Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Le Préposé

POST CH AG
CH-3003 Bern | EDÖB; EDÖB-A-AAB03401/1

À la Commission des Affaires Juridiques
du Conseil National

Services du Parlement
Palais du Parlement
3003 Berne

Votre référence:
Notre référence: EDÖB-A-AAB03401/1
Chargé(e) de dossiers: Petru Emanuel Zlatescu
Berne, 4 avril 2023

Motion d'ordre du 10.01.23 concernant le « contrôle des messageries instantanées »

Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants du 11 mai 2022

Madame la Présidente

Par courriel du 13 janvier 2023, vous avez demandé au Préposé fédéral à la protection des données et à la transparence (PFPDT) de répondre à plusieurs questions concernant le projet de règlement de la Commission européenne établissant des règles pour prévenir et combattre les abus sexuels sur enfants ("contrôle des messageries instantanées").

A. Remarques préliminaires sur le projet de règlement de l'UE

1. État des travaux législatifs

Le projet de règlement est une proposition législative de l'Union européenne (UE). Les présentes explications du Préposé se fondent sur les documents de la Commission Européenne, du Comité européen de la protection des données (EDPB) et du Contrôleur européen de la protection des données (CEPD) publiés dans le cadre du processus législatif. Il convient également de souligner que le processus législatif dans cette affaire n'en est qu'à ses débuts, qu'il laisse de nombreux points en suspens et que des modifications (fondamentales) peuvent encore être apportées au projet.

Feldeggweg 1
3003 Bern
Tel. +41 58 462 48 58, Fax +41 58 465 99 96
www.edoeb.admin.ch

2. Objectif, ampleur, autorités et procédures

a) Objectif et ampleur

Le projet soumet les fournisseurs de services d'hébergement et les fournisseurs de services de communication interpersonnelle à des obligations spécifiques de surveillance des communications privées de leurs clients, concernant

- la détection, le signalement, le blocage et le retrait du matériel connu et nouveau relatif à des abus sexuels sur enfants en ligne;
- ainsi que la sollicitation d'enfants (pédopiégeage).

b) Autorités

Le projet prévoit la création de nouvelles autorités pour mettre en œuvre les mesures prévues contre les abus sur enfants. Au niveau de l'UE, il est prévu de créer un centre chargé de prévenir et de combattre les abus sexuels sur enfants, dont le siège sera à La Haye, ainsi que des autorités de coordination dans les États membres, qui disposeront de pouvoirs de surveillance et d'enquête particuliers vis-à-vis des fournisseurs. Chaque autorité de coordination contrôle le respect des obligations par les fournisseurs soumis au règlement dans son domaine de compétence, notamment en surveillant l'Internet et en recevant les plaintes du public, y compris des enfants. Si une autorité de coordination constate qu'un fournisseur a enfreint les obligations prévues par le règlement, elle peut imposer des sanctions pouvant aller jusqu'à 6% des recettes annuelles.

c) Procédure de mise en œuvre de la surveillance

Les entreprises de télécommunications qui fournissent des services d'hébergement ou des fournisseurs de services de communication interpersonnelle, tels que les opérateurs de plateformes gratuites, sont tenues par l'injonction de procéder à des analyses complètes des risques d'abus sur les enfants et des mesures appropriées pour les réduire. Ils doivent présenter ces analyses à l'autorité de coordination compétente sous forme de rapport.

L'autorité de coordination du lieu d'établissement est habilitée à demander à l'autorité judiciaire locale de l'État membre ou à une autorité administrative indépendante désignée par ce dernier d'émettre une injonction de détection obligeant un fournisseur de services donné à mettre en œuvre des mesures de surveillance concrètes. Après consultation préalable du fournisseur sous obligation, du centre européen et, dans le cas de la surveillance concernant le pédopiégeage, de l'autorité compétente en matière de protection des données par l'autorité de coordination, l'autorité compétente décide de l'exécution de la surveillance. La surveillance de la distribution de matériel pédopornographique ne doit pas dépasser 24 mois et celle du pédopiégeage 12 mois.

Les fournisseurs de services ont la possibilité de contester l'injonction de détection par voie juridique. Ils doivent informer leurs utilisateurs de l'injonction de détection. Ces derniers peuvent également contester cette injonction en justice.

d) Obligation de signalement

Si un fournisseur a connaissance d'informations indiquant que des enfants pourraient être victimes d'abus sexuels sur Internet par le biais de ses services, il les signale immédiatement au Centre européen. Les signalements sont effectués via un système géré par ce dernier et comprennent :

- toutes les données de contenu sur les abus sexuels sur enfants en ligne, y compris les images et les vidéos;
- textes et messages vocaux ou transcriptions d'entretiens identifiés comme des sollicitations d'enfants (pédopiégeage).

