48e séance à huis clos de l'Assemblée mondiale pour la protection de la vie privée (AMVP)

Novembre 2026

Résolution sur une intelligence artificielle agentique respectueuse de la vie privée

Cette résolution est soumise par le Groupe de travail sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle.

PARRAINEURS :

- Commissariat à la protection de la vie privée du Canada
- Autorité catalane de protection des données (Autoritat Catalana de Protecció de Dades)
- Commissariat à la protection de la vie privée et des données personnelles, Hong Kong, Chine
- Commission de protection des renseignements personnels, Corée
- Agence espagnole de protection des données (Agencia Española de Protección de Datos)
- Préposé fédéral à la protection des données et à la transparence, Suisse
- Commissariat à l'information, Royaume-Uni

COPARRAINEURS :

- Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, Canada
- Commissariat à l'information et à la protection de la vie privée de l'Ontario, Canada
- Contrôleur européen de la protection des données, Europe
- Commission nationale de l'informatique et des libertés, France
- Commissaire fédéral allemand chargé de la protection des données et de la liberté de l'information [BfDI]
- Commissaire à la protection des données de Rhénanie-Palatinate
- Commissaire à l'information de l'île de Man

À l'occasion de la 48e séance à huis clos de l'Assemblée mondiale pour la protection de la vie privée qui a eu lieu en 2026 :

Reconnaissant l'émergence et l'adoption croissante des agents d'intelligence artificielle (IA) et des systèmes d'IA agentique;

Entendant par « agent d'IA », selon la définition (en anglais seulement) de l'Organisation de coopération et de développement économiques (OCDE), une entité logicielle qui perçoit son environnement et agit sur celui-ci avec un certain degré d'autonomie, en utilisant au besoin des outils afin d'atteindre des objectifs précis et de s'adapter à l'évolution des données d'entrée et des contextes;

Entendant également par « système d'IA agentique », toujours selon la définition (en anglais seulement) de l'OCDE, un système composé d'un ou de plusieurs agents d'IA capables de décomposer des tâches, de collaborer au besoin et de poursuivre de manière autonome des objectifs complexes sur de longues périodes, conçu pour fonctionner dans des environnements physiques ou virtuels ouverts ou moins prévisibles et avec une supervision humaine minimale;

Reconnaissant que le principal élément sur lequel reposent la plupart des systèmes d'IA agentique actuels est un grand modèle de langage, que les défis en matière de protection des données inhérents à de tels modèles s'appliquent également aux systèmes d'IA agentique et que, la présente résolution étant fondée sur ce constat, certains éléments à considérer pourraient devoir évoluer si d'autres fondements technologiques de l'IA agentique venaient à se généraliser;

Reconnaissant également que certaines autorités de protection des données pourraient préciser davantage ces notions, notamment en définissant les systèmes d'IA agentique comme assurant une fonction d'orchestration, plutôt que de coordination, des agents d'IA;

Limitant la portée de la présente résolution aux systèmes et aux situations dans lesquels un système d'IA agentique traite les données personnelles d'un ou de plusieurs individus, y compris lorsque de tels systèmes sont utilisés pour prendre des décisions automatisées concernant ces individus ou pour prendre des mesures ayant une incidence sur eux;

Notant également que, bien que des outils permettant aux individus de créer des agents d'IA ou d'utiliser des systèmes d'IA agentique à titre personnel soient de plus en plus répandus, la présente résolution se limite à l'utilisation, au déploiement ou à la distribution d'agents d'IA et de systèmes d'IA agentique au sein des organisations publiques et privées et par celles-ci;

Ayant conscience qu'une approche centrée sur l'être humain à l'égard de l'IA pourrait procurer d'importants avantages pour l'économie, la société et l'intérêt public, notamment en favorisant la prospérité et en permettant de s'attaquer aux défis mondiaux urgents;

Insistant sur l'importance de veiller à ce que l'utilisation des systèmes d'IA respecte les droits de la personne (y compris le droit à la non-discrimination), soit équitable et licite, et prévienne les biais;

Reconnaissant que l'adoption de systèmes d'IA agentique pourrait accroître le risque de répercussions négatives importantes associées aux processus décisionnels automatisés, en particulier lorsque l'utilisation de tels systèmes réduit la supervision humaine, accentue le biais d'automatisation ou limite la possibilité pour les individus concernés de contester utilement les décisions prises à leur égard;

