LA VEILLE JURIDIQUE

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

RUBRIQUE

DROIT DE L'ESPACE NUMÉRIQUE

ANNÉE 2021

PAR LE GÉNÉRAL D'ARMÉE (2S) MARC WATIN-AUGOUARD

PAR LE CAPITAINE THIBAUT HECKMANN

PAR LE CAPITAINE MATTHIEU AUDIBERT

PAR LE LIEUTENANT OCÉANE GERRIET

CREOGN

TABLE DES MATIÈRES

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Janvier

Février

Mars

Avril

Mai

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Juin

Septembre

JANVIER 2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Général d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE JUDICIAIRE

Cour de cassation, Chambre criminelle (n° 20-82.078), arrêt du 1er décembre 2020

Faute de pouvoir identifier son origine éventuellement publique, une sonorisation remise à la justice par un média ne porte pas atteinte à la loyauté de la preuve et demeure contestable au titre de sa valeur probante.

À l'occasion d'une manifestation, les réseaux sociaux diffusent une vidéo représentant un individu casqué portant des coups à un autre. L'auteur, mis en examen et placé sous contrôle judiciaire, va néanmoins violer ses obligations en rencontrant une personne dont la fréquentation lui était interdite. C'est le journal *Mediapart* qui révèle les faits en assortissant ses propos d'extraits de conversations entre les deux mis en examen. Les journalistes de *Mediapart* remettent aux enquêteurs les originaux des fichiers audios à l'origine de leur article, mais invoquent le droit à la protection de leurs sources, s'agissant des conditions dans lesquelles ils sont entrés en possession desdits enregistrements.
Le service central de la police technique et scientifique, saisi en vue de l'authentification des enregistrements et de la reconnaissance des voix, conclut que les enregistrements litigieux ont été édités par un logiciel en libre accès sur Internet, mais n'apporte aucun élément sur l'origine des enregistrements litigieux.
Les enregistrements sont versés à la procédure, ce que conteste l'une des personnes mises en examen qui demande la constatation

de la nullité des pièces. Le demandeur soulève le problème de l'illégalité d'une telle captation qui constitue, selon lui, une atteinte au principe de loyauté de la preuve de nature à entraîner la nullité des pièces.
Pour la Cour de cassation, les journalistes, n'étant pas parties au procès, ne se voient pas imposer les impératifs de loyauté et de légalité de la preuve. L'impossibilité de connaître la participation éventuelle d'une autorité publique à ces enregistrements, telle qu'elle ressort de l'enquête, ne peut exclure une telle éventualité ; l'origine des enregistrements n'a toutefois pas, en l'espèce, d'incidence sur la régularité de la procédure. Le versement au dossier des enregistrements est régulier en la forme. C'est la valeur probante des enregistrements qui fera débat.

Dans cette affaire, la question principale n'est pas l'intervention d'un média dans la transmission d'informations à l'occasion d'une affaire judiciaire, mais les conditions dans lesquelles a été opérée la sonorisation de la rencontre entre les deux mis en examen. Le Code de procédure pénale (CPP) encadre de manière stricte cette technique spéciale d'enquête réservée à la criminalité et à la délinquance organisées et aux crimes (art. 706-96 du CPP). Le cas d'espèce ne relève pas de cette catégorie et ne justifie donc pas la mise en œuvre d'un tel procédé.
Si la preuve avait été apportée de la participation d'une autorité publique à de tels enregistrements, la Cour de cassation aurait censuré la décision d'insérer les documents transposés dans la procédure, en vertu du double principe de régularité et de loyauté de la preuve. Faute de pouvoir prouver, après enquête par les services de la police technique et scientifique, l'origine des enregistrements, la Cour de cassation ne remet pas en cause la

régularité du procédé et reporte le débat sur la valeur probante qui doit être appréciée par les juges du fond.

(Sur ce même arrêt, voir rubrique « Actualité pénale »*, La veille juridique*, n° 92, janvier 2021, p. 38-40)

Cour de cassation, Chambre criminelle (n° 20-83.885), arrêt du 8 décembre 2020

La mise en œuvre d'une vidéosurveillance sur la voie publique par des enquêteurs dans le cadre d'une enquête préliminaire ne relève pas des dispositions de l'article 706-96 du Code de procédure pénale (CPP). Elle nécessite une autorisation spéciale du procureur de la République qui doit en assurer le contrôle.

Dans le cadre d'une enquête préliminaire, un procureur de la République prescrit à des officiers de police judiciaire (OPJ) de mettre en œuvre un moyen de vidéosurveillance sur la voie publique afin de surveiller une maison dans laquelle se livre un trafic de stupéfiants. Selon un renseignement, elle abriterait une plantation de cannabis d'environ mille plants devant être récoltée à court terme. Les investigations ont effectivement permis d'y découvrir cinq kilogrammes d'herbe de cannabis, séchée.
Les enquêteurs ont alors mis en place des surveillances physiques doublées par le système de vidéosurveillance, dont la légalité de la mise en œuvre est contestée par une des personnes interpellées.
Celle-ci a déposé une requête devant la chambre de l'instruction aux fins de voir constater que les vidéosurveillances réalisées sur la voie publique, datées des 21 janvier 2019, 14 février 2019 et 27 février ont été mises en œuvre sans l'accord d'un magistrat du siège

indépendant et, en conséquence, de voir ordonner la nullité des procès-verbaux relatifs aux surveillances précitées ainsi que l'annulation de différents actes en découlant.

Est mise en exergue la violation de l'article 14 du CPP et de l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. La chambre de l'instruction rejetant cette requête, la Cour de cassation doit statuer sur son arrêt qui a validé l'installation d'une vidéosurveillance sur un lieu public par des officiers de police judiciaire agissant en enquête préliminaire, sans autorisation préalable du juge, alors que, selon le moyen du requérant, *« tout dispositif de captage et d'enregistrement d'une image, d'une personne, fût-ce dans un lieu public, suppose nécessairement une ingérence dans sa vie privée et ne peut être mis en place que sous le contrôle effectif d'un juge, et selon les modalités qu'il a au préalable autorisées »*.

Pour la Haute juridiction, le procureur de la République tient des articles 39-3 et 41 du CPP le pouvoir de faire procéder, sous son contrôle effectif et selon les modalités qu'il autorise s'agissant de sa durée et de son périmètre, à une vidéosurveillance sur la voie publique, aux fins de rechercher la preuve des infractions à la loi pénale.

Art. 39-3 du CPP

« Dans le cadre de ses attributions de direction de la police judiciaire, le procureur de la République peut adresser des instructions générales ou particulières aux enquêteurs. Il contrôle la légalité des moyens mis en œuvre par ces derniers, la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits, l'orientation donnée à l'enquête ainsi que la qualité de celle-ci.

Il veille à ce que les investigations tendent à la manifestation de la vérité et qu'elles soient accomplies à charge et à décharge, dans le respect des droits de la victime, du plaignant et de la personne suspectée. »

Art. 41 du CPP

« Le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions à la loi pénale. À cette fin, il dirige l'activité des officiers et agents de la police judiciaire dans le ressort de son tribunal. Il peut, en outre, requérir tout officier de police judiciaire, sur l'ensemble du territoire national, de procéder aux actes d'enquête qu'il estime nécessaires dans les lieux où chacun d'eux est territorialement compétent. […] »

La mise en œuvre d'un système de vidéosurveillance constitue une ingérence dans la vie privée, ayant un caractère limité et proportionné à l'objectif poursuivi. De ce fait, elle n'est pas contraire aux dispositions de l'article 8 de la Convention européenne des droits de l'Homme. Par ailleurs, le dispositif n'implique pas d'acte de contrainte, ni d'atteinte à l'intégrité des personnes dont l'image est ainsi recueillie, ni de saisie, d'interception ou d'enregistrement des paroles de ces personnes. Les OPJ, agissant en préliminaire, tiennent de l'article 14 du CPP le droit de mettre en place et d'exploiter, au surplus avec l'autorisation préalable du procureur de la République et sous le contrôle de celui-ci, un dispositif de vidéosurveillance ayant pour objet, sans le consentement des intéressés, de capter, fixer et enregistrer les images de personnes se trouvant dans un lieu public, afin d'identifier les auteurs ou complices d'infractions.