Le Centre européen examine et traite les signalements des fournisseurs. Toutes les notifications qui ne sont pas manifestement infondées sont transmises par le Centre à Europol et aux autorités de poursuite pénale compétentes des États membres. En cas de transmission du signalement, le Centre informe le fournisseur que l'utilisateur concerné ne peut pas être informé.

3. Critique du EDPB et du CEPD

Dans leur avis commun du 28 juillet 2022, les deux institutions se sont montrées critiques à l'égard du projet, sans toutefois le rejeter dans son ensemble. Les deux organes de protection des données déplorent que :

- le projet est formulé de manière trop générale et parfois peu claire et laisse aux autorités une trop grande marge d'appréciation, ce qui ouvre la voie à des abus;
- la pertinence et l'efficacité des mesures de surveillance ne sont pas suffisamment prouvées;
- il faut s'attendre à ce que les technologies utilisées pour découvrir les informations pertinentes entraînent des taux d'erreur inacceptablement élevés;
- les mesures de détection du pédopiégeage et de la surveillance des communications vocales doivent être supprimées;
- les indications présentes dans le projet, selon lesquelles les fournisseurs assujettis doivent briser ou interdire le cryptage des communications en ligne, sont disproportionnées;
- l'échange de données prévu entre le centre de l'UE et Interpol doit se dérouler dans le cadre d'une transmission d'informations au cas par cas.

4. Appréciation du PFPDT

Le Préposé ne peut pas se prononcer sur les projets de l'UE. Il peut toutefois comprendre les observations du EDPB et du CEPD selon lesquelles le long texte juridique est peu précis, notamment en ce qui concerne des questions centrales telles que le traitement de données personnelles dans le cadre du pédopiégeage ou le cryptage de données.

Le projet visant à lutter contre les abus sexuels sur enfants en ligne vise à créer dans l'UE un réseau institutionnel complexe et complet de surveillance automatisée des communications privées, dont le fonctionnement est, selon l'estimation du Préposé, similaire à celui de la lutte contre le blanchiment d'argent. Comme le secteur financier, le secteur des télécommunications deviendrait, avec le règlement prévu, un auxiliaire de l'Etat, en ce sens qu'il devrait transmettre à leur insu, sur la base de processus automatisés, les données de communication privées de ses clients, y compris les messages de chat et les photos, à un bureau central de communication qui, après un triage, transmettrait une partie de ces informations aux autorités de poursuite pénale.

Si le projet se concrétise, le Préposé s'attend à ce que ce ne soit qu'une question de temps avant que le coûteux réseau institutionnel de l'UE contre les abus sexuels commis sur des enfants ne s'étende à d'autres infractions et phénomènes criminels. D'une part, parce que l'on observe déjà une telle extension dans la lutte contre le blanchiment d'argent, les objectifs d'utilisation de ce système étant complétés par des objectifs plus larges, tels que des objectifs fiscaux, et les catalogues des infractions préalables punissables étant élargis en conséquence. Et d'autre part, parce que toute recherche automatique de masse dans les communications privées conduit inévitablement à des découvertes fortuites dont l'exploitation est autorisée par le droit de procédure pénale à partir d'une certaine gravité.

B. Réponses aux questions de la Commission

I. Le projet de loi actuel de la Commission européenne comprend-il une éventuelle obligation pour les fournisseurs de surveiller leurs chaînes d'information en continu et de manière automatisée, sans soupçon initial ?

Par le biais d'une injonction de détection, les autorités de coordination obligent les fournisseurs privés à surveiller de manière généralisée les communications écrites, vocales et visuelles de leurs clients pendant une phase de plusieurs mois. Les mesures sont considérées comme automatisées, car elles passent par l'utilisation de logiciels de surveillance que le centre européen met à la disposition des fournisseurs assujettis. Il n'est pas nécessaire de disposer d'un soupçon initial à l'encontre de certains utilisateurs pour émettre une injonction de détection ou pour mettre en œuvre les mesures de surveillance.

II. Le projet de loi actuel de la Commission européenne comprend-il une obligation de transmettre les contenus interceptés par cette surveillance automatisée à un centre de l'UE ? Un recours juridique est-il prévu ? Qu'advient-il de ces notifications et des contenus ?

Tout fournisseur de services soumis au règlement est tenu de notifier les contenus concernés au Centre de l'UE. Si le Centre européen estime qu'une notification n'est pas manifestement infondée, il la transmet à Europol et à l'autorité nationale compétente en matière de répression.

