MiNET et ses obligations légales et juridiques

CONSERVATION DE DONNÉES, TRAITEMENT DE DONNÉES ET AUTRES OBLIGATIONS

Sommaire

- Obligations en tant que FAI
  - Conservation des données de connexion
  - Traitement de données personnelles (RGPD)
- Obligations en tant qu'hébergeur
  - LCEN ou Directive eCommerce
  - Directive Copyright
  - Règlement européen contre le terrorisme
  - Futur : Digital Service Act

Obligations en temps que FAI

Conservation des données de connexion

- France, Loi des postes et des télécommunications (article R10-13) :
  - Savoir qui utilise notre réseau à quel moment : conservation des adresses IP et ports utilisés avec horodatage
  - Ces données dites de connexion doivent être conservés pendant un an et accessibles sur demande de la justice
  - Les données de navigation (pages web visitées) ne sont pas et ne doivent pas être conservées !

Conservation des données de connexion

- Europe : c’est compliqué
  - Par défaut, contraire au droit européen (arrêts CJUE *Digital Rights*, *Télé2*, *FFDN*, *Estonie*) car surveillance généralisée et indifférenciée
  - Peut-être autorisé dans un cas très précis et exceptionnel :
    - Période limité
    - Menace grave pour la sécurité nationale
  - Mais il peut y avoir une conservation ciblée pour lutter contre la criminalité grave
  - Mais il peut y avoir une conservation rapide et généralisée en cas d’urgence pour lutter contre la criminalité grave

Conservation des données de connexion

- Mise en conformité du droit français avec le droit européen :
  - Le gouvernement a explicitement demandé au conseil d'Etat d'ignorer le droit européen
  - Arrêt du Conseil d'Etat :
    - Le gouvernement ne peut pas décider ce qui relève de la criminalité grave ou pas, c'est le rôle du juge
    - On ne peut donc pas faire de tri préalable, on ne peut le faire qu'a posteriori, donc on conserve tout en faisant appel à la conservation rapide et généralisée d'urgence
    - La durée de conservation d'un an est justifiée
    - Et vu qu'on a déjà conservé les données, on peut effectuer un accès a posteriori pour toute affaire juridique le nécessitant

Conservation des données de connexion

- A MiNET, on applique le droit français
  - Pas les moyens juridiques et financiers de remonter jusqu'à la CJUE
  - Conservation des adresses IP et ports utilisés par les adhérents avec horodatage
  - Accès uniquement sur demande la justice

Traitement des données (RGPD)

- Directive Européenne votée en 2016 et en application depuis le 25 Mai 2018
- S’applique à tout traitement de données personnelles sauf exception (fichiers de sécurité publique)
- S’applique dès qu’un utilisateur est européen
- S’applique aux personnes morales
- Donnée personnelle : toute information se rapportant à une personne physique

Traitement des données (RGPD)

- Principes :
  - Licéité : le traitement est légal
  - Transparence : information complète de l'utilisateur
  - Loyauté : les données collectées pour une finalité ne doivent pas être utilisées pour une autre finalité dans le futur
  - Proportionnalité : Le traitement de données doit se limiter à ce qui est strictement nécessaire au regard de la finalité poursuivie
  - Minimisation : les données personnelles ne sont conservées que le temps strictement nécessaire au traitement
  - Exactitude
  - Sécurité : obligation de moyens pour assurer l'intégrité et la confidentialité des données personnelles collectées

Traitement des données (RGPD)

- Le caractère licite du traitement :
  - La personne a consenti au traitement
  - Le traitement est nécessaire à l'exécution d'un contrat
  - Le traitement est nécessaire au respect d'une obligation légale
  - Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique
  - Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique
  - Le traitement est nécessaire aux fins des intérêts légitimes (et privés) poursuivis par le responsable du traitement ou par un tiers.