La Cour de cassation confirme l'arrêt de la chambre de l'instruction qui a écarté, dans le cas d'espèce, l'application de l'article 706-96 du CPP. Cet article encadre la mise en œuvre de captation et de fixation d'images, sur décision d'un juge d'instruction ou, sur autorisation d'un juge des libertés et de la détention (les procureurs de la République n'étant pas jugés indépendants par la Cour européenne des droits de l'Homme), à l'occasion d'enquêtes liées notamment à la criminalité organisée. En effet, la présence d'un individu dans les lieux surveillés étant par nature susceptible d'être vue par quiconque, il n'y avait pas lieu de prévoir un dispositif légal spécifique pour en capter et fixer l'image.

Néanmoins, la mise en œuvre d'une vidéosurveillance sur la voie publique par des enquêteurs nécessite une autorisation spéciale du procureur de la République qui doit en assurer le contrôle.

(Sur ce même arrêt, voir rubrique « Actualité pénale », *La veille jurdique*, n° 92, janvier 2021, p. 30-34)

Cour de cassation, chambre sociale (n° 17-19.523), arrêt du 25 novembre 2020

Les adresses Internet Protocol (IP), qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte par l'exploitation d'un fichier de journalisation constitue un traitement de données à caractère personnel.

À l'occasion d'un litige relatif à un licenciement, la Cour de cassation rappelle sa jurisprudence issue de son arrêt du 3 novembre 2016[1].

1. Cour de cassation – Première chambre civile – (n° 15-22.595), arrêt du 3 novembre 2016.

La nature de l'adresse IP a fait l'objet de prises de position contradictoires.

Dès 2000, pour le G29[2], *« on peut parler sans l'ombre d'un doute de données à caractère personnel » au sens de l'article 2, point a) de la directive 95/46/CE.* Le G29 considère, en effet, que *« les fournisseurs d'accès à internet et les gestionnaires de réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs internet auxquels ils ont attribué des adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP données à l'utilisateur d'internet »*. Le 2 août 2007[3], la Commission nationale de l'informatique et des libertés (CNIL) et le G29 soutiennent que l'adresse IP est une donnée à caractère personnel. La CNIL réagit alors à deux arrêts de la Cour d'appel de Paris relatifs au téléchargement d'œuvres musicales. Le premier, en date du 27 avril 2007[4], refuse d'admettre que l'adresse IP est une donnée à caractère personnel en considérant que celle-ci *« ne permet pas d'identifier le (sic) ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur »*. Quelques jours plus tard, le 15 mai 2007[5], elle affirme que *« le relevé de l'adresse IP de l'ordinateur ayant servi à l'infraction entre dans le constat de sa matérialité et pas dans l'identification de son auteur »*. Elle ajoute *« que cette série de chiffres en effet ne constitue en rien une donnée indirectement*

2. G 29, avis du 21 novembre 2000, « Le respect de la vie privée sur internet - Une approche européenne intégrée sur la protection des données en ligne ».
3. Commission nationale de l'informatique et des libertés, L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes, 2 août 2017.
4. CA. Paris, 13ème chambre, Anthony G./SCPP, 27 avril 2007.
5. CA. Paris, 13ème chambre, Henri S/SCPP, 15 mai 2007.

nominative relative à la personne dans la mesure où elle ne se rapporte qu'à une machine et non à l'individu qui utilise l'ordinateur ».

Le 6 septembre 2007, en revanche, le TGI de Saint-Brieuc[6] reconnaît que l'adresse IP est bien une donnée à caractère personnel : *« L'adresse IP est, au sens strict, un identifiant d'une machine lorsque celle-ci se connecte sur l'internet et non d'une personne. Mais, au même titre qu'un numéro de téléphone n'est, au sens strict, que celui d'une ligne déterminée mais pour laquelle un abonnement a été souscrit par une personne déterminée, un numéro IP associé à un fournisseur d'accès […] constitue un ensemble de moyens permettant de connaître le nom de l'utilisateur »*.

En 2009, c'est au tour de la Cour de cassation d'accentuer l'incertitude : l'arrêt du 13 janvier[7] considère que l'adresse IP n'est pas une donnée personnelle dont le traitement relèverait de la loi du 6 janvier 1978.

Mais, le 12 mars 2013, Viviane Reding, alors commissaire européen, déclare que *« tout traitement de données relatives aux clients, telles que les adresses IP, doit respecter les dispositions nationales qui mettent en œuvre les exigences de la directive 95/46/CE ; ainsi les données à caractère personnel doivent être traitées pour des motifs légitimes et dans un but spécifique, et le traitement doit être proportionné à l'objectif poursuivi »*.

Mais la Cour d'appel de Rennes, par un arrêt du 28 avril 2015[8], confirme que *« le seul relevé d'une adresse IP aux fins de localiser*

6. TGI de Saint-Brieux, 6 septembre 2007, Ministère public, SCPP, SACEM c/J.P.
7. Cass. Crim, n° 08-84.088, 13 janvier 2009.
8. CA. Rennes, ch. Com., n° 14/05708, 2 avril 2015.

un fournisseur d'accès ne constitue pas un traitement de données à caractère personnel au sens des articles 2, 9 et 25 de la loi informatique et libertés du 6 janvier 1978 [NDLR : avant les modifications liées au Règlement général sur la protection des données]. L'adresse IP est constituée d'une série de chiffres, n'est pas une donnée, même indirectement nominative, alors qu'elle se rapporte à un ordinateur et non à l'utilisateur ». Toutefois, le tribunal de grande instance de Meaux, par ordonnance de référé du 10 août 2016[9], reconnaît que la recherche d'une adresse IP est un traitement de données à caractère personnel.
L'arrêt de la Cour de justice de l'Union européenne (CJUE) du 19 octobre 2016[10] met un terme à une certaine insécurité juridique et à une divergence d'appréciation entre les autorités nationales chargées de la protection des données et certaines juridictions.

Patrick Breyer, citoyen allemand, reprochait aux autorités de son pays d'enregistrer et de conserver son adresse IP lorsqu'il consulte les sites Internet fédéraux. Ces derniers enregistrent les données de consultation, notamment l'adresse IP, pour se prémunir contre des malveillances et engager, le cas échéant, des poursuites pénales. Après un rejet de sa demande en première instance, la Cour d'appel a partiellement réformé le jugement, ce qui, bien sûr, n'a pas satisfait les deux parties qui ont engagé un recours en révision devant le Bundesgerichtshof. C'est dans ce cadre que la Cour fédérale de justice allemande a adressé à la CJUE une demande de décision préjudicielle, au titre de l'article 267 TFUE. Cette demande

---

9. *France sécurité/ NC. Numéricable*. Voir veille juridique du CREOGN n° 50, septembre 2016, p. 17-20.
10. CJUE – Arrêt C-582/14 du 19 octobre 2016, *Patrick Breyer contre Bundesrepublik Deutschland*.

portait sur l'interprétation de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
Une adresse IP « dynamique » est-elle une donnée à caractère personnel ? Telle était l'une des questions soulevées. Il existe, en effet, deux types d'adresse IP : la première, « fixe », est affectée en permanence à la « machine » connectée. La seconde est temporaire et attribuée par le fournisseur d'accès lors de chaque session. Elle peut donc changer, ce qui rend sa traçabilité plus complexe mais non impossible. Pour identifier la machine origine, il faut combiner l'action du fournisseur d'accès à Internet (FAI) et celle du site consulté. Dans son arrêt du 24 novembre 2011[11], la CJUE avait déjà pris position sur les adresses IP, dont elle avait reconnu la qualité de données à caractère personnel dans le point 51 : les adresses IP fixes sont *« des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs »*. Mais, dans cette affaire, il s'agissait de la relation directe entre le FAI et l'internaute. Dans l'affaire considérée, seul le FAI peut connaître directement l'identité de la personne (ou plus exactement de la machine), puisqu'il a attribué l'adresse IP. L'opérateur des sites Internet ne dispose pas d'information précise permettant cette opération, sauf si l'internaute s'est identifié au cours de la session.