Soulignant que les organisations demeurent responsables des données personnelles traitées au moyen de systèmes d'IA agentique, y compris lorsque ce traitement est déclenché de façon autonome par des agents d'IA ou résulte de leur recours à des outils, à des compétences, à d'autres agents ou à des services connectés, et qu'elles ne devraient pas présumer que de tels systèmes reconnaîtront ou respecteront les règles organisationnelles, les attentes contextuelles ou les limites qui leur sont imposées;

Reconnaissant également que, lorsque des mesures de sécurité appropriées et démontrables sont en place, les systèmes d'IA agentique peuvent servir à renforcer les pratiques d'une organisation en matière de protection de la vie privée en rendant certains processus plus efficaces, plus uniformes et plus faciles à auditer, en appuyant l'exécution de tâches essentielles (comme le traitement des demandes d'accès présentées par les individus concernés) ou en réduisant la fréquence à laquelle des données sensibles sont mises à la disposition de membres de l'organisation, tout en veillant à ce que les décisions sensibles sur le plan juridique ou contextuel continuent de relever du jugement humain;

Reconnaissant l'importance de comprendre les caractéristiques propres aux nouvelles technologies ainsi que les distinctions qui les caractérisent, celles-ci pouvant donner lieu à de nouveaux défis en matière de protection de la vie privée et des données;

Reconnaissant que, bien que les systèmes d'IA agentique soulèvent des préoccupations nouvelles en matière de protection de la vie privée, ils soulèvent également, dans une large mesure, bon nombre des mêmes enjeux que les autres formes d'IA et que, par conséquent, les résolutions et déclarations existantes de l'Assemblée mondiale pour la protection de la vie privée (AMVP) demeurent pertinentes à cet égard, notamment la Déclaration sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle (40e AMVP), la Résolution sur la responsabilisation dans le développement et l'utilisation de l'intelligence artificielle (42e AMVP), la Résolution sur l'intelligence artificielle dans le contexte de l'emploi et la Résolution sur les systèmes d'intelligence artificielle générative (en anglais seulement) (45e AMVP), ainsi que la Résolution sur la collecte, l'utilisation et la divulgation de données personnelles pour préentraîner, entraîner et mettre au point des modèles d'IA (en anglais seulement) et la Résolution sur la surveillance humaine véritable des décisions prises à l'aide de systèmes d'IA (47e AMVP);

Soulignant également les travaux pertinents menés par d'autres réseaux d'autorités de protection des données, notamment l'Association francophone des autorités de protection des données personnelles et sa Résolution sur la gouvernance éthique de l'intelligence artificielle, les déclarations de la Table ronde des autorités de protection des données et de la vie privée du G7 sur l'IA générative, l'IA et les enfants et le rôle des autorités de protection des données dans la promotion d'une IA digne de confiance, ainsi que la Déclaration commune sur la mise en place de cadres de gouvernance des données fiables pour favoriser une intelligence artificielle innovante et protectrice de la vie privée, signée par 20 autorités de protection des données;

Insistant sur le fait que, en plus des facteurs relatifs à la protection de la vie privée énoncés dans les documents précités, les agents d'IA et les systèmes d'IA agentique peuvent engendrer, accentuer ou mettre en évidence des défis en matière de protection de la vie privée, notamment à l'égard des aspects suivants :

- **Utilisation dynamique des outils :** Les agents d'IA au sein d'un système d'IA agentique, ou les outils, capacités, modules d'extension et autres composantes auxquels ils ont recours ou font

appel, peuvent être conçus, fournis ou contrôlés par de multiples organisations et exploitants dont les pratiques en matière de protection de la vie privée, les modalités contractuelles et les mesures de sécurité peuvent varier, évoluer ou manquer de cohérence. En outre, alors que, dans un système d'IA traditionnel, l'utilisateur peut ne pas connaître à l'avance la logique qui sera appliquée pour parvenir à une conclusion, dans un système d'IA agentique, il peut également ignorer, dès le départ, à quelles composantes le système aura recours ou fera appel et, par conséquent, ne pas savoir comment les données personnelles circuleront entre les différentes parties. Cette situation est aggravée par la fragilité des approches adoptées par les systèmes d'IA agentique (c'est-à-dire que de légères modifications à une requête peuvent avoir des répercussions importantes sur leur fonctionnement). La situation pose des défis pour les organisations lorsqu'il s'agit d'assurer la responsabilité à l'égard du traitement des données, de gérer les transferts transfrontaliers de données, d'offrir une transparence suffisante quant aux pratiques relatives aux données et de veiller à ce que les individus puissent exercer efficacement leur droit à la vie privée. Le recours à de multiples outils crée également un risque d'inexactitudes en cascade, une erreur produite par l'un d'eux pouvant compromettre l'exactitude des résultats générés par les autres.

