Les obligations légales pour Accès (FAI) & Services / Hébergement (FSI)

Alexandre Archambault

Suivre @AlexArchambault

FrNOG 23

ALLO UI CER OPJ

- Qui était derrière cette IP 192.168.0.1 ?
- Quel est le client derrière suce.ma.teu.be ?
- Quelles sont IP ayant consulté pedodjihadiste.warez.com ?
- Communique moi la liste des emails envoyés et reçus par jeankevin@dedisuffit.com…
- … pour ce soir sinon tu t'exposes à de graves ennuis et je vais le dire à ton patron

C’est ce qu’on appelle les « obligations légales »

- En Europe en général et en France en particulier, un opérateur d’accès, un fournisseur de services Internet DOIT être en mesure de contribuer à l’identification de ses utilisateurs

- Une obligation, mais pas que pour les opérateurs déclarés ARCEP
  - ✓ obligation reconnue de longue date par la jurisprudence pour les FSI non déclarés
  - ✓ confirmée par LCEN en 2004
  - ✓ consacrée au niveau Union Européenne (Directive 2006/24/CE)

- Sanctionnée par le Code Pénal
  - ✓ Au civil / commercial, le juge peut reconnaitre la faute du FSI, ouvrant droit à réparation du préjudice
  - ✓ L’ARCEP peut ouvrir une procédure de sanction L.36-11 CPCE

T’es gentil, mais la CJUE a tout cassé la Directive 2006/24/CE

- Oui mais non

- La CJUE n’a pas remis en cause le principe même de conservation des données de connexion

- Elle a effectivement annulé la Directive 2006/24/CE mais pour des motifs résidant dans l’absence de garanties dans le cadre de sa mise en oeuvre

- Les dispositions nationales, plus restrictives, sont pour la plupart antérieures à la Directive

Mais qui peut me demander des infos sur mes utilisateurs ?

- Tout Officier de Police Judiciaire agissant dans le cadre d'une enquête

- Un avocat ou un huissier <u>DANS LE CADRE DE L'EXECUTION D'UNE DECISION DE JUSTICE</u>

- HADOPI et ANSSI

- Et des administrations au titre du droit de communication (Fisc, Douanes, AMF, DGCCRF) qui renvoie sur L.34-1 CPCE
  - ✓ sur ce dernier point, le Conseil d'Etat est très réservé

Les références légales

- **Article L.33-1 Code des postes et communications électroniques (CPCE) :**
  - ✓ I.-L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve d'une déclaration préalable auprès de l'Autorité de régulation des communications électroniques et des postes. **L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur** : (…)
  - ✓ e) **Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique** (…)

Les références légales

- **Article L.34-1 CPCE :**
  - ✓ III.-Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle (NDR : Hadopi) ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.
  - ✓ VI.-Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. ELLES NE PEUVENT EN AUCUN CAS PORTER SUR LE CONTENU DES CORRESPONDANCES ÉCHANGÉES OU DES INFORMATIONS CONSULTÉES, SOUS QUELQUE FORME QUE CE SOIT, DANS LE CADRE DE CES COMMUNICATION

Les références légales

- **Article L.39-3 CPCE**
  - ✓ I. - Est puni d'un an d'emprisonnement et de 75 000 euros d'amende le fait pour un opérateur de communications électroniques ou ses agents : (…)
  - ✓ 2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

On y arrive

- La Loi, qui ne peut disposer que sur des généralités, renvoie à un Décret pour la mise en oeuvre.

- Décret n°2006-0358 du 24 mars 2006 (codifié à l'article R.10-13 CPCE)

- Décret « LCEN » n°2011-0219 du 25 février 2011

- Dispositions validées par le Conseil d'Etat

On reprend

- Vous êtes déclarés ARCEP, vous êtes donc soumis (notamment) au CPCE
- L'article L.34-1 CPCE pose un principe d'effacement / anonymisation des données techniques de connexion MAIS à application différée
- Catégories précisées à l'article R.10-13 CPCE
- Dans l'intervalle, il faut donc conserver les données, sur 1 an

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.

