Legal update : on en est où de l'accès aux logs ?

(It's complicated)

FRnOG 36 - 16 Septembre 2022

Retour en arrière

C’est la faute des juges rouges / de l’Europe / complétez la liste ici

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

La France se fait rattraper par la patrouille

Salauds de juges rouges de l'Europe !

Cour de justice de l'Union européenne

COMMUNIQUE DE PRESSE n° 123/20

Luxembourg, le 6 octobre 2020

Presse et Information

Arrêts dans l'affaire C-623/17 Privacy International et dans les affaires jointes C-511/18 La Quadrature du Net e.a. et C-512/18, French Data Network e.a., ainsi que C-520/18 Ordre des barreaux francophones et germanophone e.a.

La Cour de justice confirme que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation

En revanche, dans des situations dans lesquelles un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, celui-ci peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant, par des mesures législatives, une conservation généralisée et indifférenciée de ces données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. S'agissant de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, un État membre peut également prévoir la conservation ciblée desdites données ainsi que leur conservation rapide. Une telle ingérence dans les droits fondamentaux doit être assortie de garanties effectives et contrôlée par un juge ou une autorité administrative indépendante. De même, il est loisible à un État membre de procéder à une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication dès lors que la durée de conservation est limitée au strict nécessaire ou encore de procéder à une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, sans que cela soit dans ce dernier cas limité à un délai particulier

Damage control par le Conseil d'Etat

On appelle cela le dialogue fructueux des juges

CONSEIL D'ÉTAT

Paris, le 21 avril 2021

COMMUNIQUÉ DE PRESSE

Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité

Saisi par plusieurs associations ainsi qu'un opérateur de télécoms, le Conseil d'État a examiné la conformité des règles françaises de conservation des données de connexion au droit européen. Il a aussi été amené à vérifier que le respect du droit européen tel qu'interprété par la CJUE ne compromettait pas les exigences de la Constitution française. Il juge que la conservation généralisée des données est aujourd'hui justifiée par la menace existante pour la sécurité nationale. Il relève également que la possibilité d'accéder à ces données pour la lutte contre la criminalité grave permet, à ce jour, de garantir les exigences constitutionnelles de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales.
En revanche, il ordonne au Gouvernement de réévaluer régulièrement la menace qui pèse sur le territoire pour justifier la conservation généralisée des données et de subordonner l'exploitation de ces données par les services de renseignement à l'autorisation d'une autorité indépendante.

Le nouveau cadre

Faire d’une exception un principe, une passion française

Version en vigueur depuis le 31 juillet 2021

Code des postes et des communications électroniques

- Partie législative (Articles L1 à L144)
  - LIVRE II : Les communications électroniques (Articles L32 à L97-4)
    - TITRE Ier : Dispositions générales (Articles L32 à L40-1)
      - Chapitre II : Régime juridique. (Articles L33 à L34-15)
        - Section 3 : Protection de la vie privée des utilisateurs de réseaux et services de communications électroniques. (Articles L34-1 à L34-6)

Naviguer dans le sommaire du code

› Article L34-1

Version en vigueur depuis le 31 juillet 2021

Modifié par LOI n°2021-998 du 30 juillet 2021 - art. 17

I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonymes, sous réserve des II bis à VI, les données relatives aux communications électroniques.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes .

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

II bis.-Les opérateurs de communications électroniques sont tenus de conserver :

1° Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité de son contrat ;

2° Pour les mêmes finalités que celles énoncées au 1° du présent II bis, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ;

3° Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux.

III.-Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II bis, et de données de localisation précisées par décret en Conseil d'Etat.

L'injonction du Premier ministre, dont la durée d'application ne peut excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies. Son expiration est sans incidence sur la durée de conservation des données mentionnées au premier alinéa du présent III.

III bis.-Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données.

Le nouveau cadre

Faire d'une exception un principe, une passion française

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, pris en application du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

NOR : *PRMD2127502D*

Publics concernés : *fournisseurs d'accès à des services de communication au public en ligne, fournisseurs de services d'hébergement de contenus en ligne, autorités disposant d'un accès aux données conservées.*

Objet : *détermination des catégories de données devant être conservées afin de permettre l'identification de toute personne ayant contribué à la création d'un contenu mis en ligne.*

Entrée en vigueur : *le texte entre en vigueur immédiatement.*

Notice : *le décret abroge et remplace le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Il vise à préciser les catégories de données de connexion devant être conservées par les personnes visées aux 1 et 2 du I de l'article 6 de la loi pour la confiance dans l'économie numérique. Il détermine ainsi les informations relatives à l'identité civile de l'utilisateur, les informations fournies par l'utilisateur lors de la souscription d'un contrat et les informations relatives au paiement, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés ainsi que les autres données de trafic et les données de localisation.*

Références : *le décret est pris pour l'application du II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique, dans sa rédaction modifiée par l'article 17 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Il peut être consulté sur le site Légifrance (https://www.legifrance.gouv.fr).*

Le nouveau cadre

Faire d’une exception un principe, une passion française

Article 2

Les informations relatives à l'identité civile de l'utilisateur, au sens du 1° du II bis de l'article L. 34-1 du code des postes et des communications électroniques, que les personnes mentionnées à l'article 1er sont tenues de conserver jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité du contrat de l'utilisateur, sont les suivantes :

1° Les nom et prénom, la date et le lieu de naissance ou la raison sociale, ainsi que les nom et prénom, date et lieu de naissance de la personne agissant en son nom lorsque le compte est ouvert au nom d'une personne morale ;

2° La ou les adresses postales associées ;

3° La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant ;

4° Le ou les numéros de téléphone.

