Legal Update

« Ouais, ben si vous vouliez du captivant, fallait peut-être me faire lire autre chose que des textes de lois ! »

Alexandre Archambault

Suivre @AlexArchambault

FrNOG 28

Un ~~dé~~enchainement de mesures sécuritaires

- **Printemps 2016 : <u>Procédure pénale / lutte contre le crime organisé et le terrorisme</u>**
  - ✓ extension au Judiciaire des moyens accordés au renseignement, encadrement chiffrement, délit de contournement de blocage, délit de consultation habituelle

- **Lois de prolongation de l'état d'urgence**
  - ✓ <u>Loi n°2016-629 du 20 mai 2016</u> (2 mois)
  - ✓ <u>Loi n°2016-987 du 21 juillet 2016</u> : 6 mois + extension du périmètre des « Boites Noires » (constituant une menace ➪ susceptible d'être en lien avec une menace + entourage)
  - ✓ <u>Loi n°2017-1767 du 19 décembre 2016</u> : jusqu'au 15 juillet 2017

- **Février 2017 : <u>Loi Sécurité Publique</u>**
  - ✓ Rétablissement délit de consultation habituelle suite à sa censure par le Conseil Constitutionnel

Réforme procédure pénale

- Texte définitivement adopté : Loi n° 2016-731 du 3 juin 2016
  - ✓ Extension des IMSI-Catchers au judiciaire (art. 3 ➠ Art 706-95-4 à 706-95-10 CPP)
  - ✓ Techniques spéciales d'investigation dès l'enquête préliminaire : interceptions (Art. 706-95 CPP), keyloggers (art. 5 ➠ Art 706-102-1 à 706-102-3 CPP), saisie contenus / webmail stockés (art. 2 ➠ Art 706-95-1 à 706-95-3 CPP)
  - ✓ Obligation de communiquer les données chiffrées (Art.16 ➠ Art. 434-15-2 Code pénal)
  - ✓ Pénalisation mesures de contournement blocage & délit de consultation habituelle de sites pas bien (Art. 18 ➠ Art. 421-2-5-1 & 421-2-5-2 Code pénal)
    - Délit consultation habituelle censuré par C. Const en février 2017
    - Mais rétabli dans la foulée (Loi n°2017-258 relative à la sécurité publique)
  - ✓ Recours obligatoire à la PNIJ pour réquisitions & interceptions (Art. 88)
  - ✓ Rejet en cours de débat de l'aggravation (2 ans & 15 000 €) sanction en cas de non réponse à réquisition (Actuellement 3 750 €, Art. 60-1 & 60-2 CPP)

C'est encore la faute à l'Europe !

- Première salve : invalidation Directive 2006/24/CE en 2014
  - ✓ La CJUE n'a toutefois pas remis en cause le principe même de conservation des données de connexion
  - ✓ Pour le Gouvernement Français, cette invalidation est sans impact au cadre national
  - ✓ Ou pas

- Seconde salve : Arrêt Tele2 du 21 décembre 2016
  - ✓ Cette fois-ci, la CJUE censure tous les dispositifs nationaux non bornés de conservation des données de connexion

L'arrêt Tele2 Sverige

- A la suite de l'invalidation Directive 2004/24/CE, un opérateur Suédois et des Parlementaire Britanniques ont contesté leur législation nationale

- La CJUE leur donne raison
  - ✓ La conservation des données de connexion reste soumise au respect de la Charte des droits fondamentaux
  - ✓ La dérogation prévue à l'art.15 de la Directive 2002/58/CE doit rester une exception, et ne saurait devenir la norme
  - ✓ Uniquement « à des fins de lutte contre la criminalité grave »
  - ✓ L'accès aux données conservées doit faire suite à une décision issue d'un contrôle préalable et indépendant
  - ✓ Données stockées sur le territoire de l'Union
  - ✓ Information des personnes dont les données sont sollicitées

Une refonte au niveau Européen

- GDPR/RGPD (Tous secteurs)
  - ✓ Règlement général sur la protection des données, publié en mai 2016
  - ✓ Règlement > Directive
  - ✓ D'application directe à compter 25 mai 2018

- Proposition de règlement ePrivacy (Secteur Telecom)
  - ✓ En cours de discussion, calendrier optimiste pour une entrée en vigueur en 2018