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

Un début de commencement

CATÉGORIES DE DONNÉES	CODE	PRESTATIONS REQUISES	TARIFS
Liaisons louées de renvoi.	FI 12 FI 13	En sus des frais fixes d'accès au service, pour les liaisons inférieures ou égales à 10 km, abonnement par période indivisible de 31 jours : 1,1 x (37,77 € + 0,79 € par km).	497,00 € pour les frais fixes d'accès au service (sauf sites prééquipés)
		En sus des frais fixes d'accès au service, pour les liaisons supérieures à 10 km, abonnement par période indivisible de 31 jours : 1,1 x (60,10 € + 0,08 € par km).	
Interception des communications de téléphonie de voix sur IP.	FI 23	Le tarif inclut la fourniture du détail de trafic pour toute la période d'interception.	24,00 €
Interception de communication à l'international.	FI 27	Le tarif inclut la fourniture du détail de trafic pour toute la période d'interception.	24,00 €
Interception des communications de téléphonie mobile.	MI 20	Le tarif inclut la fourniture du détail de trafic pour toute la période d'interception.	24,00 €
Mise en suivi du trafic.	MS 14	Délivrance en temps réel des appels émis et reçus avec le code en temps réel de la cellule déclenchée par un téléphone mobile sous interception. La prestation comprend la localisation des bornes, la mise en service et le récapitulatif historique des données fournies.	17,50 € par numéro + 17,50 € par mois

IV. – Tarifs hors taxes applicables à la fourniture de données par les opérateurs de communications électroniques.

CATÉGORIES DE DONNÉES	CODE	PRESTATIONS REQUISES	TARIFS
	WA 0X	A partir d'une demande dématérialisée conforme sur des adresses IP horodatées, rechercher sommairement dans le SI le plus pertinent les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	De 1 à 20 : 4 € Au-dessus de 20 : 0,18 € par IP
	WA 0H	A partir d'une demande accompagnée d'un fichier électronique copiable, rechercher sommairement dans le SI le plus pertinent les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	1 et 20 IP : 6,10 € Au-dessus de 20 : 0,28 € par IP
	WA 01	A partir d'une adresse IP horodatée et d'informations complémentaires, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	18 €
	WA 07	A partir de caractéristiques de compte, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	15,70 €
	WA 08	A partir d'une adresse courriel, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	15,70 €
	WA 09	A partir d'une adresse URL de site visité horodatée, obtenir les éléments d'identification relatifs à la personne physique, à l'installation, à la connexion, au contrat et aux identifications numériques.	15,70 €
	WI 01	Interception du trafic DATA/IP émis et à destination de l'accès internet, à partir d'éléments caractéristique du compte (identité, adresse IP horodatée...) mettre en place l'interception du trafic DATA/IP sur la période demandée spécifiant les caractéristiques de renvoi.	24 €

Concrètement (accès)

- IP attribuée <=> Utilisateur
- Identifiant courrier électronique / messagerie <=> Utilisateur
- Moyen de paiement <=> Utilisateur
- Utilisateur <=> adresse postale (de facturation, d'installation…)
- Serveur attribué <=> Utilisateur

Concrètement (Services)

- Serveur attribué <=> Utilisateur
- Identifiant compte / courrier électronique / messagerie <=> Utilisateur
- Moyen de paiement <=> Utilisateur
- Requête (Mail, Web…) <=> IP (en RFC 6302 / BCP 162 de préférence)

Focus sur l'hébergement

- Le métier a considérablement évolué
  - ✓ historiquement mise en commun de ressources (serveurs, connectivité) opérées par l'hébergeur,
  - ✓ complété depuis par serveurs / racks dédiés, baies, housing pur, DC privatif

- Du coup, fonction de l'offre souscrite par le client, il y a des choses possibles et d'autres pas

Focus sur l'hébergement

- **Serveur mutualisé**
  - ✓ L'hébergeur a la main sur la machine et les services
- **Serveur dédié**
  - ✓ L'hébergeur a la main sur la machine, mais pas sur les services (Web, BdD…)
- **Housing**
  - ✓ L'hébergeur n'a aucune visibilité sur l'activité des serveurs

Oh, mais ça me va coûter un CRS ce truc !

- La bonne nouvelle : l'Etat est tenu d'indemniser les réquisitions judiciaires
- Un barème est établi au Code de procédure pénale
  - ✓ article A-43-9 CPP (arrêté 21/08/2013)
- Dans l'intervalle, il faut donc conserver les données, sur 1 an
  - ✓ suppose une déclaration CNIL sur périmètre données conservées + registre réquisitions judiciaires

GENIE !