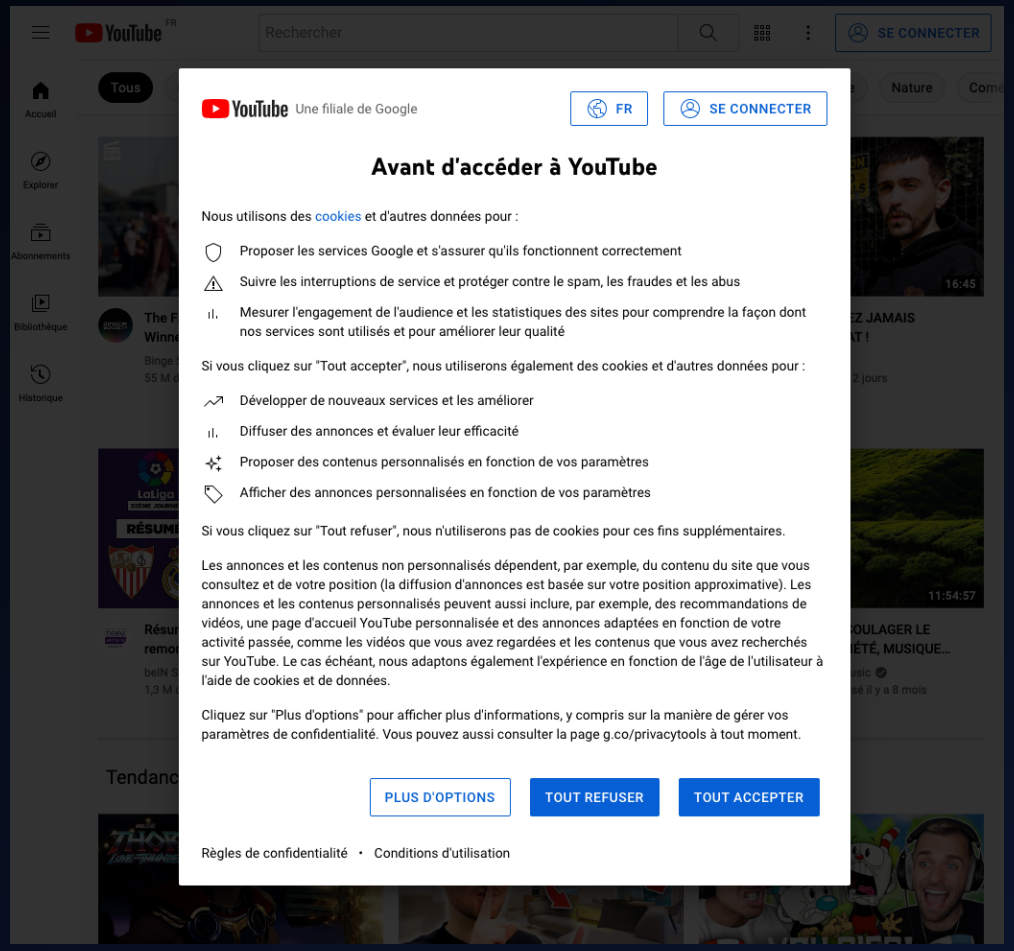
Traitement des données (RGPD)

- Le consentement comme base du traitement de données :
  - Libre : pas de contreparties à l'acceptation ou refus du traitement
  - Spécifique : chaque traitement doit faire l'objet d'un consentement
  - Eclairé : l'utilisateur doit être informé des données collectées et des finalités du traitement
  - Univoque : le consentement doit être donnée explicitement, il ne peut pas être obtenu par défaut

Traitement des données (RGPD)

- Application au cas des cookies :
  - Bouton « Tout accepter »
  - Bouton « Tout refuser » (en théorie ne doit pas être moins visible que le bouton « Tout accepter »)
  - Bouton « Personnaliser »
- Les cookies walls sont de ce fait théoriquement illégaux
  - La CNIL a dit en 2020 que c'était illégal mais le Conseil d'Etat a dit que la CNIL n'avait pas le pouvoir d'émettre une telle interdiction générale
  - Donc, à voir au cas par cas

Traitement des données (RGPD)



Traitement des données (RGPD)