L'adresse IP dynamique ne constitue pas donc à elle seule pour le fournisseur de services en ligne une information se rapportant à une personne physique identifiée, mais elle peut être qualifiée d'information se rapportant à une personne physique identifiable si

11. CJUE, affaire C-70/10, *Scarlet Extended SA c/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*.

des informations supplémentaires sont détenues par le FAI. Comme l'a souligné l'avocat général, M. Campos Sánchez-Bordona, la conjugaison n'est pas irréalisable en pratique, car elle n'implique pas un effort démesuré en termes de temps, de coût et de main-d'œuvre.

Pour la CJUE, une adresse de protocole Internet dynamique, enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel lorsqu'il dispose des moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont il dispose.

L'arrêt du 19 octobre 2016, combiné à celui du 24 novembre 2011, clarifie d'une manière définitive le lien entre l'adresse IP et la notion de données à caractère personnel. Il met un terme aux hésitations jurisprudentielles.

C'est donc tout naturellement que la Cour de cassation se range derrière cette analyse par son arrêt du 3 novembre 2016 : *« Les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel »*. L'arrêt du 25 novembre 2020 en est la confirmation logique.

Cour d'appel de Paris, 4ème chambre de l'instruction, arrêt du 13 novembre 2020

L'administrateur d'une page Facebook, sans être l'auteur d'un propos diffamatoire publié sur cette page depuis son interface d'administration, peut être poursuivi comme auteur principal.

La Cour d'appel est saisie d'une ordonnance de non-lieu prise par un

juge d'instruction dans une affaire de diffamation publique envers un particulier via un compte page Facebook.
Une plainte avec constitution de partie civile est déposée pour des propos diffamatoires tenus sur le compte « Asnières ma ville ». Une information judiciaire est ouverte et les investigations permettent de constater que les propos en cause ne sont plus accessibles en ligne. Toutefois, les recherches restent vaines pour identifier l'auteur des propos litigieux, notamment en raison du silence de Facebook opposé aux sollicitations des enquêteurs. Seule l'identité de l'administrateur de la page Facebook incriminée est connue.
Celui-ci, pour sa défense, nie être l'auteur des propos litigieux et indique que tous les membres de son association ont la possibilité de publier sur la page, les codes d'accès de celle-ci étant sauvegardés sur l'ordinateur du local de son association et figurant également à côté de l'ordinateur. Il ajoute qu'il a supprimé la publication contestée dès qu'il en a eu connaissance.
Le Parquet délivre des réquisitions de non-lieu en s'appuyant sur ces éléments et en évoquant l'article 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle. Celui-ci exclut la responsabilité pénale du directeur de publication sous plusieurs conditions :

– l'infraction résulte du contenu d'un message adressé par un internaute à un service de communication au public en ligne et mis par ce service à la disposition du public dans un espace de contribution personnelle identifié comme tel ;
– il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message.
La partie civile rappelle cependant les dispositions de l'art. 93-3 de la loi du n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle qui instaure un régime de responsabilité *« en*

cascade » : « Au cas où l'une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication au public par voie électronique, le directeur de la publication ou, dans le cas prévu au deuxième alinéa de l'article 93-2 de la présente loi, le codirecteur de la publication sera poursuivi comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public. A défaut, l'auteur, et à défaut de l'auteur, le producteur sera poursuivi comme auteur principal ».

Dans le cas d'espèce, l'article litigieux n'est pas un message adressé par un internaute sur la page Facebook de M. Z. mais publié depuis l'interface d'administration de la page. Pour la Cour d'appel qui censure l'arrêt de non-lieu, il convient de rechercher si le mis en cause peut être qualifié de producteur et donc voir sa responsabilité pénale engagée à ce titre.

FÉVRIER 2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Général d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE CONSTITUTIONNELLE

Décision n° 2020-882 QPC du 5 février 2021 (Société Bouygues Telecom et autre)

Les dispositions prévues par la loi n° 2019-810 du 1er août 2019, relative au contrôle par le Premier ministre du déploiement d'équipements pour la 5G, sont conformes à la Constitution au regard de la sauvegarde des intérêts fondamentaux de la Nation et ne visent aucun fournisseur ou État particulier.

Dans le cadre d'un recours portant sur le décret n° 2019-1300 du 6 décembre 2019, relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques, Bouygues Telecom et SFR demandent au Conseil d'État de saisir le Conseil constitutionnel d'une question prioritaire de constitutionnalité (QPC) se rapportant à la loi n° 2019-810 du 1er août 2019. Celle-ci vise à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles. Free mobile s'ajoute en qualité de société intervenante devant le Conseil constitutionnel.
La question prioritaire de constitutionnalité porte sur le premier alinéa du paragraphe I de l'article L. 34-11 du Code des postes et des communications électroniques et sur les mots « et le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un État non membre de l'Union européenne » figurant au second alinéa de l'article L. 34-12 du même Code.

Article L. 34-11
« - I.- Est soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou logiciels, permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile, à l'exception des réseaux de quatrième génération et des générations antérieures, qui, par leurs fonctions, présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages transmis et des informations liées aux communications, à l'exclusion des appareils installés chez les utilisateurs finaux ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils. […] »

Article L. 34-12
« - Le Premier ministre refuse l'octroi de l'autorisation prévue à l'article L. 34-11 s'il estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale résultant du manque de garantie du respect des règles mentionnées aux a, b, e, f et f bis du I de l'article L. 33-1 relatives à la permanence, à l'intégrité, à la sécurité, à la disponibilité du réseau, ou à la confidentialité des messages transmis et des informations liées aux communications.[…]
Le Premier ministre prend en considération, pour l'appréciation de ce risque, le niveau de sécurité des appareils, leurs modalités de déploiement et d'exploitation envisagées par l'opérateur et le fait que l'opérateur ou ses prestataires, y compris par sous-traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un État non

membre de l'Union européenne. »
Article L. 34-13. « - Si l'exploitation des appareils mentionnés au I de l'article L. 34-11 est réalisée sur le territoire national sans autorisation préalable ou sans respecter les conditions fixées par l'autorisation, le Premier ministre peut enjoindre à l'opérateur de déposer une demande d'autorisation ou de renouvellement ou de faire rétablir à ses frais la situation antérieure, dans un délai qu'il fixe. […] »

I. La position des sociétés requérantes

Les sociétés requérantes contestent le fait d'imposer aux opérateurs de communications électroniques de se soumettre à un régime d'autorisation administrative préalable, au nom des exigences de protection de la défense et de la sécurité nationale, pour exploiter des équipements tels que les antennes-relais, permettant l'accès aux réseaux de communications mobiles. Cette autorisation est, selon elles, insuffisamment encadrée, compte tenu de la généralité de la notion d'« intérêts de la défense et de la sécurité nationale ». Elles doivent procéder au remplacement de tout ou partie de leurs équipements déjà installés au titre des réseaux des générations précédentes, en raison de contraintes techniques liées à l'absence d'interopérabilité des appareils. Ces charges excessives ont en réalité pour seul objet d'interdire aux opérateurs de se fournir en appareils de cinquième génération auprès de la société chinoise Huawei, en méconnaissance de la liberté d'entreprendre. Cette contrainte les restreint dans le choix de leurs équipementiers et pénalise ceux d'entre eux ayant eu recours à cette société pour leurs équipements plus anciens. Les opérateurs de communications électroniques sont obligés de

remplacer leurs équipements à leurs frais, ce qui entraîne une charge disproportionnée. Ces frais devraient incomber à l'État puisqu'il impose des règles au nom de la sécurité nationale, violant ainsi le principe d'égalité devant les charges publiques.
Par ailleurs, les sociétés requérantes soulignent qu'en vertu de l'article 226- 3 du Code pénal, elles doivent déjà soumettre à autorisation, à compter du 1er octobre 2021, certains des équipements en cause. En leur substituant un nouveau régime d'autorisation préalable, le législateur porte atteinte à des situations légalement acquises ainsi qu'aux attentes légitimes des opérateurs de demeurer soumis aux seules dispositions de cet article 226-3.
Enfin, subordonner la délivrance de l'autorisation au fait que l'opérateur ou ses prestataires ne sont pas sous le contrôle d'un État étranger ou soumis à des actes d'ingérence d'un tel État conduit à choisir des équipements à raison de la situation de leur fabricant et non de leurs caractéristiques intrinsèques.