- **Mémoire :** Les agents d'IA peuvent conserver une « mémoire de travail », qui peut contenir l'historique de tâches antérieures (par exemple pour les aider à déterminer les étapes les plus efficaces afin d'exécuter des tâches similaires à l'avenir). Lorsque cette mémoire contient des données personnelles, elle peut engendrer des risques liés à l'inexactitude ou à la collecte excessive de données, à leur conservation au-delà de la période nécessaire aux fins visées ou à la manipulation de l'agent d'une manière qui compromet la confidentialité, l'intégrité ou la disponibilité de ces données. Lorsqu'un même agent d'IA est utilisé par plusieurs utilisateurs pour l'exécution de multiples tâches, le risque que des données personnelles conservées en mémoire soient communiquées involontairement augmente.
- **Accès aux données et pouvoirs délégués :** Les agents d'IA peuvent avoir accès à de multiples sources de données, interfaces, comptes ou systèmes dans l'environnement où ils évoluent. Ces éléments peuvent être internes ou externes, ou être accessibles au moyen d'outils. Cette situation exige que l'on détermine si l'agent n'accède qu'aux données et aux capacités minimales nécessaires à l'exécution d'une tâche; s'il traite inutilement des données sensibles; si les données personnelles mises à sa disposition pour une tâche donnée peuvent être combinées à d'autres données ou réutilisées à des fins différentes ou incompatibles, et, en particulier dans le cas de données externes, si les données mises à sa disposition sont suffisamment complètes, exactes et fiables pour satisfaire les fins visées. Il existe également un risque que des agents soient manipulés de manière à communiquer de façon inappropriée des données ou à permettre à des parties non autorisées d'accéder aux sources de données auxquelles les agents ont accès, à modifier des dossiers, à changer des autorisations, à communiquer avec des parties non autorisées ou à prendre d'autres mesures importantes non intentionnelles ou inappropriées. Chacune de ces situations est plus susceptible de survenir lorsque les composantes utilisées sont non sécurisées, compromises, obsolètes ou

assorties d'autorisations inappropriées. Enfin, les pouvoirs délégués à un agent peuvent rendre difficile la distinction entre les mesures prises directement par un utilisateur et celles exécutées de façon autonome par un agent d'IA.

- **Sécurité :** Le recours aux outils et l'accès aux données par les systèmes d'IA agentique élargissent le champ d'attaque, ce qui introduit ou amplifie des vulnérabilités en matière de sécurité. Un système d'IA agentique peut, par exemple, intégrer au contexte d'une étape ultérieure d'un processus des données provenant d'une source externe ou les résultats produits par un outil tiers, ce qui peut donner lieu à des attaques par empoisonnement de données ou par injection de requêtes. Les systèmes d'IA agentique qui ont un vaste accès aux données personnelles détenues par une organisation peuvent constituer des cibles particulièrement attrayantes pour de telles attaques. La capacité des systèmes d'IA agentique à prendre des mesures, notamment au moyen d'outils, engendre également des risques accrus en matière de sécurité, puisqu'un agent compromis disposant de privilèges au sein d'une organisation pourrait rapidement accroître la portée et les répercussions d'une atteinte. Les systèmes d'IA agentique pourraient également être mis à profit pour accélérer les cyberattaques ou en accroître l'efficacité.
- **Surveillance et examen par un humain :** Une caractéristique déterminante d'un système d'IA agentique est sa capacité d'influer sur son environnement ou de prendre des mesures de façon semi-autonome ou entièrement autonome. Ainsi, afin d'en maximiser les avantages ou les gains d'efficacité perçus, les organisations pourraient être tentées de limiter le nombre de fois où un système d'IA agentique interrompt son fonctionnement pour solliciter une intervention humaine, notamment sous la forme d'approbations. Cela peut à son tour réduire la capacité d'exercer une surveillance humaine véritable à l'égard des systèmes décisionnels fondés sur l'IA ou de permettre aux individus de demander efficacement l'examen par un humain d'une décision automatisée. Le caractère semi-autonome ou entièrement autonome des agents peut également faire en sorte qu'il soit difficile d'expliquer le processus par lequel un agent est parvenu à une conclusion ou à une décision, ou de confirmer la validité et la fiabilité de cette conclusion ou de cette décision.
- **Déploiement non autorisé ou non encadré :** Comme dans le cas des autres outils fondés sur l'IA, les membres d'une organisation peuvent croire que l'adoption de systèmes d'IA agentique leur permettra d'accroître leur productivité. La facilité d'accès grandissante à ces outils peut également inciter les individus à les déployer ou à les utiliser à des fins organisationnelles sans l'approbation ou la surveillance appropriées. Toutefois, contrairement aux systèmes d'IA plus traditionnels, dans lesquels un individu doit téléverser des données de manière proactive, la configurabilité des systèmes d'IA agentique ainsi que leur capacité à se connecter aux données, aux outils et aux systèmes d'une organisation peuvent exposer d'importantes quantités de données personnelles à des agents d'IA ayant peu ou pas de mécanismes de contrôle. Une telle utilisation peut avoir pour effet de contourner les politiques organisationnelles, les inventaires de données, les contrôles d'accès, les mesures de protection contractuelles et les mécanismes d'intervention en cas