En cas de non-transmission, les utilisateurs concernés sont informés a posteriori de la notification, ce qui doit être le cas au plus tard trois mois après le dépôt de la notification. Dans quelle mesure la notification au centre de l'UE peut elle-même faire l'objet d'une plainte ne nous est pas apparu clairement dans le projet de règlement.

Si un transfert a lieu, Europol et les autorités de poursuite pénale émettent généralement une ordonnance de confidentialité, de sorte que les utilisateurs concernés ne sont informés que dans le cadre de la procédure pénale, afin de pouvoir faire valoir leurs droits.

Pour les recours contre les injonctions de détection, voir ci-dessus (cf. ch. A.2. c. *in fine*).

III. Dans quelle mesure la Suisse, les habitantes et habitants ainsi que les fournisseurs de tels services seraient-ils concernés par la loi ??

Il faut partir du principe que le règlement vise à produire des effets extraterritoriaux.

Le projet prévoit que les fournisseurs de services concernés qui n'ont pas leur établissement principal dans l'UE doivent désigner un représentant légal dans l'UE, nécessaire pour recevoir, respecter et faire appliquer les injonctions rendues dans le cadre du règlement. Cela s'applique expressément aux injonctions de détection.

Il faut en outre partir du principe que les habitantes et les habitants de la Suisse seront concernés par des mesures de surveillance s'ils utilisent les services d'un fournisseur établi également dans l'UE. Nous ne pouvons pas déduire du texte de l'ordonnance dans quelle mesure cela sera aussi le cas pour les communications individuelles sans lien avec l'étranger.

Si Interpol transmet à fedpol des informations obtenues en vertu du règlement de l'UE, le PFPDT estime que les habitantes et les habitants de la Suisse doivent s'attendre à des poursuites pénales et à une utilisation des informations en Suisse, en raison de la double incrimination des abus sexuels sur les enfants.

IV. Quelles sont les conséquences d'une notification de contenus filtrés automatiquement à un centre de l'UE sur la charge de la preuve ?

Les contenus qui, selon le projet de règlement, sont automatiquement triés dans le cadre des injonctions de détection et transmis au centre de l'UE, sont transmis par ce dernier aux autorités de poursuite pénale, à moins qu'ils ne soient manifestement infondés. Cela a pour conséquence que les clientes et les clients concernés par une communication peuvent devenir des accusés dans une procédure pénale sur la base d'informations peu étayées.

Cette circonstance ne change cependant rien à la présomption d'innocence en faveur des prévenus dans la procédure pénale. En revanche, le tri automatisé et sans soupçon d'informations compromettantes par des fournisseurs privés est en contradiction avec le droit de leurs clientes et clients de ne pas devoir s'incriminer eux-mêmes dans une éventuelle procédure pénale. Cette tension est toutefois atténuée par le fait que les fournisseurs concernés par une injonction de détection doivent annoncer cette mesure à leurs clientes et clients avant que celle-ci n'entre en vigueur.

V. Est-ce que l'actuel projet de loi de la Commission européenne est compatible avec notre conception de la protection des données, nos lois et nos droits fondamentaux ?

Il faut tout d'abord noter que le projet de loi de la Commission européenne est maintenant examiné par le Parlement européen et le Conseil quant à sa compatibilité avec l'ordre juridique de l'Union européenne. Il reste à voir si le règlement prévu, après prise en compte des critiques des organes de protection des données de l'UE, résistera dans sa forme définitive à un éventuel examen par la Cour de justice de l'UE.

En tant que chef de l'autorité fédérale de surveillance de la protection de la sphère privée et de l'autodétermination informationnelle de la population suisse, le Préposé s'oppose par principe à ce que des entreprises privées surveillent systématiquement les communications privées de l'ensemble de leurs clientes et clients, indépendamment de tout soupçon.

Le Préposé n'ignore pas que la détection et la poursuite d'infractions graves, telles que le terrorisme ou les abus sexuels commis sur des enfants, représentent des intérêts publics importants, pour la réalisation desquels la surveillance des communications individuelles privées peut très bien s'avérer nécessaire, appropriée et conforme à la protection des données. Le Préposé est toutefois convaincu que, compte tenu de la nature de droit fondamental du droit à la vie privée et à l'autodétermination en matière d'information, la conformité à la protection des données de telles mesures présuppose qu'elles reposent sur une base légale formelle qui fait dépendre leur mise en œuvre d'une autorisation judiciaire au cas par cas (comme la loi fédérale sur le renseignement le prévoit également en ce qui concerne la surveillance par les autorités des communications individuelles de personnes à des fins de détection d'activités terroristes).

C'est avec plaisir que j'expliquerai plus en détail mes réponses dans le cadre de l'audition prévue.

Avec mes salutations les plus cordiales,

p.o Pleuger
Adrian Lobsiger