II. La réponse des Sages

Nul n'est visé par le législateur

Le Conseil constitutionnel rappelle tout d'abord qu'il est possible d'apporter des limitations à la liberté d'entreprendre liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteinte disproportionnée au regard de l'objectif poursuivi. Le niveau de sécurité des appareils, leurs modalités de déploiement et d'exploitation envisagées par l'opérateur, comme l'absence de contrôle ou d'ingérence d'un État non membre de l'Union européenne sur l'opérateur, ses prestataires ou sous-traitants, préservent les intérêts de la défense

et de la sécurité nationale et prémunissent les réseaux radioélectriques mobiles contre des risques d'espionnage, de piratage et de sabotage qui peuvent résulter des nouvelles fonctionnalités offertes par la cinquième génération de communication mobile, lorsque les fonctions des appareils présentent un risque pour la permanence, l'intégrité, la sécurité ou la disponibilité du réseau ou pour la confidentialité des messages transmis et des informations liées aux communications. Le législateur n'a visé ni un opérateur ou un prestataire déterminé ni les appareils d'un fabricant déterminé mais a voulu sauvegarder les intérêts fondamentaux de la Nation.

La sauvegarde des intérêts fondamentaux de la Nation

L'autorisation ne concerne que les entreprises qui, exploitant un réseau de communications électroniques au public, sont désignées par l'autorité administrative comme opérateurs d'importance vitale parce qu'elles utilisent des installations dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre de la Nation, son potentiel économique, sa sécurité ou sa capacité de survie. Ces entreprises sont, de ce fait, tenues de coopérer à la protection de ces installations contre toute menace (article L. 13321 du Code de la défense). L'autorisation n'est requise que pour exploiter, sur le territoire national, des appareils permettant de connecter les terminaux des utilisateurs finaux aux réseaux radioélectriques mobiles postérieurs à ceux de quatrième génération. Elle ne peut être refusée que si le Premier ministre estime qu'il existe un risque sérieux d'atteinte aux intérêts de la défense et de la sécurité nationale, dû à l'insuffisance des garanties du respect des règles relatives à la permanence, à l'intégrité, à la sécurité ou à la disponibilité du réseau ou relatives à la

confidentialité des messages transmis et des informations liées aux communications. Ainsi, ces dispositions mettent en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation.

La charge incombe aux opérateurs

Les dispositions de la loi sont susceptibles d'entraîner des charges pour les opérateurs, liées à la nécessité de remplacer certains anciens équipements afin de les rendre matériellement compatibles avec les appareils dont l'exploitation est subordonnée à l'autorisation contestée. Mais ces charges résultent des seuls choix de matériels et de fournisseurs, initialement effectués par les opérateurs, et ne sont donc pas imputables à l'État. L'autorisation préalable d'exploitation de certains appareils sécurise les réseaux de communication. Elle a un lien direct avec les activités des opérateurs qui utilisent et exploitent ces réseaux dans le cadre de l'offre au public des services de communications électroniques. Les frais engagés sont, par nature, des dépenses qui leur incombent, le législateur n'ayant pas reporté sur des personnes privées des dépenses qui seraient imputables à l'État.

Une absence d'atteinte aux situations légalement acquises

Le régime d'autorisation du Premier ministre ne concerne que les équipements nouveaux, mis en œuvre dans le cadre du déploiement de la 5G. Les générations précédentes, dont la 4G, ne sont donc pas concernées. Il n'a aucune incidence sur les autorisations d'utilisation des fréquences dont disposent les opérateurs pour exploiter ces mêmes réseaux. Les dispositions contestées ne portent donc aucune

atteinte à des situations légalement acquises.
Avant que la loi ne soit promulguée, les opérateurs de communications électroniques étaient soumis au régime d'autorisation applicable à la détention et à l'utilisation de certains appareils, prévu à l'article 226-3 du Code pénal.

Article 226-3

« Est puni de cinq ans d'emprisonnement et de 300 000 € d'amende :
1° La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure et figurant sur une liste dressée dans des conditions fixées par décret en Conseil d'État, lorsque ces faits sont commis, y compris par négligence, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par ce même décret ou sans respecter les conditions fixées par cette autorisation ;
2° Le fait de réaliser une publicité en faveur d'un appareil ou d'un dispositif technique susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 lorsque cette publicité constitue une incitation à commettre cette infraction ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure lorsque cette publicité constitue une incitation à en faire un usage frauduleux.

Le présent article n'est pas applicable à la détention ou à l'acquisition par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public, des appareils soumis à une autorisation du Premier ministre en application de la section 7 du chapitre II du titre Ier du livre II du code des postes et des communications électroniques. » (ajout de la loi n° 2019-810 du 1er août 2019)

L'arrêté du 11 août 2016 (art. 1er), venant en application de l'article 226-3, dispose que les règles imposées par ce dernier ne s'appliquent qu'à compter du 1er octobre 2021 aux « appareils qui permettent aux opérateurs de communications électroniques de connecter les équipements de leurs clients au cœur de leur réseau radioélectrique mobile ouvert au public, dès lors que ces appareils disposent de fonctionnalités, pouvant être configurées et activées à distance, permettant de dupliquer les correspondances des clients, à l'exclusion des appareils installés chez ceux-ci ». La finalité de l'article 226-3 du Code pénal est distincte de celle de la loi contestée. La première encadre la détention et l'utilisation de certains appareils, à raison des atteintes qu'ils permettent de porter à la vie privée et au secret des correspondances. La seconde est applicable aux équipements permettant la connexion à un réseau mobile à raison des atteintes susceptibles d'être portées aux intérêts de la défense et de la sécurité nationale.
La loi n° 2019-810 du 1er août 2019 exclut de son champ les appareils mis en œuvre par les opérateurs qui sont soumis au nouveau régime d'autorisation par le Premier ministre. Pour le Conseil constitutionnel, le fait d'être soumis à un régime d'autorisation répondant à certaines finalités ne peut faire naître l'attente légitime

que n'intervienne aucun nouveau régime d'autorisation répondant à d'autres finalités. Le nouveau régime ne s'applique qu'aux seuls équipements permettant l'accès aux réseaux mobiles postérieurs à ceux de quatrième génération, afin de répondre aux enjeux de sécurité spécifiques à ces nouveaux réseaux. Les opérateurs de communications électroniques, sur le seul fondement du régime d'autorisation résultant de l'article 226-3 du Code pénal, ne peuvent légitimement s'attendre à ce que ne soient pas instituées, même avant le 1er octobre 2021, des règles d'exploitation des appareils permettant la connexion aux réseaux de nouvelles générations, à des fins de protection de la défense et de la sécurité nationale.

JURISPRUDENCE ADMINISTRATIVE

Conseil d'État, 10ème - 9ème chambres réunies, n° 429956 du 21 janvier 2021, Association « Ouvre-Boîte »

La loi du 7 octobre 2016 (loi Lemaire), complétée par la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, a créé les bases légales de l'open data des décisions de justice judiciaire et administrative. Faute d'avoir publié les textes d'application dans un délai raisonnable, l'État est enjoint par le Conseil d'État de prendre, dans un délai de trois mois à compter de la notification de sa décision, l'arrêté prévu à l'article 9 du décret du 29 juin 2020.

La loi pour une République numérique du 7 octobre 2016 (art. 20 et 21), dite loi Lemaire, a modifié l'article L. 10 du Code de justice administrative et inséré un article L. 111-13 dans le Code de

l'organisation judiciaire afin de mettre à disposition du public, à titre gratuit et dans le respect de la vie privée des personnes concernées, des décisions rendues par les juridictions administratives et judiciaires. Elle a ainsi posé les bases légales de l'open data judiciaire. La complexité de ce dispositif, au regard de la sécurité des personnes ou du respect de leur vie privée ou de celle de leur entourage, a conduit le législateur à apporter des modifications par l'article 33 de la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. Cet article comporte plusieurs dispositions relatives à l'occultation des noms et prénoms des personnes physiques lorsqu'elles sont parties ou tiers, à l'occultation, lorsque sa divulgation est de nature à porter atteinte, de tout élément permettant d'identifier les parties, les tiers, les magistrats et les membres du greffe. Il interdit de réutiliser les données d'identité des magistrats et des membres du greffe pour évaluer, analyser, comparer ou prédire les pratiques professionnelles réelles ou supposées des membres des juridictions ou des juridictions entre elles.