d'incident, et d'exposer des données personnelles ou des systèmes internes à des agents, outils ou services externes non approuvés.

Reconnaissant que les organisations ont des obligations en matière de protection de la vie privée lorsqu'elles utilisent ou déploient des systèmes d'IA agentique, celles-ci devraient mettre en place des mesures fondées sur les risques afin de respecter ces obligations et d'atténuer les répercussions négatives des facteurs décrits précédemment. Voici quelques exemples de ces mesures :

- **Mettre en place des mécanismes appropriés d'examen et de surveillance** tout au long du cycle de vie d'un système d'IA agentique, depuis sa préparation et son déploiement jusqu'à son utilisation et son éventuelle mise hors service. Ces mécanismes pourraient comprendre des analyses d'impact relatives à la protection des données (AIPD) visant à garantir que les risques pour la vie privée sont recensés et atténués avant le déploiement; des audits techniques des systèmes d'IA agentique lors du processus d'approvisionnement ou avant leur déploiement; ainsi qu'une évaluation périodique de leur validité, de leur exactitude, de leur fiabilité et de leur pertinence. Ces mesures devraient être réexaminées régulièrement, ainsi qu'à la suite de changements importants, d'incidents ou de la découverte de nouvelles vulnérabilités. Des agents d'IA spécialisés pourraient également contribuer à la mise en œuvre de ces mesures.
- **Établir des limites appropriées à l'utilisation des systèmes d'IA agentique**, en fonction de la nature du traitement, de la sensibilité des données et des répercussions potentielles sur les individus. Dans certains cas, il pourrait s'agir de limiter les mesures ou les décisions prises par les systèmes d'IA agentique à celles dont les effets peuvent être annulés ou corrigés et dont les préjudices aux individus sont minimes ou inexistants.
- **Établir des politiques régissant l'accès des agents aux actifs de données ainsi que leur utilisation, leur conservation, leur suppression et leur communication**. Il pourrait s'agir de tenir des inventaires des données auxquelles un agent peut avoir accès; de limiter les circonstances dans lesquelles un agent peut accéder à des données sensibles, les utiliser ou les communiquer; de définir clairement les fins auxquelles les données personnelles peuvent être consultées, traitées ou utilisées par les systèmes d'IA agentique, en réduisant au minimum la quantité de données personnelles auxquelles un agent peut accéder à ces fins et en mettant en place des mesures de sécurité visant à empêcher toute utilisation de ces données à d'autres fins; de pseudonymiser les données avant qu'un agent d'IA puisse y avoir accès; de vérifier l'exactitude des données accessibles aux agents d'IA; de mettre en place des mécanismes appropriés de validation et de contrôle à l'égard des outils accessibles aux agents d'IA et d'encadrer la quantité ou la nature des données pouvant être communiquées à ces outils; ou encore de veiller à ce que les données personnelles traitées par l'agent d'IA ou le système d'IA agentique ne soient pas conservées plus longtemps que nécessaire. Il pourrait également s'agir de mettre en place des architectures de déploiement sécurisées adaptées à la nature du traitement et aux risques qu'il présente, notamment au moyen de mesures proportionnées visant à isoler ou à circonscrire les environnements d'exploitation des systèmes d'IA agentique, à limiter les accès réseau aux seuls accès nécessaires et à empêcher

