

Commentaires formels du CEPD sur la consultation publique de la DG MARKT sur les procédures de notification des contenus illégaux hébergés par des intermédiaires en ligne, et sur la lutte contre ce phénomène

Le CEPD soutient l'initiative de la Commission visant à mieux définir et harmoniser les conditions d'application des procédures de notification et action. Il souligne toutefois que les procédures de notification et action doivent respecter les droits fondamentaux, y compris les droits à la protection des données et au respect de la vie privée, qui sont protégés notamment par les articles 7 et 8 de la Charte des droits fondamentaux de l'UE, l'article 16 du Traité sur le fonctionnement de l'UE et les directives 95/46/CE et 2002/58/CE.

Le CEPD souhaite contribuer à cette consultation publique en limitant ses commentaires uniquement aux domaines de la consultation qui ont trait aux droits à la protection des données et au respect de la vie privée, ou ayant une influence sur ces droits.

I. Catégories de contenu illégal concernées par les procédures de notification et action

Le CEPD estime qu'il est indispensable d'établir une définition plus harmonisée à l'échelle paneuropéenne de la notion de «contenu illégal» auquel les procédures de notification et action seraient applicables (**question 5**). Le CEPD souligne que les procédures de notification et action pourraient impliquer le traitement de données personnelles sensibles (par exemple des données relatives à des infractions), ce qui exige des garanties supplémentaires en termes de protection des données (conformément à l'article 8 de la directive 95/46/CE).

Les catégories énumérées à la question 5 n'ont pas toutes la même valeur et il serait plus judicieux d'adresser la procédure de notification et action à un hébergeur (**question 24**). Par exemple, les atteintes à la vie privée pourraient ainsi être mieux signalées aux autorités de protection des données (tout comme les infractions aux règles de protection des consommateurs pourraient être mieux signalées aux autorités compétentes et/ou aux associations nationales de défense des intérêts des consommateurs). Plusieurs types d'infractions nécessiteraient la collaboration des organismes chargés de l'application de la loi, par exemple en cas de contenu pédopornographique ou terroriste. De plus, le type d'action demandé aux hébergeurs dans ces cas-là devrait être défini plus clairement (par exemple, les conditions et les modalités de transfert de ces demandes aux autorités/organismes compétents).

II. Procédures de notification et action en Europe

Le CEPD reconnaît qu'il y a actuellement une fragmentation et une incertitude juridiques trop importantes pour les hébergeurs et les personnes chargées de la procédure de notification (**question 6**).

Le CEPD encourage la clarification de la notion d'«hébergement» (**question 8**), en tenant compte de l'environnement numérique et des intervenants actuels. Par la même occasion, le CEPD voudrait attirer l'attention sur le fait que la définition des activités considérées comme de l'«hébergement» pour déterminer les conditions d'application des dérogations en matière de responsabilité de la directive Commerce électronique ne devrait pas avoir de conséquences sur la responsabilité engagée par les prestataires de services énumérés à la question 8 conformément à la loi sur la protection des données. Bon nombre des activités envisagées à la question 8 impliquent le traitement de données à caractère personnel, certaines reposant sur ou générant le traitement intensif de données à caractère personnel à valeur ajoutée (par ex., les réseaux sociaux et les services «en nuage»). Dans ces cas, ces prestataires de services demeurent responsables du traitement des données à caractère personnel, conformément à la loi sur la protection des données.

Par conséquent, dans de nombreux cas, les hébergeurs peuvent être considérés comme des responsables du traitement conformément à la loi sur la protection des données, chargés d'assurer un traitement approprié des données. Par exemple, dans le cas des réseaux sociaux, les autorités européennes de protection des données ont conclu que, en concevant la plateforme et les outils pour le traitement de données à caractère personnel, les réseaux sociaux sont les responsables du traitement des données à caractère personnel sur leurs sites¹, bien que le contenu, qui comprend des données à caractère personnel, soit fourni par les internautes². Dès lors, les réseaux sociaux restent entièrement responsables, conformément à la loi sur la protection des données, du traitement des données à caractère personnel sur leurs sites, bien qu'ils ne soient pas les fournisseurs du contenu. De la même manière, les moteurs de recherche doivent être, dans une certaine mesure, considérés comme les responsables du traitement des données à caractère personnel qu'ils traitent puisqu'ils ont conçu ces moyens de traitement, à savoir les outils d'indexage et de référencement, pour fonctionner d'une certaine manière³.

III. Notification de contenu illégal aux hébergeurs

Le CEPD soutient la définition et la mise en place de procédures et d'un formulaire de notification de contenu illégal harmonisés à l'échelle de l'UE. Cette harmonisation permettra de réduire les disparités nationales et apportera davantage de certitude juridique pour toutes les parties prenantes.