Le 29 juin 2020, un décret a été pris pour l'application des articles L. 10 du Code de justice administrative et L. 111-13 du Code de l'organisation judiciaire dans leur nouvelle rédaction. L'article 9 de ce décret renvoie toutefois à un arrêté du garde des Sceaux, ministre de la Justice, le soin de fixer « pour chacun des ordres judiciaire et administratif et le cas échéant par niveau d'instance et par type de contentieux, la date à compter de laquelle les décisions de justice sont mises à la disposition du public ».

Le 18 décembre 2018, après la loi Lemaire mais avant la promulgation de la loi et du décret précités, l'association « Ouvre-boîte », dont l'objet est de promouvoir l'accès et la publication effective des documents, a demandé au Premier ministre de

procéder à la publication des décrets d'application des articles L. 10 du Code de justice administrative et L. 111-13 du Code de l'organisation judiciaire. Le silence du Premier ministre valant décision implicite de rejet, son illégalité est mise en avant par l'association qui, le 18 avril 2019, demande l'annulation pour excès de pouvoir et reproche au Premier ministre d'avoir dépassé le délai raisonnable dont il disposait pour édicter ces mesures.

Mais, postérieurement au recours, un décret a été pris le 29 juin 2020 pour l'application des articles L. 10 du Code de justice administrative et L. 111-13 du Code de l'organisation judiciaire dans leur nouvelle rédaction. L'article 9 de ce décret renvoie toutefois à un arrêté du garde des Sceaux, ministre de la Justice, le soin de fixer « pour chacun des ordres judiciaire et administratif et le cas échéant par niveau d'instance et par type de contentieux, la date à compter de laquelle les décisions de justice sont mises à la disposition du public ». Il ne peut, à lui seul, assurer l'application des dispositions des articles L. 10 du Code de justice administrative et L. 111-13 du Code de l'organisation judiciaire.

Si la publication en cours d'instance du décret d'application d'une loi rend sans objet le recours dirigé contre le refus de prendre un tel décret[1], l'arrêté ministériel prévu par le décret du 29 juin 2020 n'est, quant à lui, toujours pas paru à la date de sa décision. Le ministre de la Justice est fondé à soutenir que la requête de l'association « Ouvre-boîte » a perdu son objet en tant qu'elle est dirigée contre le refus du Premier ministre de prendre un décret d'application des dispositions législatives en cause, mais cette requête conserve un objet en tant qu'elle est dirigée contre le refus du garde des Sceaux de fixer par arrêté le calendrier d'entrée en vigueur de ces dispositions.

1. CE 27 juill. 2005, n° 261694, Association Bretagne Ateliers.

Le Conseil d'État rappelle que l'exercice du pouvoir réglementaire comporte non seulement le droit mais aussi l'obligation de prendre dans un délai raisonnable les mesures qu'implique nécessairement l'application de la loi, hors le cas où le respect d'engagements internationaux de la France y ferait obstacle. Lorsqu'un décret pris pour l'application d'une loi renvoie lui-même à un arrêté la détermination de certaines mesures nécessaires à cette application, cet arrêté doit également intervenir dans un délai raisonnable.

Tout en reconnaissant que la mise à disposition du public des décisions de justice constitue une opération d'une grande complexité pouvant nécessiter, à compter de l'intervention du décret en organisant la mise en œuvre, des dispositions transitoires, la Haute juridiction relève que le ministre de la Justice, ne pouvait, sans méconnaître ses obligations, s'abstenir de prendre l'arrêté prévu à l'article 9 du décret du 29 juin 2020 et de fixer le calendrier d'entrée en vigueur des dispositions de ce décret dans un délai raisonnable. Or, plus de 20 mois se sont écoulés après la loi du 23 mars 2019 et plus de six mois après la publication du décret du 29 juin 2020 à la date de la présente décision, pour l'application des dispositions législatives relatives à la mise à disposition du public des décisions de justice, prévue par le législateur dès 2016.
Il s'ensuit que l'association « Ouvre-boîte » est fondée à soutenir que le garde des Sceaux, ministre de la Justice, ne pouvait légalement refuser de prendre cet arrêté.

Investigations fiscales et douanières

Décret en Conseil d'État n° 2021-148 du 11 février 2021

Le décret met en application l'article 154 de la loi de finances pour 2020 qui autorise les administrations fiscales et douanières à opérer à titre expérimental des traitements de données ouvertes.

La loi de finances pour 2020, par son article 154, permet à l'administration fiscale et à l'administration des douanes et des droits indirects de collecter et d'exploiter au moyen de traitements informatisés les contenus « librement accessibles », publiés sur Internet par les utilisateurs de opérateurs de plateformes en ligne relevant de l'article L. 111-7-I-2° du Code de la consommation. Ces plateformes permettent la mise en relation en vue de la vente, de la fourniture d'un service, de l'échange ou du partage d'un bien ou d'un service (« places de marché »), mais aussi le partage de contenus (« réseaux sociaux »).
Cette disposition est autorisée à titre expérimental pour une durée de trois ans.
L'objectif poursuivi est de rechercher par ce moyen les infractions fiscales et douanières les plus graves. Internet constitue aujourd'hui une source d'informations peu exploitée eu égard aux limites de l'exploitation manuelle par une ressource humaine limitée en nombre. Le législateur permet un « changement d'échelle significatif dans le cadre des prérogatives confiées à ces administrations dans le cadre de leurs missions », comme le souligne la Commission nationale de l'informatique et des libertés (CNIL), saisie pour avis[2], qui considère que ce type de traitement est d'un

2. Délibération CNIL n° 2019-114 du 12 septembre 2019.

« genre nouveau » par rapport aux cas qu'elle a eu à traiter auparavant.

Les traitements en cause peuvent être mis en œuvre pour la recherche de certains manquements et de certaines infractions dont la commission est rendue possible ou favorisée par l'usage d'Internet. Peuvent être ainsi concernés le défaut ou le retard de production d'une déclaration fiscale en cas de découverte d'une activité occulte et de la fabrication, de la détention, de la vente ou du transport illicites de tabac, des pratiques frauduleuses en matière d'alcool, de tabac et de métaux précieux, de contrefaçon et des délits douaniers sanctionnant la contrebande, l'importation et l'exportation de marchandises non déclarées, ainsi que le blanchiment de produits financiers provenant d'un délit douanier ou d'une infraction à la législation sur les stupéfiants. D'autres cas sont envisagés qui ne sont pas « rendus possibles ou favorisés » par l'usage d'Internet mais constituent un des cas les plus graves de soustraction à l'impôt, telle l'insuffisance de déclaration mentionnée à l'article 1729 du Code général des impôts découlant d'un manquement aux règles de domiciliation fiscale fixées à l'article 4 B. Comme le souligne le gouvernement, l'article 154 permet à l'administration de collecter et d'exploiter des données publiées par des internautes qui révèleraient une pratique de fraude fiscale réalisée exclusivement dans le monde physique, par exemple dans le cas où son auteur en ferait simplement état publiquement sur un réseau social.

Le Conseil constitutionnel a partiellement censuré cet article mais en a validé l'essentiel en vérifiant les conditions garantissant un équilibre entre l'atteinte aux libertés et l'objectif constitutionnel de

lutte contre les fraudes fiscales et douanières les plus graves.
Le décret en Conseil d'État n° 2021-148 du 11 février 2021, pris après avis de la CNIL, précise les modalités de mise en œuvre par la direction générale des finances publiques et la direction générale des douanes et droits indirects de traitements informatisés et automatisés permettant la collecte et l'exploitation de données rendues publiques sur les sites Internet des opérateurs de plateforme en ligne.
Le décret autorise les traitements dans la phase d'apprentissage et de conception et dans la phase d'exploitation (art. 1). Il rappelle que seuls les contenus se rapportant à la personne qui les a « délibérément » divulgués et dont l'accès ne nécessite ni saisie d'un mot de passe ni inscription sur le site en cause peuvent être exploités. Est ainsi prohibée la collecte des contenus librement accessibles et manifestement rendus publics sur les sites Internet des plateformes au moyen d'identités d'emprunt ou de comptes spécialement utilisés à cet effet, sous la seule réserve de la création de comptes destinés à être utilisés par l'intermédiaire d'interfaces de programmation mises à disposition par les opérateurs de plateforme.
Par ailleurs, il indique que les commentaires et les interactions avec des tiers, déposés sur une page Internet, ne peuvent faire l'objet d'aucune exploitation. Le décret précise également en quoi les données sont adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est strictement nécessaire.