- Cas des enfants de moins de 13 ans : il ne peuvent pas légalement consentir à un traitement de données, requiert une autorisation parentale
- Cas des données dites sensibles (opinions politiques et religieuse, orientation sexuelle, santé, etc.) : Interdiction de principe sauf dans certains cas :
  - En cas de consentement de la personne
  - En matière de sécurité sociale, protection sociale ou droit du travail.
  - Lorsque des intérêts vitaux sont en jeu,
  - Pour les associations à finalité politique, philosophique, religieuse ou syndicale,
  - Quand les données ont été rendues publiques par la personne
  - Dans le secteur de la justice
  - Si sont en jeu des « *motifs d'intérêt public importants* » qui doivent néanmoins respecter « l'*essence du droit à la protection de la donnée* ».
  - Dans le secteur de la santé (médecine, etc.)
  - Pour l'archivage, la recherche scientifique ou historique, etc.

Traitement des données (RGPD)

- Droits des personnes sur ses données personnelles :
  - Droit à l'accès et à la rectification
  - Droit à l'effacement et à l'oubli
  - Droit à la portabilité des données
  - Droit d'opposition
- Ces droits peuvent être limités par différents motifs (obligation légale, sécurité nationale, droit à l'information, etc.)

Traitement des données (RGPD)

- Sécurité des données collectées
  - Obligation de moyens et pas de résultat
- En cas d’accès non autorisé :
  - Notification aux autorités compétentes
  - Notification aux utilisateurs concernés

Traitement des données (RGPD)

- Sous-traitance :
  - Responsabilité de ce que font les sous-traitants
- Délégué à la protection des données (DPD/DPO) :
  - Obligatoire
  - Professionnel du droit
  - Doit être associé à tout traitement de données

Traitement des données (RGPD)

- Transfert des données en dehors de l'Union Européenne :
  - Par défaut interdit
  - Sauf si il y a un accord de l'UE avec un pays tiers pour confirmer que ce pays tiers offre le même niveau de protection
  - Sauf si l'entreprise apporte suffisamment de garanties sur le transfert des données en dehors de l'UE ie les clauses types

Traitement des données (RGPD)

