décrites ci-dessous devraient être examinées et approuvées par le Groupe de travail international sur l'application des lois dans le cadre de son plan de travail 2023, afin de produire des résultats clairs et pratiques :

- Le Groupe de travail international sur l'application de la loi a évolué ces dernières années pour développer sa capacité à organiser des sessions à huis clos sur l'application de la loi, et actuellement, ce Groupe de travail est le mieux placé pour fournir un travail exploratoire d'ici 2023 sur les menaces de surveillance et les préjudices pour les individus et la société.

- Le Groupe de travail ne travaillerait pas de manière isolée, mais tiendrait plutôt compte des travaux pertinents menés par d'autres Groupes de travail de la GPA, comme l'examen actuel d'autres domaines d'intersection interréglementaire fait par le groupe de travail << Digital Citizen and Consumer Working Group >> (Citoyens et consommateurs numériques), et aussi consulterait plutôt le panel de référence des parties prenantes le cas échéant.

- La GPA devrait faire des efforts initiaux pour explorer les possibilités de coopération dans ce domaine. Il pourrait être utile que les autorités chargées de la protection des données et de la vie privée échangent des informations afin de lutter plus efficacement

[7] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org) Voir notamment la page 16.
[8] Comme ci-dessus, page 21.

contre la cyberactivité criminelle liée aux données personnelles des individus. Il peut s'agir d'explorer les domaines dans lesquels une action commune peut être entreprise pour mettre en lumière les problèmes auxquels les différentes juridictions sont confrontées simultanément. Cela permettra d'éviter la duplication des efforts dans les enquêtes des membres de la GPA.

- La GPA pourrait également, le cas échéant, s'engager dans le partage d'informations et explorer la coopération avec les organisations régionales et internationales qui traitent de la cybersécurité.

- L'Assemblée reste bien placée pour agir, compte tenu de la collaboration fructueuse qui s'est instaurée par le passé sur des questions isolées liées à des cyberincidents décrites ci-dessus. En l'occurrence, la GPA pourrait partager ses expériences ou comparer les modèles existants pour prévenir, atténuer ou éviter les dommages générés par les cybermenaces, contribuant ainsi au renforcement des capacités en matière de cybersécurité au niveau national. La GPA peut également aider à tirer parti des compétences techniques des grandes autorités au profit des membres disposant de moins de ressources pour ce domaine d'activité.

Ce travail de coopération internationale réalisé dans le cadre de la GPA peut contribuer à protéger les individus dans de multiples juridictions contre les préjudices économiques et psychologiques. Il peut également soutenir les efforts nationaux visant à conseiller les organisations en cas d'attaques par ransomware. Par exemple, lorsque les organisations sont privées de leurs propres données jusqu'à ce qu'une somme d'argent soit versée, ou bien d'autres conséquences économiques graves des attaques de la chaîne d'approvisionnement.

La GPA devrait déterminer, lors de la session fermée de 2023, s'il convient de poursuivre les travaux sur la cybersécurité et les menaces et préjudices liés à la surveillance. Il devrait s'appuyer sur les travaux exploratoires réalisés en 2022 conformément à la présente résolution. Tout travail supplémentaire serait réalisé dans le cadre du prochain plan stratégique de la GPA, qui doit être adopté en 2023.

FIN