Lieutenant Océane GERRIET

Facebook ou la cour de recré 2.0

Dans deux jugements rendus au cours du mois de janvier 2021, la 17ème chambre du tribunal judiciaire (TJ) de Paris a de nouveau démontré que la diffamation et l'injure n'avaient pas leur place sur un réseau social, y compris pour les personnalités politiques.

L'année commence sur des chapeaux de roues avec, au programme, deux abus à la liberté d'expression sur notre réseau social favori (ou pas)[3] qui est déjà sous le feu des projecteurs avec sa cour suprême numérique[4] ! Et pourtant, les faits étant antérieurs à la Saint-Sylvestre, les deux protagonistes ne pourront pas arguer d'avoir abusé d'une bonne bouteille de champagne.

Dans le jugement rendu le 13 janvier 2021, le tribunal judiciaire de Paris statue sur une **diffamation** réalisée en ligne, à savoir sur la page publique Facebook d'une ville où une ancienne élue est accusée de ne pas avoir restitué du matériel appartenant à la commune avant d'avoir été menacée de dépôt de plainte. Dans les faits, le matériel avait finalement été rendu. Ainsi, l'ancienne élue a agi en diffamation. Pour mémoire, **l'article 29 al.1 de la loi du 29 juillet 1881** définit la diffamation comme « toute allégation ou

3. Nous, on préfère Twitter ou LinkedIn, cliquez et vous verrez.

4. « Nous ne devons pas laisser la seule régulation aux plates-formes numériques », Entretien avec Stanislas Guérini, *Le Monde*, janvier 2021 [consulté le 30 janvier 2021]. Disponible sur : https://www.lemonde.fr/international/article/2021/01/13/stanislas-guerini-nous-ne-devons-pas-laisser-la-seule-regulation-aux-plates-formes-numeriques_6066052_3210.html

imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé ». Pour être constituée, la diffamation doit imputer **un fait précis** à l'encontre **d'une personne déterminée**. Comme le rappelle le TJ, le fait précis se distingue de l'opinion ou du jugement de valeur qui peut être « librement discuté ». En outre, cette allégation doit **porter atteinte « à l'honneur ou la considération »** de ladite personne. En l'espèce, le message posté sur la page Facebook de la mairie visait expressément et nommément l'ancienne élue. De plus, il faisait état d'un fait précis puisqu'il évoquait le fait qu'elle n'ait pas rendu du matériel informatique appartenant à la mairie (ce qui ne serait pas le cas du propos suivant par exemple « les collectivités territoriales ferment les yeux sur des vols »). Enfin, le propos était accompagné de la référence au Code pénal. Comme le souligne le TJ, l'atteinte doit s'apprécier objectivement, c'est-à-dire au regard du contexte général (fait pénalement répréhensible, fait contraire à la morale communément admise, etc.). Dès lors, le contenu du message a manifestement porté atteinte à l'honneur de la personne visée puisqu'il sous-entend que la personne a commis un fait pénalement répréhensible.

La défense estimait, quant à elle, qu'il n'y avait pas d'imputation de fait précis puisqu'en réalité, l'ancienne élue avait bien restitué le matériel après avoir été menacée d'un dépôt de plainte, de sorte qu'il n'y avait pas eu d'infraction. Cependant, cet argumentaire ne peut prospérer, dès lors que le commentaire dit l'inverse, à savoir que l'élue a tenté de « voler la collectivité » et n'a restitué le matériel qu'après avoir été menacée d'une plainte.

Ensuite, la défense tenta d'invoquer **la bonne foi**. Les 4 critères élaborés par la jurisprudence (exemple : Crim. 24 mai 2005, n° 03-86.460) ne sont toutefois pas remplis. Les propos tenus ne sont pas

légitimes dans le sens où ils ne s'inscrivent pas dans un débat d'intérêt général (historique, scientifique ou autre). Il convient de noter que, s'agissant du débat politique, la jurisprudence est plus souple et admet plus aisément la critique et repousse *de facto* les limites de la liberté d'expression[5]. En l'espèce, la défense tente de faire valoir la « dose d'exagération ou de provocation » communément admise en politique. Toutefois, le juge souligne que les faits datent d'il y a 4 ans et que ce commentaire intervient dans le cadre d'un article relatif à des voyages organisés pour les séniors de la commune, de sorte que le propos tenu ne présente aucun intérêt général dans ce contexte. En outre, il poursuit en précisant que, si l'ancienne élue s'est montrée récalcitrante à rendre le matériel dans les temps, elle n'a, à aucun moment, commis les faits allégués.

Ensuite, s'agissant du critère de la mesure dans le propos, force est de constater que le contenu en est privé dès lors que l'élue est accusée d'un vol. Enfin, les propos démontrent une animosité personnelle, étant donné que les faits, commis il y a 4 ans, ne constituent pas l'infraction alléguée, de sorte que le propos tenu vise bien à déstabiliser la personne visée. Par ailleurs, le tribunal souligne que les deux femmes sont adversaires politiques. Partant, l'excuse de bonne foi n'est pas recevable et l'élue s'est rendue coupable de diffamation.

Dans le second jugement rendu le 18 janvier 2021, le tribunal judiciaire de Paris a l'opportunité de rappeler les conditions d'application de l'injure qui relève de l'article 29 al. 2 de la loi de 1881. Définie comme « toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait »,

5. CEDH, *Mamere c/ FRANCE*, 7 novembre 2006 : le fait de qualifier une personne de « sinistre personnage » n'excède pas les limites de la liberté d'expression.

l'injure est constituée lorsqu'elle porte atteinte à la dignité d'une personne déterminée (ou d'un groupe de personnes) et qu'elle renferme un propos dévalorisant. Contrairement à la diffamation vue précédemment, ici, il n'est pas nécessaire d'évoquer un fait précis. En tous les cas, la jurisprudence est particulièrement riche d'exemples (« pouffiasse », Crim. 15 avril 1959 ; « petite vermine », Crim. 11 mai 1960) et a eu l'occasion de souligner que le comportement injurieux s'apprécie de manière objective et qu'il importe peu que le mis en cause ait une perception du message plus rationnelle (Crim. 24 novembre 2009, n° 83.256). Toutefois, les magistrats portent une attention sur le contexte qui permet d'éclairer la portée du propos injurieux qui pourrait, par exemple, ne pas l'être de prime abord, mais qui, au regard d'un contexte particulier, revêtirait un certain sens.

Dans ce cas d'espèce, les faits sont plutôt simples. Sur fond de tensions, reproches et non-dits entre amis, le prévenu a publié sur sa propre page Facebook, accessible de tous « sans restrictions », des propos fort dévalorisants et visant nommément son ancien ami : « faussaire », « muffle, goujat, malotru, connard », « aigri, arriviste, malveillant » entre autres… Le tribunal ne peut, dès lors, que constater qu'il s'agit de propos outrageants visant une personne déterminée.

Pour tenter d'échapper à la condamnation, le prévenu invoque deux faits justificatifs : la bonne foi et l'excuse de provocation. S'agissant de la bonne foi, les 4 critères énoncés *supra* ne sont pas remplis. Les propos tenus ne sont pas légitimes dans le sens où ils ne s'inscrivent pas dans un débat d'intérêt général, s'agissant d'invectives purement personnelles. L'énumération d'invectives ne reposant sur aucun fait démontre, de plus, qu'ils ne font l'objet d'aucune mesure, reflétant une esquisse de critique, notamment eu égard aux faits qu'il peut reprocher à l'intéressé (et non démontrés par ailleurs).