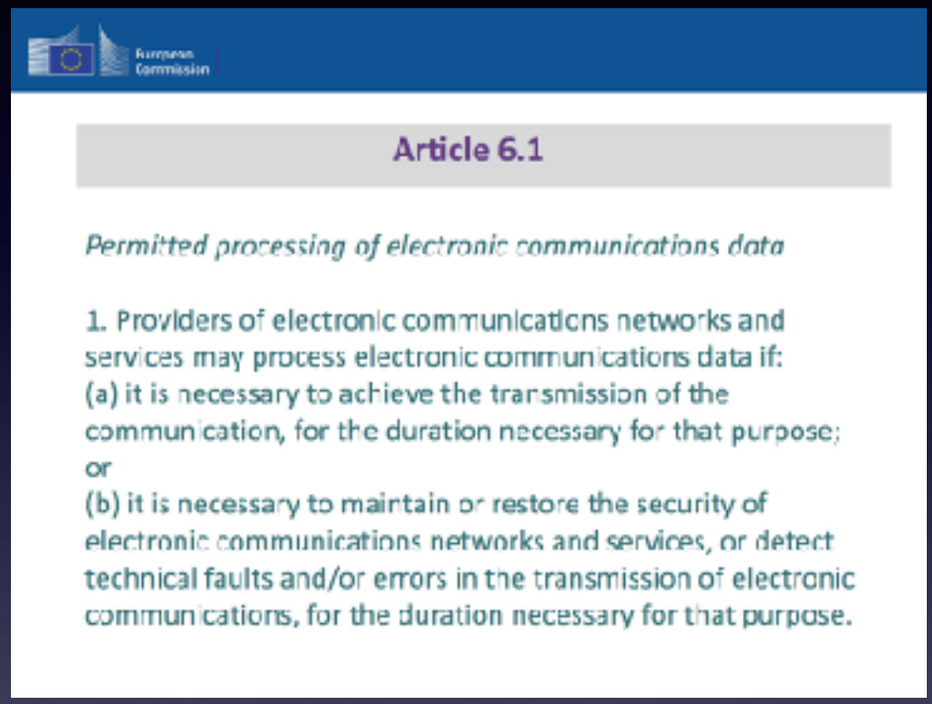
Focus sur ePrivacy

- Texte spécifique aux communications électroniques
  - ✓ Vise à remplacer Directive 2002/58/CE actuellement en vigueur
  - ✓ Règlement : s'applique d'autorité
    - ➡ date prévue : 25 mai 2018 (pour se caler sur GDPR)

- Des nouveautés par rapport à la Directive actuelle
  - ✓ Les services OTT (messagerie, VoIP…) sont désormais concernés
  - ✓ Un véritable statut pour les métadonnées
  - ✓ Gestion des cookies

ePrivacy - Métadonnées

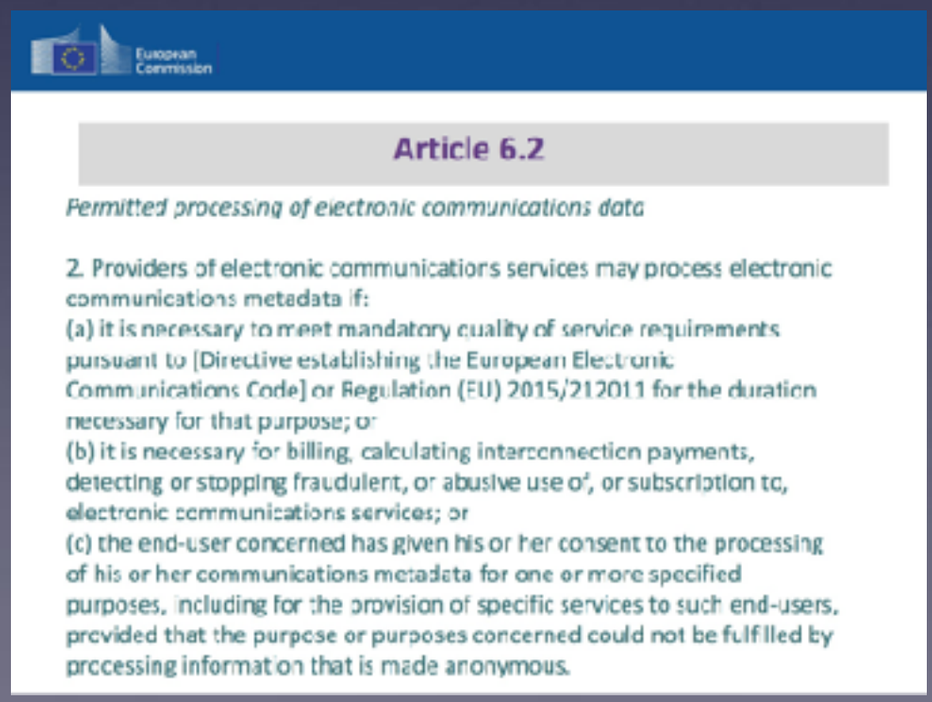
- Actuellement : Données de connexion / Données de localisation
- Avec le règlement, une seule catégorie unifiée : les métadonnées
  - ✓ traitement possible si nécessaire à l'acheminement d'une communication ou à sa sécurité / QoS / facturation
  - ✓ données liées au terminal (IMEI, IMSI, …) possible si nécessaire à l'acheminement / sécurité / QoS ou si accord utilisateur (art. 8.2)
- La pertinence d'une métadonnée peut varier d'un acteur à l'autre (cf. URL)



