Siméon de Brouwer, membre de la commission Nouvelles Technologies et Vie privée de la Ligue des droits humains

ChatControl, ou “jusqu'où ira-t-on pour réduire le crime” ?

Tous les moyens sont-ils bons, pour prévenir ou résoudre un crime ? C'est la question que soulève la proposition de Règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants. **Cette proposition de Règlement européen vise à lutter contre les pédophiles qui approchent des enfants sur internet et/ou s'échangent des vidéos et photos (i.e. du ‘contenu') à caractère pédopornographique – le CSAM (pour** Child Sexual Abuse Material**). Un sujet lourd, ce qui pourrait laisser présumer que l'on sera prêt à tout supporter si c'est pour protéger les enfants. C'est justement sur ce (faux) dilemme que parie la Commission Européenne.**

INTRODUCTION

Cette proposition de Règlement est surnommée ‘**ChatControl**’ (*Surveillance des Correspondances*) car au nom de la protection en ligne des enfants contre les abus sexuels, elle permettrait au pouvoir exécutif d’imposer **la surveillance des communications privées par des algorithmes**, en chasse de conversations suspectes et de contenu illicite. Les droits à la vie privée, à la protection des données, à la confidentialité des communications, à la liberté d’expression et à l’information seraient impactés, certains dans leur essence même. Aucun garde-fou ne peut compenser ça.[1]

Se verrait imposer une “injonction de détection”, tout service numérique pour lequel il y a un risque important et non-atténuable d’être :

- utilisé pour échanger ou héberger des contenus représentant des abus sexuels sur enfants ;
- utilisé par des adultes afin de solliciter sexuellement des mineur·es (“pédo-piégeage”, ou *grooming* en anglais).
-

Concrètement, aucun service de communication (WhatsApp, Signal, email, forum, canal de communication dans un jeu vidéo, etc.) ou d’hébergement et de partage de fichiers (Drive, Dropbox, etc.) ne peut être exempt de ce risque. **Toute forme de communication inclut par définition le risque d’être le véhicule de contenu illégal.**

Sous l’injonction de détection, le dit service devrait alors mettre en place un algorithme scannant tous les messages et tous les contenus qui passent par lui. Dès qu’il détecterait du contenu ‘suspect’, l’algorithme le signalerait au fournisseur de service et aux autorités pour qu’iels l’examinent et, le cas échéant, prennent les mesures adéquates (enquête, poursuite pénale).
Cette approche techno-solutioniste a de nombreux problèmes, dont certains fondamentaux.

1 Pour plus d’information : https://edri.org/our-work/most-criticised-eu-law-of-all-time/

Les conséquences d'un taux d'erreur même minime

Le taux d'erreur des algorithmes augmente considérablement en fonction que ceux-ci recherchent du contenu connu[2], du contenu inconnu[3] ou du pédo-piégeage[4]. Rien qu'en Belgique, 8.3 milliards d'emails sont envoyés chaque jour en moyenne. Un taux de faux-positifs (signalements erronés) de même seulement 0.1 % résulterait en 8.3 millions d'emails envoyés aux autorités belges pour confirmation. Chaque jour. Sans compter les autres moyens de communication. Un raz-de-marée qui accaparerait toutes les ressources de la police, aux dépens des autres efforts.

De l'importance du contexte dans l'évaluation des échanges textuels

Un algorithme ne peut pas faire la différence entre une photo pédopornographique et un *selfie* échangé consensuellement d'un·e mineur·e à un·e autre, pas plus qu'un·e humain·e, sans contexte. Tout échange consensuel de photos dénudé.es entre mineur·es serait donc systématiquement envoyé aux autorités.

Le Centre, possible nid à problèmes

La proposition de Règlement inclut la création d'un nouveau Centre européen. Il hébergerait la base de données de contenu CSAM connu (sur base duquel sont comparés les nouveaux contenus), recevrait tous les signalements, et les transmettrait aux autorités nationales compétentes. Encore faut-il bien l'équiper, bien le protéger (cette base de données sera le sésame des pédophiles), bien le staffer (du personnel sain d'esprit et résilient, qui ne soit pas lui-même intéressé par le CSAM), qu'il soit indépendant du pouvoir exécutif (Europol étant friand et déjà coupable d'abus de collection de données) … De sérieux écueils à prendre en compte.

Le débat du chiffrement

Chiffrer ses communications de bout en bout est une pratique de cybersécurité banale qui permet qu'une correspondance ne soit lue par personne d'autre que son destinataire légitime. Ceux qui transportent le message ou l'interceptent n'ont pas la 'clé' pour le déchiffrer. Le chiffrement peut être appliqué aux communications (WhatsApp, Signal) comme au contenu hébergé (sur ordinateur, dans le nuage). Mesure de protection légitime voire obligatoire[5] (que ce soit pour se protéger des hackers, de la NSA, de l'espionnage politique ou industriel) et nécessaire pour tous ceux travaillant avec des informations sensibles, le chiffrement est aussi diabolisé car utile *aussi* aux criminels.