qu'une défaillance ou une compromission n'ait des répercussions sur d'autres systèmes ou données. Enfin, les organisations devraient également mettre en place des mesures leur permettant de vérifier le respect de ces politiques et d'en évaluer l'efficacité.

- **Veiller à l'intégration des contrôles nécessaires** dans les agents d'IA et les systèmes d'IA agentique dès leur conception. Ces contrôles pourraient comprendre des mesures de protection de la vie privée dès la conception et par défaut qui facilitent l'exercice du droit à la protection des données (notamment des droits d'accès et de rectification); l'obligation pour l'agent ou le système d'IA agentique d'assurer une traçabilité de bout en bout (au moyen, par exemple, de registres des appels d'outils, des entrées et des résultats); le recours privilégié à des systèmes d'IA agentique dont le comportement est reproductible ou fiable; le partitionnement de la mémoire des agents selon les utilisateurs ou, lorsque cela est approprié, la désactivation du stockage en mémoire; l'établissement de points de décision ou d'intervention clés (y compris, au besoin, à des étapes intermédiaires du processus décisionnel avant qu'une mesure ne soit prise), où l'agent est tenu de solliciter une intervention humaine, ou l'imposition d'autres limites à l'autonomie des agents d'IA ou des systèmes d'IA agentique, ainsi que l'évaluation régulière de l'efficacité de ces mesures; ou encore la possibilité, pour les utilisateurs ou les exploitants, de suspendre ou d'interrompre l'exécution et, lorsque cela est faisable et raisonnablement possible, d'annuler des mesures prises ou de rétablir les systèmes et les données.
- **Mettre à l'essai les systèmes d'IA agentique et en assurer la surveillance en temps réel**. La mise à l'essai permet de garantir que les systèmes d'IA agentique se comportent comme prévu avant leur déploiement. Elle peut comprendre des essais fonctionnels, des essais menés par une équipe adverse afin de repérer les vulnérabilités, ainsi qu'une validation rigoureuse des mesures de sécurité, notamment les contrôles d'accès aux données, les mécanismes déclenchant une intervention humaine et les mécanismes de réversibilité. Après le déploiement, à mesure que les agents interagissent avec des environnements dynamiques en temps réel, y compris avec d'autres agents, des mesures devraient être mises en place afin de surveiller les comportements ou défaillances inattendus et d'en rendre compte.
- **Tenir des registres** suffisamment détaillés des décisions, des mesures prises, des appels d'outils, des entrées, des résultats et des interventions humaines pour appuyer la surveillance, les enquêtes et la reddition de comptes. Les mesures de journalisation et de traçabilité devraient elles-mêmes être conformes aux principes applicables en matière de protection des données et de la vie privée, notamment la minimisation des données, la limitation des fins, les contrôles d'accès, les mesures de sécurité et les périodes de conservation appropriées, sachant que les journaux peuvent contenir des requêtes ainsi que des données personnelles sensibles concernant des utilisateurs ou des tiers.
- **Assurer une gouvernance appropriée du déploiement, de la configuration et de l'utilisation des systèmes d'IA agentique au sein de l'organisation**. Il pourrait s'agir de désigner des parties responsables respectivement de la conception, de l'utilisation et des résultats du système d'IA agentique, et de tenir un inventaire à jour des systèmes approuvés et de leurs

finalités, modèles, outils, capacités, sources de données, connexions et autorisations; de détecter les déploiements non autorisés ou ayant subi des modifications importantes; d'établir des procédures permettant de détecter les incidents, d'enquêter sur ceux-ci et d'y réagir; et de mettre à jour les dossiers pertinents à la suite de changements importants.