Cachet de la juridiction

MÉMOIRE OU ÉTAT

cerfa n° 10 0096

des sommes dues à M. _____

demeurant _____

REFERENCES ET NATURE DE L'AFFAIRE	NOM ET QUALITE DE L'AUTORITE REQUERANTE

Nature et date de la décision d'engagement de la dépense :

Références des textes permettant l'avance par le Trésor :

Nature des opérations	Dates des opérations

DETAIL DES HONORAIRES ET FRAIS		NOMBRE	PRIX	MONTANT	OBSERVATIONS (5)
Honoraires ou indemnités (1)					
Déboursés (2)					
Mode de transport utilisé (3)					
Puissance fiscale du véhicule (4)					
Lieu et kilomètres parcourus					
Grade, groupe, emploi ou indice (4)					
Indemnités de séjour et dates					
Nombre de kms déjà parcourus (4)					
	TOTAL				

Je soussigné atteste sur l'honneur ne bénéficier à quelque titre que ce soit ○ *d'avantages de tarifs*
○ *d'aucun autre avantage de tarifs*

que ceux indiqués ci-dessus et certifie sincère et véritable le présent mémoire établi en un exemplaire unique arrêté à la somme de (en toutes lettres) :

et en demande le règlement par virement *postal / bancaire* *au compte suivant :*

Nom

CCP n° *Centre*

Compte bancaire n° *Banque*

Nom et adresse de l'agence bancaire :

Fait le :

Signature

Pour acquit
le

Signature

Imp. Adm. Melun

(1) Pour les indemnités se reporter aux articles R 112, R 129 et R 140 du Code de procédure pénale, joindre le cas échéant les justifications.
(2) Joindre les justifications
(3) Joindre le cas échéant les justifications
(4) le cas échéant
(5) Pour les expertises, références de l'accord préalable obtenu en application de l'article R 107 du Code de procédure pénale.

94 OM 66 - édition 2002

Le cas particulier du Droit de Communication de l'Administration

- L'Administration (fisc, douanes, ANSSI, AMF, Sécurité Sociale…) dispose d'un droit de communication
- Initialement cantonné à l'identification clients / pièces comptables
- Etendu aux données de connexion via renvoi sur article L.34-1 CPCE qui lui-même renvoie sur R.10-13 CPCE
- Le Conseil d'Etat se montre réservé : cf. proposition 38 de l'étude 2014 « Numérique et Droits Fondamentaux »

Fondements légaux du Droit de Communication de l'Administration

- Fisc : art. L.96 G du Livre des Procédures Fiscales
- Douanes : art. 65 du code des Douanes
- DGCCRF : art. L.450-3 du code de commerce / L.215-3 du code de la consommation
- Prestations sociales : art. L.114-19 du code de la sécurité sociale
- AMF : art. L.621-10 du code monétaire et financier
- ANSSI (pour les demandes hors périmètre L.34-1 CPCE) : art. L. 2321-3 du code de la défense. Périmètre borné à identité & coordonnées postales / électroniques

Les interceptions

- Les « écoutes » ne sont plus que téléphoniques depuis 2004 et concernent l'ensemble des communications électroniques

- 2 catégories d'interceptions
  - ✓ Interceptions judiciaires : ordonnées par un magistrat, en cours de refonte avec mise en oeuvre plateforme centralisée PNIJ
  - ✓ Interceptions administratives : ordonnées par le Premier Ministre, gérées par un service dépendant directement de lui, et ne pouvant être mise en oeuvre que par des entités & personnel habilité

- Surcoûts de mise en oeuvre (études, investissements, développements, fonctionnement…) pris en charge par Etat en application décision Conseil Constitutionnel n°2000-441-DC du 28 décembre 2000

Le Droit de Communication dans le cadre de la LPM

- La Loi de Programmation Militaire est venue instaurer un accès - indirect - des services administratifs de renseignement & lutte contre fraude / criminalité aux données de connexion & localisation
- cf. art. L.246-1 & suivants du code de la sécurité intérieure.
  Applicable à partir de 2015
- Dans les conditions applicables aux interceptions administratives :
  - ✓ mise en oeuvre sur territoire national, par l'intermédiaire d'un service dépendant du Premier Ministre (pas d'accès direct des services enquêteurs aux réseaux & SI)
  - ✓ selon des procédures sécurisés et nécessitant une habilitation SD : en clair, toute demande adressée à une entité non habilitée est nulle et non avenue compte tenu des risques encourus

Conduite à tenir en cas de réquisition / décision de justice

- **Ne jamais faire le mort et toujours accuser réception**
  - ✓ défaut de réponse : 3 750 € (cf. art. 60-1 & 60-2 Code de procédure pénale) / alourdissement probable (cf. préconisation Rapport « Robert » cybercriminalité)
  - ✓ 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 (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