Article 6.1

Permitted processing of electronic communications data

1. Providers of electronic communications networks and services may process electronic communications data if:
(a) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
(b) it is necessary to maintain or restore the security of electronic communications networks and services, or detect technical faults and/or errors in the transmission of electronic communications, for the duration necessary for that purpose.

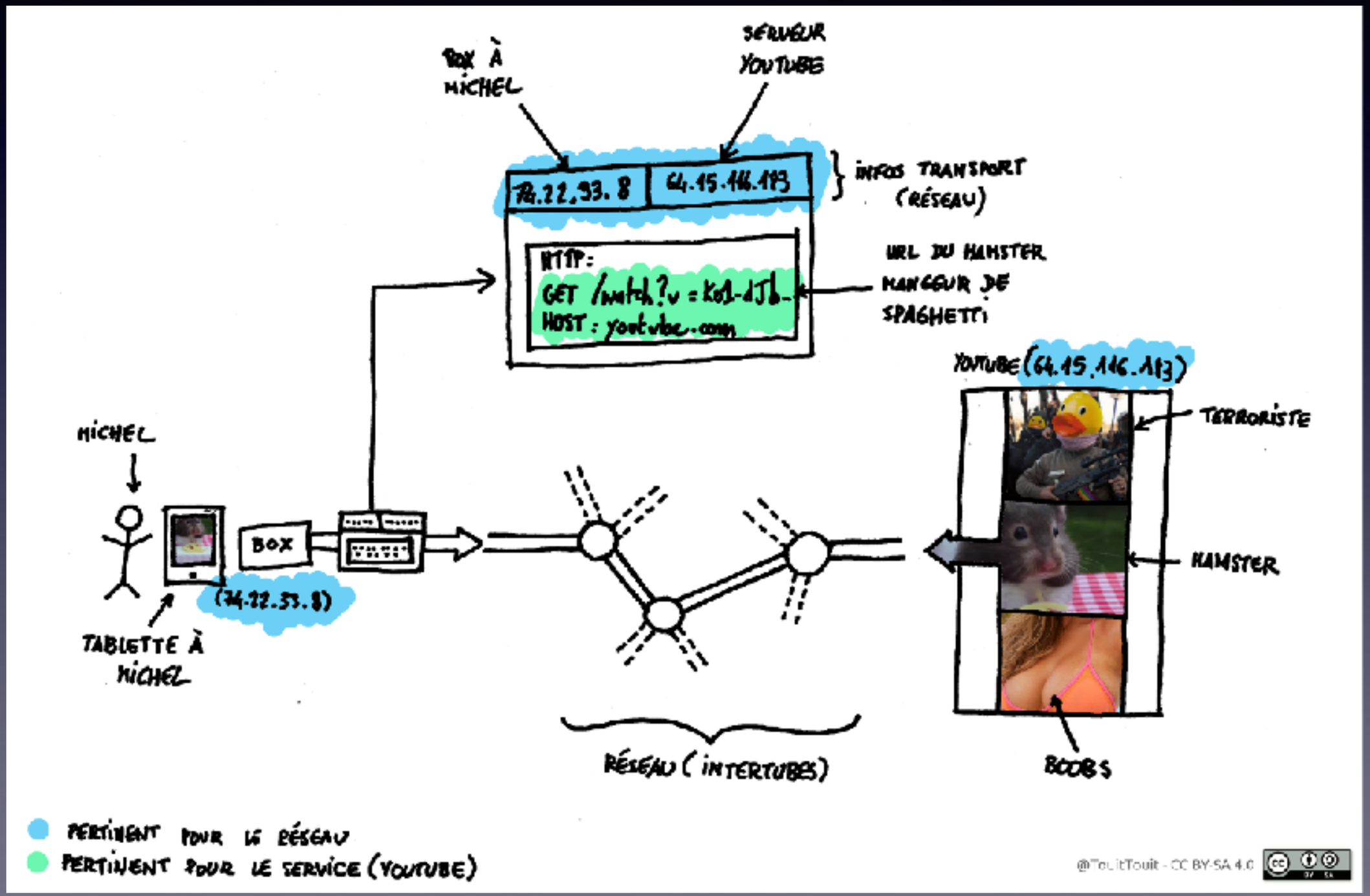


Article 6.2