Le CEPD recommande que les procédures tiennent pleinement compte des principes de confidentialité et de protection des données et que les aspects suivants soient abordés:

- la confidentialité de la personne à l'origine de la notification et des autres personnes impliquées (par ex., le plaignant, le suspect, les témoins, etc.);
- le traitement de leurs données personnelles à des fins de contrôle et ultérieurement (les données sont-elles conservées, pendant combien de temps?, les données sont-elles communiquées, à qui?);
- une manière transparente et facile de contester la décision d'un prestataire de service de retirer du contenu, et
- les modalités de la coopération avec les autorités chargées de l'application de la loi (quand, quoi, qui).

¹ Avis 5/2009 du Groupe de travail «Article 29» sur les réseaux sociaux en ligne, 12 juin 2009.

² Même si les internautes peuvent aussi être responsables dans une certaine mesure, par ex. au niveau de l'exactitude des données, surtout si leur utilisation des réseaux sociaux dépasse le cadre d'une utilisation privée.

³ Pour une analyse des responsabilités respectives, voir l'avis du Groupe de travail «Article 29» sur les aspects de la protection des données liés aux moteurs de recherche, 4 avril 2008.

Le respect de la loi sur la protection des données dans le cadre d'une notification est également extrêmement important pour protéger les contrevenants présumés, surtout dans les cas où il apparaît par la suite que ces personnes ont été accusées à tort ou ont fait l'objet de notifications abusives. Nous sommes d'avis que les notifications injustifiées ou abusives devraient faire l'objet d'une réglementation et de sanctions éventuelles, tout comme les personnes à l'origine de notifications abusives devraient également être tenues pour responsables, en vertu des règlements en matière de protection des données, de la transmission intentionnelle des données inexacts (**questions 13 et 14**).

La conception du formulaire doit suivre le principe de proportionnalité et limiter les informations personnelles requises aux fins de la notification au strict minimum. Il serait utile que ce formulaire contienne tout au plus, outre les coordonnées de la personne à l'origine de la notification, des réponses à choix multiple prédéfinies, et seulement quelques questions ouvertes ciblées (par ex., «fournir un URL»). Cela permettrait de garantir que seules les données à caractère personnel indispensables sont traitées. À cet égard, nous recommandons de remplacer la «*description détaillée de la nature illicite présumée du contenu*» (**question 12**) par des cases prédéfinies à cocher reprenant les types de contenu illégal possibles qui peuvent être signalés, parmi lesquels la personne à l'origine de la notification peut choisir.

IV. Action des hébergeurs contre le contenu illégal

Le CEPD note qu'il existe effectivement des cas où les autorités chargées de l'application de la loi doivent examiner plus attentivement le contenu illégal présumé dans le contexte d'enquêtes criminelles. Dès lors, le retrait de ce contenu pourrait limiter fortement leur enquête (**question 17**). La réponse à la question 17 est également liée à la classification du type de contenu illégal présumé faisant l'objet d'une notification (voir nos remarques au point I. ci-dessus). Il est également nécessaire d'examiner plus en détail la possibilité d'une meilleure classification des types de contenu illégal pouvant être signalés, ce qui pourrait permettre de distinguer les notifications nécessitant l'implication d'autres autorités/organismes (y compris les autorités chargées de l'application de la loi) des autres types de notification. Des étapes séparées et distinctes pourraient être envisagées en fonction du type de notification reçue, la notification invitant éventuellement les hébergeurs à bloquer l'accès alors qu'il serait plus judicieux (de préférence, après une procédure d'examen bien déterminée) de retirer le contenu dans certains cas spécifiques.

S'agissant des mesures proactives que doivent prendre les hébergeurs afin de prévenir les cas de contenu illégal, le CEPD souligne qu'il convient de clarifier les mesures proactives dont il est question (**question 22**). En dehors de la question d'exonération de responsabilité, le CEPD insiste sur l'importance de l'article 15 de la directive Commerce électronique qui indique clairement que les fournisseurs de service n'ont aucune obligation «*de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites*». La Cour de justice de l'UE a rappelé l'importance de ce principe à plusieurs reprises⁴. Il est, dès lors permis de s'interroger sur la légalité des types de mesures proactives réclamées aux hébergeurs en vertu de la directive Commerce électronique et de la directive sur la protection de la vie privée dans le secteur des communications électroniques, ainsi que sur la proportionnalité de ces mesures en vertu de la directive sur la protection des données.

⁴ Voir en particulier l'Affaire C-70/10, *Scarlet Extended SA contre la Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, arrêt du 24 novembre 2011, et l'Affaire C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, arrêt du 16 février 2012.

V. Le rôle de l'UE dans les procédures de notification et action

Le CEPD estime que l'UE doit jouer un rôle en contribuant au fonctionnement des procédures de notification et action, de préférence en adoptant des règles détaillées et harmonisées (du moins, quelques règles minimales contraignantes et quelques règles détaillées contraignantes) (**question 23**).

Bruxelles, le 13 septembre 2012