- **Établir des mécanismes proportionnés de contestation, d'examen par un humain et de recours effectif.** Lorsqu'un système d'IA agentique prend, recommande ou exécute une décision ou une mesure qui produit un effet juridique et considérable sur un individu ou qui pourrait, de façon similaire, avoir une incidence importante sur lui, les organisations devraient offrir un moyen accessible de contester le résultat et d'obtenir un examen véritable de celui-ci par un décideur humain dûment qualifié et autorisé.
- **Mettre en œuvre des programmes de sensibilisation et d'éducation en matière d'IA adaptés aux différents rôles**, à l'intention des utilisateurs de systèmes d'IA agentique (ainsi que du personnel participant à la gouvernance, à l'approvisionnement et au déploiement de tels systèmes), des cadres supérieurs et des responsables de la protection des données, afin de veiller à ce que chacun de ces groupes possède les connaissances et les compétences nécessaires pour comprendre les capacités, les limites, les risques, les exigences en matière de gouvernance et les incidences sur la protection de la vie privée associées au déploiement et à l'utilisation des agents d'IA, ainsi que les responsabilités qui lui incombent dans le cadre de l'utilisation de systèmes d'IA agentique. Cela peut comprendre des connaissances propres à l'organisation, notamment les attentes ou les pratiques exemplaires relatives à la formulation des requêtes et à la définition des tâches confiées à un agent, les limites applicables aux types de tâches pour lesquels un agent peut être utilisé, ainsi que les exigences relatives à la documentation devant être conservée lorsqu'un agent est utilisé dans le cadre d'un processus décisionnel. De tels programmes pourraient également appuyer l'exercice d'une surveillance humaine véritable en permettant aux individus responsables de l'examen, de la validation, de la contestation ou de l'intervention à l'égard des décisions et des résultats produits par les systèmes d'IA agentique de le faire efficacement.
- **Aviser les individus concernés en temps opportun, faire preuve de transparence et fournir des explications utiles.** Les organisations devraient veiller à ce que les individus soient informés de façon claire, accessible et en temps opportun lorsqu'ils interagissent avec un agent d'IA, reçoivent des données générées par l'IA ou sont touchés par une décision ou une mesure prise par un système d'IA agentique ou qui repose en grande partie sur un tel système. Les données fournies devraient être proportionnelles à la nature du traitement et aux répercussions potentielles de celui-ci, et permettre aux individus de comprendre le rôle du système, les données personnelles utilisées, les principaux facteurs ou processus ayant mené au résultat pertinent, ainsi que la manière dont la responsabilité des mesures prises par le système peut être établie.

Dans le cadre de la 48e séance à huis clos de l'Assemblée mondiale pour la protection de la vie privée, il est donc convenu de ce qui suit :

1. Inviter les organisations à tenir compte des risques pour la vie privée énoncés dans la présente résolution lorsqu'elles conçoivent ou utilisent des systèmes d'IA agentique, et encourager celles qui conçoivent de tels systèmes à mettre au point et à mettre en œuvre des solutions novatrices pour relever les défis en matière de protection de la vie privée.

2. Par l'intermédiaire du Groupe de travail sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle de l'AMVP, poursuivre les travaux visant à enrichir et à mettre en commun les connaissances et les pratiques exemplaires en ce qui concerne :
    a. les facteurs relatifs à la protection de la vie privée qui sont associés aux systèmes d'IA agentique et les moyens de les atténuer;
    b. les cas dans lesquels des organisations ont déployé des systèmes d'IA agentique afin d'améliorer leurs pratiques en matière de protection des données;
    c. les moyens d'appliquer de façon efficace et prévisible les principes existants de protection de la vie privée aux systèmes d'IA agentique;
    d. les moyens par lesquels les autorités de protection des données peuvent favoriser le développement et l'utilisation responsables de l'IA agentique grâce à une approche réglementaire favorable à l'innovation, notamment par la création et l'exploitation de bacs à sable réglementaires.

3. Examiner la possibilité d'entreprendre d'autres travaux sur ce sujet, notamment l'élaboration d'orientations à l'intention des organisations qui souhaitent déployer des systèmes d'IA agentique ainsi que la réalisation d'activités de sensibilisation du public, dont l'élaboration d'orientations à l'intention des individus qui envisagent d'utiliser de tels systèmes.

4. Continuer de souligner l'importance d'intégrer la protection de la vie privée dès la conception des technologies nouvelles et émergentes, particulièrement lorsque celles-ci reposent sur le traitement de données personnelles.

FTC abstention: La Commission fédérale du commerce des États-Unis s'abstient d'adopter cette résolution.