Le nouveau cadre

Faire d’une exception un principe, une passion française

› Article 5

Les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, mentionnées au 3° du II bis de l'article L. 34-1 du code des postes et des communications électroniques, que les personnes mentionnées à l'article 1er sont tenues de conserver jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux, sont les suivantes :
1° Pour les personnes mentionnées au 1 du I de l'article 6 de la loi du 21 juin 2004 susvisée et pour chaque connexion de leurs abonnés :
a) L'identifiant de la connexion ;
b) L'identifiant attribué par ces personnes à l'abonné ;
c) L'adresse IP attribuée à la source de la connexion et le port associé ;
2° Pour les personnes mentionnées au 2 du I de l'article 6 de la loi du 21 juin 2004 susvisée et pour chaque opération de création d'un contenu telle que définie à l'article 6 :
a) L'identifiant de la connexion à l'origine de la communication ;
b) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus.
Le délai mentionné au premier alinéa du présent article court à compter du jour de la connexion ou de la création d'un contenu, pour chaque opération contribuant à cette création.

Le nouveau cadre

Vous pouvez conserver, mais si vous ne le faites pas, on vous aligne

Code des postes et des communications électroniques

- Partie législative (Articles L1 à L144)
  - LIVRE II : Les communications électroniques (Articles L32 à L97-4)
    - TITRE Ier : Dispositions générales (Articles L32 à L40-1)

> Chapitre V : Dispositions pénales. (Articles L39 à L40-1)

Naviguer dans le sommaire du code

Article L39-3

Version en vigueur depuis le 10 juillet 2004

Modifié par Loi n°2004-669 du 9 juillet 2004 - art. 19 () JORF 10 juillet 2004

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 :

1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans les cas où ces opérations sont prescrites par la loi ;

2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi.

Les personnes physiques coupables de ces infractions encourent également l'interdiction, pour une durée de cinq ans au plus, d'exercer l'activité professionnelle à l'occasion de laquelle l'infraction a été commise.

VI.-1. Est puni d'un an d'emprisonnement et de 250 000 Euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux 1 et 2 du I, de ne pas satisfaire aux obligations définies aux quatrième et cinquième alinéas du 7 du I du présent article ni à celles prévues à l'article 6-1 de la présente loi, de ne pas avoir conservé les éléments d'information visés au II du présent article ou de ne pas déférer à la demande d'une autorité judiciaire d'obtenir communication desdits éléments.

Patatras, la Cour de Cassation a remis le couvert

Justice laxiste, Taubira démissio^h^h^h^OHWAIT

COUR DE CASSATION

LA COUR DÉCISIONS KIOSQUE COLLOQUES INTERNATIONAL PARQUET GÉNÉRAL MES DÉMARCHES

ccueil > Toutes les actualités > Enquêtes pénales : conservation et accès aux données de connexion

Enquêtes pénales : conservation et accès aux données de connexion

TÉLÉCHARGER PDF

12/07/2022

Read the press release in english

Pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652

La Cour de cassation tire les conséquences des décisions rendues par la Cour de justice de l'Union européenne relatives à la conservation des données de connexion et à l'accès à celles-ci dans le cadre de procédures pénales.

FRnOG 36 - 16 Septembre 2022

Donc concrètement, ça donne quoi ?

Lutter contre les méchants ne dispense pas de respecter l'état de droit

	Données relatives à l'identité civile des utilisateurs	Adresses IP attribuées à la source d'une connexion	Données relatives au trafic et à la localisation
En cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée
Lutte contre la criminalité grave	Conservation généralisée et indifférenciée	Conservation généralisée et indifférenciée pour une période temporellement limitée au strict nécessaire	Pas de conservation généralisée et indifférenciée, mais conservation ciblée pour une période temporellement limitée au strict nécessaire et injonction de conservation rapide
Infractions ne relevant pas de la criminalité grave	Conservation généralisée et indifférenciée	Pas de conservation	Pas de conservation

Et sur l'accès ?

Il y aura bien un Cerfa pour cela

- **Données d'identification** : **possible** en toutes circonstances
- **Données de connexion** : **accès désormais très restreint**

➡ Uniquement au pénal et pour criminalité & délinquance grave

➡ Réquisitions émises sous l'autorité du Parquet : **NOK**

➡ Réquisitions émises sur autorisation d'un Magistrat : **OK**

➡ Droit de communication de l'administration : **oui** (d'après le Conseil d'Etat) **mais non** (d'après la Cour de Justice de l'Union Européenne)

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