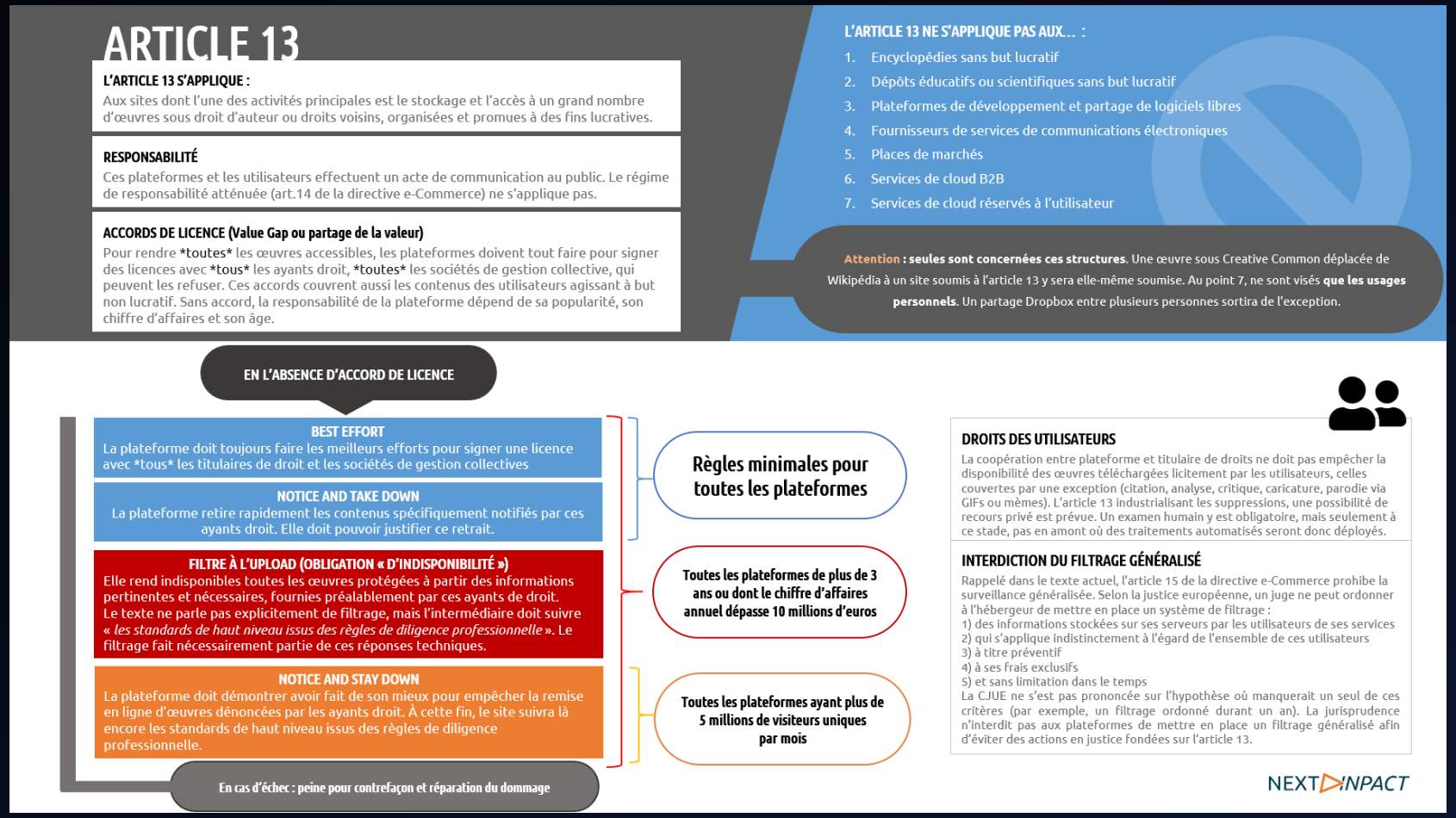
- Transfert des données vers les USA :
  - Historique :
    - Safe Harbor annulé par l'arrêt Schrems I
    - Privacy Shield annulé par l'arrêt Schrems II
    - Nouvel accord en cours de négociation -> annulation par l'arrêt Schrems III ?
  - En principe peut toujours s'appuyer sur les clauses types
  - Mais la CNIL a récemment jugé dans le cadre de l'utilisation de Google Analytics que les transferts vers les USA étaient illégaux par manque d'encadrement et de garanties des droits Européens sur le sol Américain
    - Peut potentiellement s'appliquer à tous les transferts vers les USA

Obligations en tant qu’hébergeur

LCEN/Directive eCommerce

- Obligations en tant qu'hébergeur :
  - L'hébergeur n'est pas responsable du contenu qu'il héberge a priori
  - Il devient responsable civilement s'il a été notifié de la présence de contenu **manifestement** illégal sur ses serveurs et qu'il ne l'a pas retiré
- Concrètement :
  - Il faut avoir mis en place un mécanisme de notification de contenu manifestement illégal et traiter rapidement les notifications qui peuvent arriver

Directive Copyright



Arrêt de la CJUE du 26/04/2022 peut potentiellement changer des choses

Directive Copyright

- Article 15 sur les droits voisins des articles de presse :
  - Il faut payer une licence pour pouvoir utiliser des titres de presse
  - S’applique à tous sauf aux usages individuels non commerciaux, si juste le lien est posté ou si juste un très court extrait est posté
  - Vise à l’origine Google News mais concerne dans les faits tout le monde, dont Wikipédia par exemple

Règlement européen contre le terrorisme

- Mise en place de mesures proactives pour lutter contre la mise en ligne de contenu faisant l'apologie du terrorisme
- Obligation de transparence sur ses mesures proactives
- Retrait dans l'heure sous notification des autorités compétentes de contenu faisant l'apologie du terrorisme
- Conservation du contenu retiré pour un possible traitement a posteriori par la justice