Dès que, pour s'attaquer à un problème sociétal, la solution proposée repose sur l'accès au contenu des communications, ça coince. La proposition de Règlement tente de contourner le problème en ne mentionnant pas explicitement les communications chiffrées, mais celles-ci tombent *de facto* sous le champ d'application. Les fournisseurs de services chiffrés auront une obligation de résultat, et devront donc affaiblir leur chiffrement, ou le contourner ('*client-side scanning*'), ce qui le rendrait postiche, impossible, ou inutile.

2 Comparer une photo non connue de l'algorithme avec une photo qui a été confirmée illégale.

3 Entraîner via le *machine learning* un algorithme a 'reconnaître' dans les photos les patterns typiques d'une scène d'abus sexuel sur enfant.

4 Entraîner via le *machine learning* un algorithme a 'reconnaître', dans des échanges textuels, les patterns typiques (i.e. les tournures typiques, ou les configurations comme le mensonge ou la mise sous pression) de pédophiles cherchant à rencontrer un enfant ou à obtenir des photos de lui/elle.

5 Le recours au chiffrement est explicitement permis dans la loi belge. Les entités visées par le futur *Règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union,* doivent aussi considérer son utilisation.

La question de la proportionnalité

Posséder/partager du CSAM et/ou pédo-piéger est un crime grave, mais il lui faut une réponse pertinente, et surtout proportionnée. On ne place pas un agent de police dans chaque foyer au nom de la protection des enfants (alors que 2/3 des abus sexuels sont commis au sein de la famille). La proportionnalité est le problème fondamental de cette proposition de Règlement. La solution qui est proposée par la Commission Européenne au problème du CSAM présente les mêmes problèmes que ceux posés par les lois de rétention des données, retoquées maintes fois déjà par la Cour de Justice. Si la proposition CSAM n'est pas adaptée à la lumière de cette jurisprudence-là, on peut s'attendre au même résultat, auquel cas **on aura juste perdu du temps à suivre une méthode dont on savait qu'elle menait à une impasse.** Le principe jusqu'à présent au cœur du raisonnement de la Cour de Justice est qu'**on ne met pas les gens sur écoute – que ce soit par des machines ou des personnes – juste parce que ça pourrait être utile**.

Aussi, difficile de ne pas déraper : une fois en place, ce mécanisme de détection serait facilement augmenté ou détourné. « Puisqu'il est là », on pourrait se dire : « pourquoi ne pas l'utiliser pour trouver les terroristes, les fraudeurs, ou les manifestants avant qu'ils n'agissent » ?

Surveiller pour mieux protéger ? Un faux dilemme, selon le Parlement Européen

En plus de tous les problèmes énoncés ci-dessus, on peut se demander : doit-on vraiment chaperonner de manière intrusive les enfants, pour bien les protéger ?
Le Parlement Européen a tranché d'une seule voix. Pour lui, la surveillance algorithmique devrait être ciblée sur celleux qui sont soupçonnés d'être pertinents pour le crime recherché. Les services chiffrés devraient être exemptés du champ d'application. Et surtout, l'autonomie, les compétences et la résilience des enfants face aux risques qu'iels courent devraient être mises en avant et renforcées : Les jeunes devraient bénéficier de sécurité accrue par défaut ; il devrait être plus difficile pour des inconnus de les contacter; iels devraient être plus sujet au contrôle parental ; des mécanismes devraient être mis en place pour leur fournir de l'aide ; quand du CSAM et/ou du pédo-piégeage est signalé aux fournisseurs de services, ceux-ci devraient avoir l'obligation de dûment et rapidement examiner ces signalements, pour les transmettre aux autorités le cas échéant. Il restera au Parlement de négocier avec le Conseil.

Le rôle crucial de la Belgique

Le Conseil de l'Union Européenne, qui rassemble les gouvernements des Pays Membres, n'a pas encore trouvé son mandat de négociation. Ce dossier est explosif, et trois présidences successives n'ont pas réussi à faire avancer le dossier sur les éléments de 'surveillance' et 'chiffrement.' La pression augmente d'un cran, avec l'adoption unanime par le Parlement de sa position.
La Belgique, qui assurera la prochaine Présidence du Conseil (1er janvier - 30 juin 2024), jouera un rôle clef pour débloquer et faire avancer le projet de loi au sein du Conseil. C'est à elle que reviendra la mission de clôturer un maximum de dossiers avant les élections du nouveau Parlement Européen (mai 2024) – qui coïncideront avec les élections belges.
Nous, électeur·ices belges, avons donc aussi un rôle, si nous voulons bien l'endosser : celui d'indiquer à nos ministres les dossiers qui nous tiennent particulièrement à cœur, et la direction que nous voulons les voir prendre. Contactons-les ! Six mois avant les élections, iels seront beaucoup plus enclins à nous écouter.
Il est rare pour les citoyens d'avoir autant d'influence sur le Conseil, l'institution européenne réputée pour être la moins transparente et démocratique.