Permitted processing of electronic communications data

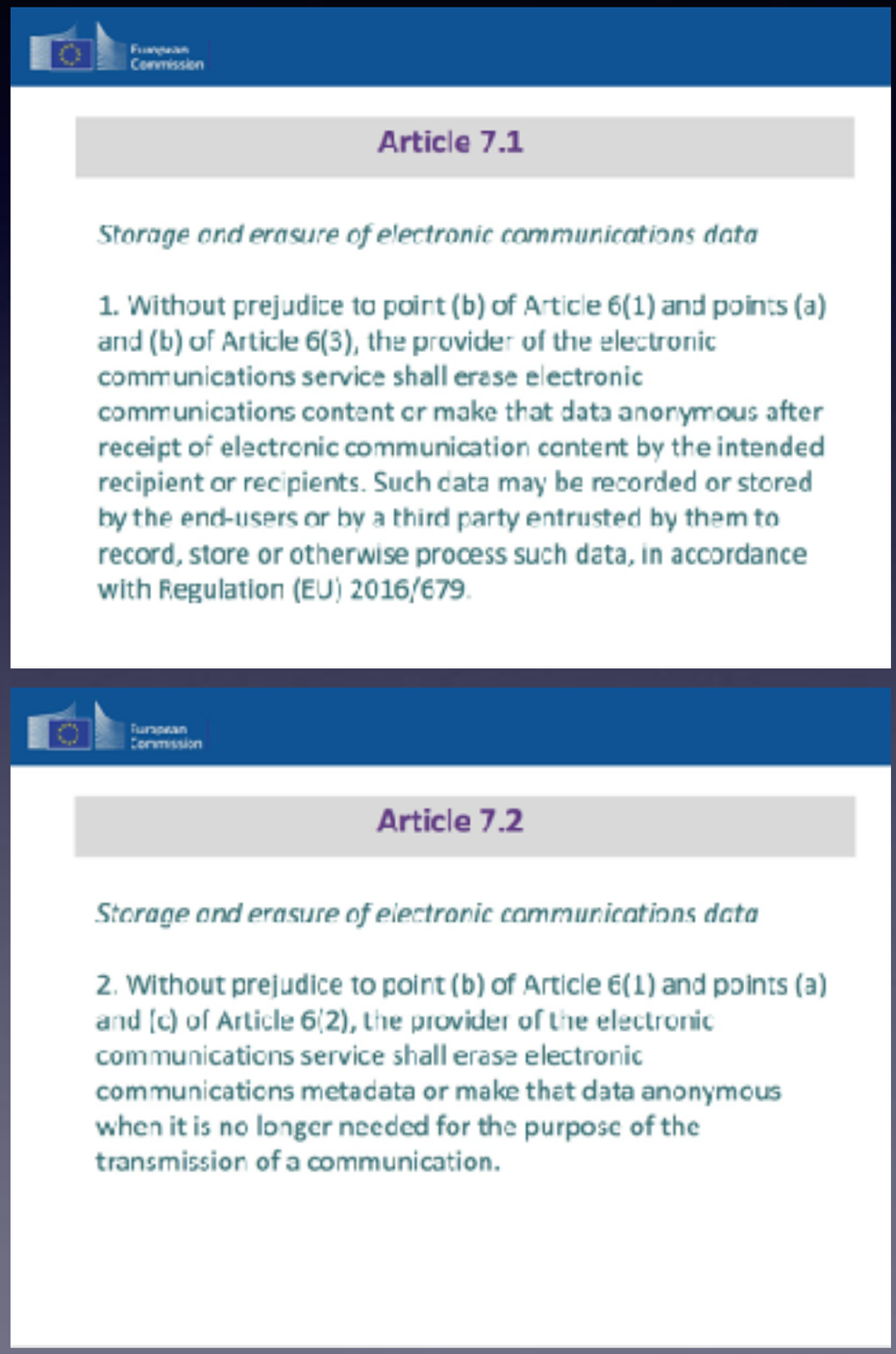
2. Providers of electronic communications services may process electronic communications metadata if:
(a) it is necessary to meet mandatory quality of service requirements pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/212011 for the duration necessary for that purpose; or
(b) it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services; or
(c) the end-user concerned has given his or her consent to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous.