Partant, les propos tenus démontrent au contraire une animosité personnelle. S'agissant de **l'excuse de provocation**, la jurisprudence exige une provocation telle qu'elle soit de nature à faire perdre son sang-froid pouvant générer une riposte mais dans un temps rapproché de la provocation et proportionnée (exemple : Crim. 24 novembre 2009, n° 09-83.256). En l'espèce, le prévenu allègue un contentieux antérieur à son post Facebook qu'il n'est, par ailleurs, pas en mesure de dater et de démontrer. En outre, il estime que le fait d'avoir reçu une invitation Facebook du nouveau manager de son ami constitue une provocation mais cet argument ne prospère pas devant la juridiction qui estime que ce n'est pas une provocation « directe et personnelle ».
Par conséquent, le TJ condamne le prévenu pour injure publique. Ce qui est intéressant de noter dans cette affaire est que la personne injuriée avait demandé le retrait du contenu litigieux. Néanmoins, le tribunal a estimé qu'un tel retrait constituerait une « atteinte disproportionnée à la liberté d'expression », d'autant plus que le propos n'a pas d'écho en dehors de la page Facebook de l'intéressé. Une décision qui peut interroger mais illustre une nouvelle fois la place importante qu'occupe la liberté d'expression dans nos démocraties, qui implique, comme le souligne la Cour européenne des droits de l'Homme, que puisse être exprimés des propos « qui heurtent, choquent ou inquiètent l'État ou une fraction quelconque de la population »[6].

Cette question du retrait des contenus est en réalité bien plus complexe et pourrait justifier à elle seule de nombreuses lignes. Les récents évènements du Capitole ont remis à l'ordre du jour cette

6. CEDH, 7 décembre 1976, *Handyside c/ Royaume-Uni*.

question et la place qu'occupent les plateformes numériques et les États en la matière. Pour mémoire, en France, la loi pour la confiance dans l'économie numérique exige des hébergeurs qu'ils retirent les contenus manifestement illicites dès qu'ils en ont connaissance. La Commission européenne prépare actuellement deux projets de règlement pour réguler le marché numérique[7] et certains parlementaires français tentent déjà de l'anticiper, ce qui génère de nombreuses interrogations[8].

7. CRICHTON, Cécile. Le *Digital Services Act*, un cadre européen pour la fourniture de services en ligne, *Dalloz.actualité*, janvier 2021. Disponible sur : https://www.dalloz-actualite.fr/flash/digital-service-act-un-cadre-europeen-pour-fourniture-de-services-en-ligne#.YBU4cuhKiUk

8. En France, anticiper le *Digital Services Act*, ignorer le droit européen existant, *nextinpact.com*, janvier 2021 [consulté le 30 janvier 2021]. Disponible sur : https://www.nextinpact.com/lebrief/45470/en-france-anticiper-digital-services-act-ignorer-droit-europeen-existant

MARS
2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

JURISPRUDENCE JUDICIAIRE

Capitaine Matthieu Audibert

La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?

Cour de justice de l'Union européenne (CJUE), affaire C-746/18, arrêt du 2 mars 2021 H.K/Prokuratuur

Dans la continuité de sa jurisprudence établie depuis 2014[1], la CJUE poursuit l'encadrement des dispositions juridiques liées à la conservation[2] et maintenant à l'accès, à des fins pénales, aux données techniques de connexion. Dans le même temps, la CJUE pose un certain nombre de garanties liées à cet accès qui mettent à mal les prérogatives du procureur de la République et certaines prérogatives du juge d'instruction au regard de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 lue à la lumière de la charte des droits fondamentaux de l'Union européenne (UE).

S'agissant des faits, un individu (H.K) a été condamné en première instance à une peine privative de liberté de deux ans pour avoir commis plusieurs vols, escroqueries et exercé des actes de

1. Arrêt du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., C-293/12 et C-594/12 ; arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15 ; arrêt du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a., C-511/18, C-512/18 et C-520/18.

2. LASSALLE, Maxime, Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE, *Recueil Dalloz 2021*, p. 406.

violences. Pour déclarer coupable cet individu, la juridiction de première instance s'est fondée sur différents actes réalisés par les services d'enquête et notamment l'obtention de données relatives aux communications électroniques. Ces données peuvent être récupérées par les enquêteurs suite à l'autorisation délivrée par le procureur territorialement compétent. Plus précisément, ces données concernent plusieurs numéros de téléphones de l'individu et les différentes identités associées.
Condamné en première instance, il fait appel et celui-ci est rejeté par la cour d'appel estonienne. Il introduit alors un pourvoi en cassation contre cette décision auprès de la Cour suprême de son pays et conteste notamment la recevabilité des procès-verbaux établis à partir des données techniques de connexion récupérées par les enquêteurs sur autorisation du procureur.
Saisie de ce pourvoi, la juridiction suprême estonienne va sursoir à statuer et va adresser trois questions préjudicielles à la CJUE :

« Convient-il d'interpréter l'article 15, paragraphe 1, de la directive [2002/58], lu conjointement avec les articles 7, 8, 11 et 52, paragraphe 1, de la [Charte], en ce sens que l'accès des autorités nationales, dans le cadre d'une procédure pénale, à des données permettant de retrouver et d'identifier la source et la destination d'une communication téléphonique à partir du téléphone fixe ou mobile du suspect, d'en déterminer la date, l'heure, la durée et la nature, d'identifier le matériel de communication utilisé ainsi que de localiser le matériel de communication mobile utilisé constitue une ingérence tellement grave dans les droits fondamentaux garantis par les articlesprécités de la Charte que, lors de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales, cet accès doit être limité à la lutte contre la criminalité grave, indépendamment de la période pour laquelle les autorités nationales

ont accès aux données conservées ?

Convient-il d'interpréter l'article 15, paragraphe 1, de la directive [2002/58] à partir du principe de proportionnalité tel que formulé aux points 55 à 57 de [l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788),] en ce sens que, si la quantité des données visées à la première question, auxquelles les autorités nationales ont accès, n'est pas très importante (tant du point de vue de la nature des données que du point de vue de la longueur de la période concernée), l'ingérence dans les droits fondamentaux qui en découle peut être justifiée de manière générale par l'objectif de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales et que, plus la quantité des données auxquelles les autorités nationales ont accès est importante, plus les infractions pénales contre lesquelles l'ingérence est destinée à lutter doivent être graves ?

Convient-il de considérer que l'exigence figurant au deuxième point du dispositif de [l'arrêt du 21 décembre 2016, Tele2 (C-203/15 et C-698/15, EU:C:2016:970)], selon laquelle l'accès des autorités nationales compétentes aux données doit être soumis à un contrôle préalable par une juridiction ou une autorité administrative indépendante, signifie que l'article 15, paragraphe 1, de la directive [2002/58] doit être interprété en ce sens que l'on peut considérer comme une autorité administrative indépendante le ministère publicqui dirige la procédure d'instruction et qui, ce faisant, est, en vertu de la loi, tenu d'agir de manière indépendante, en étant uniquement soumis à la loi et en examinant, dans le cadre de la procédure d'instruction, à la fois les éléments à charge et les éléments à décharge concernant la personne poursuivie, mais qui représente l'action publique au cours de la procédure judiciaire

ultérieure ? »

Saisie de ces questions préjudicielles, la CJUE va, tout en rappelant sa jurisprudence antérieure sur l'interdiction faite aux États membres de procéder à une conservation généralisée et indifférenciée des données techniques de connexion, préciser que cet accès doit être « circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention des menaces graves contre la sécurité publique »[3] (I).

En outre, la CJUE va indiquer que le droit de l'UE s'oppose à ce que le ministère public, en charge de diriger l'enquête pénale et, le cas échéant, d'engager l'action publique, puisse autoriser l'accès aux enquêteurs aux données techniques de connexion. Ce dernier point implique de nombreuses conséquences pour le Parquet français mais également pour le juge d'instruction (II).

3. Point 60 1).

I. La notion de criminalité grave ou de menace grave contre la sécurité publique comme seul critère autorisant l'accès aux autorités publiques aux données techniques de connexion

Ce nouvel arrêt de la CJUE rappelle une solution qui n'est pas nouvelle (A). Toutefois, combiné à l'arrêt Quadrature du Net, ce nouvel arrêt relatif aux données de connexion est susceptible d'entraîner de lourdes conséquences dans le succès de nombreuses enquêtes judiciaires (B).

