Obligations légales. Reloaded

Retour sur 18 mois de lois sécuritaires impactant le Numérique

Alexandre Archambault

Suivre @AlexArchambault

FrNOG 26

ALLO UI CER BERNARD

- Je veux que tu bloques http://www.facebook.com/mechant_barbu_pas_tres_charlie
- Mes équipes de Levallois voudraient savoir qui est derrière 10.0.0.66 ?
- Je t'envoie les amis du petit-déjeuner pour perquisitionner le DarkNet dans ton DataCenter
- Sois Charlie, adopte une BoiteNoire
- Tu chiffres, c'est mal, tu es un complice des méchants du Darkweb

Un ~~dé~~enchainement de mesures sécuritaires

- **Novembre 2014 : Loi renforçant l'efficacité lutte contre terrorisme**
  - ✓ Blocage des contenus terroristes
- **Décembre 2014 : Mise en application LPM** (Loi de Programmation Militaire)
  - ✓ Accès administratif aux données de connexion
- **Juillet 2015 : Loi Renseignement**
  - ✓ Renforcement accès administratif données de connexion (temps réel), BoitesNoires, Imsi-Catchers, CNCIS remplacée par CNCTR
- **Novembre 2015 : Loi Surveillance Internationale**
  - ✓ Patch de la loi Renseignement suite à censure partielle par Conseil Constitutionnel
- **Novembre 2015 : Etat d'urgence**
  - ✓ Blocage accéléré & perquisitions informatiques
- **Printemps 2016 : Procédure pénale / lutte contre le crime organisé et le terrorisme**
  - ✓ extension au Judiciaire des moyens accordés au renseignement, encadrement chiffrement

Blocage des contenus terro

- Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme

- 2 décrets d'application : Décret n°2015-125 du 05/02/2015 (FAIs) & Décret n°2015-253 du 04/03/2015 (Moteurs de recherche)
  - ✓ Décrets validés par Conseil d'Etat (arrêt 15 février 2016) suite au recours LQDN

- Mode opératoire : OCLCTIC gère la liste (concerne également contenus pedo), sous contrôle CNIL, et l'adresse aux FAIs & FSIs concernés. Blocage DNS sur FQDN

Mise en application LPM

- L'article 20 LPM est venu mettre fin au flou entourant l'accès administratif aux données de connexion
  - ✓ Le fameux art. 22 de la loi n°91-646 sur les interceptions
- A fait l'objet d'un Décret n°2014-1576 relatif à l'accès administratif aux données de connexion
  - ✓ Décret validé par Conseil d'Etat (arrêt du 12 février 2016) suite au recours LQDN
  - ✓ QPC (2015-478 QPC) intéressante sur périmètre données de connexion : « *qu'ainsi, le législateur a suffisamment défini les données de connexion,* ***qui ne peuvent porter sur le contenu de correspondances ou les informations consultées*** *(…) que, par suite,* ***les autorités administratives ne peuvent accéder directement au réseau des opérateurs*** »
- Procédure d'accès en conformité avec interceptions administratives (cf. FrNOG 23)
  - ✓ IGI 1300 sera ton amie

Loi Renseignement

- Une loi qui dormait dans les cartons (cf. rapport JJ. Urvoas 2013)
  - ✓ Plutôt sain dans une société démocratique d'avoir un texte encadrant clairement le périmètre et les pratiques de renseignement

- En pratique :
  - ✓ un festival de mesures venant renforcer des dispositifs existants, pour certains non pleinement appliqués
  - ✓ surenchère politique en réaction aux évènements tragiques janvier 2015
  - ✓ des dispositifs complexes et vulnérabilisant pour les réseaux concernés

Loi Renseignement, en détail

- Reprise du dispositif accès aux données de connexion LPM
  - ✓ Art. L.851-1 CSI remplace art. L.246-1 CSI
- Recueil en temps réel
  - ✓ des données de connexion des personnes «*présentant une menace*» (Art. L.851-2 CSI)
  - ✓ des données de géolocalisation (Art. L.851-4 CSI)
- Les « Boites Noires » (Art. L.851-3 CSI)
  - ✓ Mise en oeuvre d'algorithmes visant à détecter une menace terroriste
  - ✓ Modalités définies dans un décret classifié, donc non publié
- Les IMSI-Catchers (Art. L.851-6 CSI)
- Aggravation peines en cas de défaut de réponse (2 ans & 150 000 €) aux réquisitions administratives & atteintes STAD (jusqu'à 300 000 €)
- La CNCIS est morte, vive la CNCTR !