Futur : Digital Service Act

- Futur réglementation Européenne en cours de discussion au Parlement Européen (accord de principe le 25/04/2022)
- Refonte de la directive eCommerce qui date de 2001
- Pas de changements si on reste un acteur passif :
  - Simple transport de données
  - Caching
  - Hébergeur
- Micro et petite entreprise exemptée de certaines obligations

Futur : Digital Service Act

- Changements :
  - Obligation de transparence sur les retraits de contenus (nombres, type, origine de la demande de retrait, etc.)
  - Simplification de la procédure de notification
  - Il faudra informé l'utilisateur à l'origine de la notification de l'issue de sa notification (rien, retrait, blocage de l'utilisateur, avertissement de l'utilisateur, etc.)
  - Notification de l'utilisateur concerné par le retrait ou le blocage avec exposé des motifs et possibilités de recours
  - Obligations renforcées pour les très grandes plateformes de plus de 45 millions d'utilisateurs actifs mensuels (10% de la population de l'EU)

Conclusion

- C’est compliqué
- Internet n’est pas un espace de non-droit
- S’il faut retenir quelque chose : le RGPD

Bibliographie

- Conservation des données de connexion
  - https://www.nextinpact.com/article/44019/conservation-donnees-connexion-justice-ue-siffle-fin-match-ou-presque
  - https://www.nextinpact.com/article/12018/86929-pourquoi-directive-sur-conservation-donnees-est-invalidee
  - https://www.nextinpact.com/article/45613/comment-conseil-detat-a-sauve-conservation-donnees-connexion
  - https://www.nextinpact.com/article/24897/102607-la-cjue-s-oppose-a-obligation-generalisee-conservation-donnees-connexion

Bibliographie

- RGPD
  - https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679
  - https://www.nextinpact.com/article/28043/106135-le-rgpd-explique-ligne-par-ligne-articles-1-a-23
  - https://www.nextinpact.com/article/28047/106168-le-rgpd-explique-ligne-par-ligne-articles-24-a-50
  - https://www.nextinpact.com/article/28052/106169-le-rgpd-explique-ligne-par-ligne-articles-51-a-99
  - https://www.cnil.fr/fr/cookie-walls-et-monetisation-des-donnees-personnelles-les-enjeux-juridiques-et-ethiques

Bibliographie

- RGPD transfert vers les USA :
  - https://www.nextinpact.com/article/19497/96763-la-cjue-invalide-safe-harbor-americain-quelles-consequences
  - https://www.nextinpact.com/article/30416/109182-retour-sur-invalidation-privacy-shield-par-justice-europeenne
  - https://www.nextinpact.com/article/68834/vers-nouvel-accord-pour-transfert-donnees-entre-lue-et-etats-unis
  - https://www.nextinpact.com/article/49790/pour-cnil-aussi-transferts-internationaux-google-analytics-sont-illegaux
  - https://www.nextinpact.com/article/49870/google-analytics-retour-sur-mise-en-demeure-cnil

Bibliographie

- LCEN/directive eCommerce
  - https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000801164
  - https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex%3A32000L0031
- Directive Copyright
  - https://www.nextinpact.com/article/29250/107705-directive-droit-dauteur-notre-schema-pour-comprendre-larticle-13
  - https://www.nextinpact.com/article/29123/107530-pour-senat-sites-doivent-payer-editeurs-pour-reprise-darticles-presse
  - https://www.nextinpact.com/article/29318/107791-la-directive-droit-dauteur-passe-definitivement-cap-europeen
  - https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32019L0790

Bibliographie

- Règlement européen contre la diffusion du terrorisme en ligne
  - https://fr.wikipedia.org/wiki/R%C3%A8glement_europ%C3%A9en_contre_la_diffusion_du_terrorisme_en_ligne#Principales_dispositions
  - https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2021.172.01.0079.01.FRA
- Digital Service Act
  - https://www.nextinpact.com/article/45070/le-digital-services-act-explique-ligne-par-ligne-article-1-a-24
  - https://www.nextinpact.com/article/45249/le-digital-services-act-explique-ligne-par-ligne-article-25-a-74