URL est-elle une donnée de connexion / métadonnée ?



ePrivacy - Métadonnées

- Les métadonnées doivent être anonymisées ou effacées une fois la communication accomplie
- Les données liées au terminal (MAC, IMEI, IMSI…) ne peuvent être traitées et conservées (art. 8.2)
- Exceptions :
  - ✓ pour des motifs liés à la sécurité, à l'ordre public, ou divers aspects techniques ;
  - ✓ consentement de l'utilisateur final



European Commission

Article 7.1

Storage and erasure of electronic communications data

1. Without prejudice to point (b) of Article 6(1) and points (a) and (b) of Article 6(3), the provider of the electronic communications service shall erase electronic communications content or make that data anonymous after receipt of electronic communication content by the intended recipient or recipients. Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with Regulation (EU) 2016/679.

European Commission

Article 7.2

Storage and erasure of electronic communications data

2. Without prejudice to point (b) of Article 6(1) and points (a) and (c) of Article 6(2), the provider of the electronic communications service shall erase electronic communications metadata or make that data anonymous when it is no longer needed for the purpose of the transmission of a communication.

ePrivacy : Cookies

- Remplacement des bandeaux en page d'accueil par un consentement (opt-in) via le navigateur (art. 9)
  - ✓ Susceptible d'évoluer au gré des discussions & compromis (cookies audience vs cookies tracking)

- Les éditeurs de navigateurs doivent proposer une option permettant d'interdire l'utilisation de cookies tiers (art.10)

- Pas d'interdiction du « cookie wall »
  - ✓ Point susceptible d'évoluer au gré des discussions & compromis
  - ✓ En France CNIL très critique sur cette disposition

ePrivacy : autres dispositions

- passage d'un opt-out à un opt-in pour les annuaires (art. 15)
- présentation et restriction de l'identification des lignes appelante, blocage des appels entrants (art. 12 & 14) ;
- traitement des communications non sollicitées (art. 16)
- amendes administratives
  - ✓ jusqu'à 4 % du chiffre d'affaires annuel (harmonisation avec RGPD)

Conduite à tenir en cas de réquisition / décision de justice

- **Ne jamais faire le mort et toujours accuser réception**
  - ✓ défaut de réponse sanctionné au niveau pénal
  - ✓ pour ceux qui disposent d'un service juridique, les mettre dans la boucle
  - ✓ prendre attache avec l'OPJ / magistrat pour lui expliquer (avec des mots simples) ce qui est possible, ce qui n'est pas possible
  - ✓ si réquisition internationale, renvoyer poliment vers OCLCTIC / BEFTI qui assurent l'interface (pas de sollicitations directes)

- **En cas de décision de justice, consulter d'urgence son avocat,** de préférence rôdé aux communications électroniques & procédures civiles / pénales
  - ✓ par exemple pour obtenir une rétractation ordonnance art. 145 Code de procédure civile (perquisition civile) portant sur des éléments hors périmètre

Conduite à tenir en cas de Droit de Communication

- **<u>Ne jamais faire le mort et toujours accuser réception</u>**
  - pour ceux qui disposent d'un service juridique, les mettre dans la boucle
  - prendre attache avec le service enquêteur pour lui expliquer (avec des mots simples) ce qui est possible, ce qui n'est pas possible
  - transmettre les éléments sollicités ne posant pas problème
  - solliciter CNIL pour obtenir un avis sur les éléments pouvant poser problème (tel que l'impact de l'arrêt <u>CJUE Tele2 Sverige</u> qui semble exclure le droit de communication)

- Si visite sur site, vérifier que le délai de prévenance a été respecté
  - accueillir poliment les visiteurs, les faire patienter le temps que service juridique / avocat rapplique
  - s'abstenir de tout jugement de valeur mais ne pas hésiter à faire porter au procès-verbal toute réserve utile

Des questions ?