Loi Renseignement, au final

- Vision paranoïaque de la nécessaire collaboration public↔privé
  - ✓ Art 13 punissant le simple fait de discuter publiquement des modalités techniques
- Dispositif validé par Conseil Constitutionnel (2015-713 DC du 23/07/2015) mais avec précisions intéressantes
  - ✓ « *qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées* »
  - ✓ « *que les traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1* » (NdT : les données de connexion)
- Caractère relativement inopérant des Boites Noires face (i) aux réserves posées par C. Const (uniquement sur données de connexion) (ii) typologie & évolution du trafic côté opérateur

Etat d'urgence

- En réaction aux évènements tragiques de novembre 2015, les pouvoirs publics ont décrété l'état d'urgence

- Mesures impactant le Numérique
  - ✓ Blocage en urgence des contenus terro (jamais mis en oeuvre à ce jour)
  - ✓ Perquisitions informatiques, sur place et à distance

- Précisions intéressantes dans le cadre du contentieux sur l'état d'urgence
  - ✓ Périmètre des saisies informatiques : censure par C. Const (2016-536 QPC du 19 février 2016)

Réforme procédure pénale

- Actuellement en cours de discussion au Parlement
- Mesures impactant le Numérique
  - ✓ Extension des IMSI-Catchers au judiciaire (art. 2)
  - ✓ Techniques spéciales d'investigation dès l'enquête préliminaire : keyloggers (art. 3 bis A), saisie contenus / webmail stockés (art. 1 bis)
  - ✓ Aggravations sanction en cas de non réponse à réquisition (Art. 4 : 2 ans & 15 000 €)
  - ✓ Obligation de communiquer les données chiffrées (Art. 4 Quinquies)
  - ✓ Pénalisation mesures de contournement blocage & délit de consultation habituelle de sites pas bien (Art. 4 Sexies)
  - ✓ Recours obligatoire à la PNIJ pour réquisitions & interceptions (Art. 31 octies)

Des points restant en suspens

- Qu'entend-on réellement par «donnée de connexion» ?

- L'URL est-elle une donnée de connexion ?
  - ✓ car tu comprends, quand un méchant surfe sur You~~Porn~~Tube pour voir des vidéos pas bien, il se connecte à YouTube

OK, mais c'est quoi une donnée technique de connexion ?

- Tout ce qui a trait à l'identification d'un utilisateur d'une ressource, à la localisation et activité de ce dernier

- Rien qui a trait aux informations consultées / correspondances échangées par ce dernier

- Et comme dirait Stéphane Bortzmeyer, il y a toujours un(e) RFC (voire même un(e) BCP) pour ça

RTFM

Article R10-13 En savoir plus sur cet article...

I. - En application du II de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

a) Les informations permettant d'identifier l'utilisateur ;

b) Les données relatives aux équipements terminaux de communication utilisés ;

c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

e) Les données permettant d'identifier le ou les destinataires de la communication.

II. - Pour les activités de téléphonie l'opérateur conserve les données mentionnées au I et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

III. - La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

IV. - Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale.

URL est-elle une donnée de connexion ?

- Selon la Police : la connexion de Jean-Kevin à ses sites favoris, donc oui, l'URL est une donnée de connexion

- Selon les manifestants BOFH, Exégètes et Juristes : noms de domaine, et encore plus URL, non pertinents pour acheminement d'un paquet IP, données non conservées, ce qui est d'ailleurs proscrit par Art. L.34-1 VI CPCE

- Avis CNCTR, ARCEP & CNIL hélas peu clairs et très ambigus sur cette question

Un débat qui va être tranché au niveau Européen

- Impact invalidation Directive 2006/24/CE
  - ✓ 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

- Recours au niveau CEDH (Loi Renseignement) & CJUE (cas Anglais & Suédois)
  - ✓ Premières indications dans le courant de l'été pour CJUE
  - ✓ La CEDH a déjà condamné des dispositifs similaires déjà mis en oeuvre dans d'autres pays (par ex : Russie, Hongrie, Lettonie)

Conduite à tenir en cas de réquisition / décision de justice

- **<u>Ne jamais faire le mort et toujours accuser réception</u>**
  - ✓ 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)

- **<u>En cas de décision de justice, consulter d'urgence son avocat,</u>** de préférence rôdé aux communications électroniques & procédures civiles / pénales
  - ✓ par exemple pour obtenir une rétractation ordonnance <u>art. 145 Code de procédure civile</u> (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 (liste emails, géolocalisation utilisateur…)

- 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 ?