A) Une solution non nouvelle dégagée par la CJUE s'agissant de la conservation des données de connexion

Dans ses questions préjudicielles, la Cour suprême estonienne s'interroge sur les modalités d'accès à ces données au regard de l'article 15 §1 de la directive 2002/58. L'accès par les autorités nationales, dans le cadre d'une enquête judiciaire, à ces données constitue-t-il une ingérence tellement grave dans les droits fondamentaux garantis par la Charte que cet accès doit faire l'objet d'une limitation à la lutte contre la criminalité, nonobstant la période pendant les enquêteurs ont eu accès à ces données ?[4]

En outre, la Cour suprême estonienne s'interroge au regard du volume de données concernées. L'argumentation sous-jacente de l'Estonie étant que si le volume de données n'est pas très important, aussi bien s'agissant de la nature de celles-ci que de la période de collecte, cela peut-il justifier que l'ingérence qui en découle dans les droits fondamentaux puisse être justifiée par l'objectif de

4. Point 26 1).

prévention, de recherche, de détection et de poursuite d'infractions pénales ?[5] En outre, de manière implicite, la juridiction estonienne tente de soumettre un accès proportionné à la gravité de l'infraction. Autrement dit, plus l'infraction est grave, plus la quantité de données accessibles serait importante[6].

Dans l'argumentaire du gouvernement estonien, il est intéressant de souligner que l'accès aux données conservées en vertu du droit national estonien peut être sollicité pour tout type d'infraction pénal[7], ce qui est également le cas du droit français[8].

Pour répondre à ces questions préjudicielles, la CJUE rappelle sa jurisprudence antérieure. Tout d'abord, elle subordonne l'accès à ces données à leur conservation de manière conforme au droit de l'Union[9]. Elle rappelle le principe dégagé dans l'arrêt Quadrature du Net du 6 octobre 2020, à savoir que le droit de l'Union s'oppose à des législations nationales prévoyant à des fins pénales, à titre préventif, la conservation généralisée et indifférenciée des données techniques de connexion (de localisation et de trafic)[10] [11].

---

5. Point 26 2).
6. *Ibid*.
7. Point 28.
8. Articles L. 34-1 et R. 10-13 du Code des postes et des communications électroniques et dispositions du Code de procédure pénale, voir par exemple l'article 60-1.
9. Point 29. Voir aussi arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, point 167).
10. Point 30. Voir aussi arrêt du 6 octobre 2020. La Quadrature du Net e.a, c- 1/18, C-512/18 et c-520/18, point 168.
11. LASSALLE, Maxime. Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE. *Recueil Dalloz*, 2021, p. 406.

Ensuite, la CJUE va se livrer à un contrôle de proportionnalité dans l'accès à ces données entre, d'une part, la gravité de l'ingérence dans les droits fondamentaux et, d'autre part, l'objectif d'intérêt général poursuivi[12]. Il s'agit là encore d'un rappel de sa position exprimée dans l'arrêt Quadrature du Net[13]. La CJUE poursuit en indiquant que « seule la lutte contre la criminalité et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés [par la Charte][14] ». Ces ingérences sont notamment celles qui « impliquent la conservation des données relatives au trafic et des données de localisation, qu'elle soit généralisée et indifférenciée ou ciblée[15]».

Sur ce point, la CJUE conclut que « seules des ingérences ne présentant pas un caractère grave peuvent être justifiées par l'objectif (…) de prévention, de recherche, de détection et de poursuite d'infractions pénales en général[16]».

Sur les données, la CJUE fait ensuite la distinction avec les données relatives à l'identité civile des utilisateurs non associées aux données de communication. Pour les premières, considérant que celles-ci ne permettent pas, à elles seules, de connaître les usages de l'utilisateur ou encore sa localisation, la CJUE considère que leur conservation n'est pas en contradiction avec le droit de l'Union[17]. Il

---

12. Points 31 et 32.
13. Arrêt du 6 octobre 2020. La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, point 131.
14. Point 33.
15. *Ibid.*
16. *Ibid.* Voir aussi arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, points 140 et 146.
17. Point 34. Voir aussi arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, points 157 et 158.

convient de souligner que la Cour européenne des droits de l'Homme adopte la même solution s'agissant des données relatives à l'identité civile des utilisateurs[18] [19].

Dans la suite de son raisonnement, la CJUE considère l'accès limité à une quantité limitée de données de connexion comme étant un critère inopérant pour justifier une telle ingérence[20] et rappelle, comme dans l'arrêt Quadrature du Net[21], que le juge pénal est tenu d'écarter « des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès de l'autorité compétente à ces données en violation de ce droit, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits[22]».

Pour conclure sur ces deux questions, la CJUE écarte les critères liés à la durée de l'accès aux données et à la nature des données disponibles pour conclure que le droit de l'Union[23] n'autorise l'accès,

---

18. CEDH, *Brayer contre Allemagne*, 30 janvier 2020, n° 50001/12.
19. DE MONTECLER Marie-Christine, Protection des données : la CJUE infléchit sa jurisprudence, *AJDA*, 2020, p. 1880.
20. Point 40.
21. Arrêt du 6 octobre 2020. La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, points 226 et 227.
22. Point 44.
23. Article 15 §1 de la directive 2002/58, articles 7, 8, 11 et 52 de la Charte des droits fondamentaux.

dans le cadre des enquêtes judiciaires, aux données de connexion permettant de tirer des conclusions sur la vie privée des personnes visées par les investigations, que dans le cadre de la lutte contre la criminalité grave ou pour prévenir des menaces graves contre la sécurité publique[24].

B) Quelles conséquences pour les enquêtes judiciaires ?

Pour commencer, il peut être intéressant de comparer l'appréhension juridique des données techniques de connexion et les données de contenu par les services d'enquête.
D'un point de vue technique, s'agissant des correspondances émises par la voie des communications électroniques, on distingue traditionnellement les données relatives aux contenus et les données techniques de connexion. Les premières contiennent les paroles prononcées ou écrites et les secondes les informations relatives à la connexion des appareils aux réseaux téléphoniques ou à Internet.

Les interceptions de correspondances (donc les données de contenu) sont possibles en matière criminelle et en matière correctionnelle si la peine encourue est égale ou supérieure à trois ans d'emprisonnement[25] dans le cadre d'une information judiciaire. S'agissant de l'enquête de flagrance et de l'enquête préliminaire, les interceptions de correspondances émises par la voie des communications électroniques sont possibles pour l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 du Code de procédure pénale[26].

24. Point 45.
25. Article 100 du Code de procédure pénale.
26. Infractions relatives à la criminalité et à la délinquance organisées.

En revanche, que ce soit en enquête de flagrance[27], en enquête préliminaire[28] ou dans le cadre d'une information judiciaire[29], aucun seuil n'est exigé s'agissant de la possibilité de requérir les opérateurs de communication électroniques aux fins de récupérer des données techniques de connexion. Autrement dit, en droit français, il est possible de récupérer ces données aussi bien pour une contravention que pour un délit ou un crime. Cette différence de traitement entre ces deux types de données se comprend aisément, les premières portant sur les propos ou écrits échangés et les secondes sur les informations techniques relatives à la connexion des appareils aux différents réseaux. Le degré d'intrusion dans la vie privée est donc sensiblement différent.

Avec son arrêt H.K/Prokuratuur, la CJUE reprend ses solutions déjà dégagées dans les arrêts Tele2 Sverige et Quadrature du Net s'agissant de la non-conformité au droit de l'Union de législations nationales prévoyant une conservation généralisée et indifférenciée des données techniques de connexion. L'apport de cet arrêt réside, comme nous l'avons vu précédemment, dans un accès autorisé, à des fins pénales, aux données techniques de connexion uniquement en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique.

Or, réduire les données accessibles aux seules infractions pénales graves n'est pas concevable pour les services d'enquête, notamment parce que la notion « d'infraction grave » exclut de nombreuses possibilités d'investigations. Une réduction drastique

27. Article 60-1 du Code de procédure pénale.
28. Article 77-1-1 du Code de procédure pénale.
29. Article 99-3 du Code de procédure pénale.

du champ de conservation des données et des données accessibles méconnaît les processus d'investigations dont la vocation est aussi de garantir le droit des victimes d'obtenir un jugement et réparation pour le préjudice subi. En outre, au début d'une enquête, il est impossible de déterminer une zone délimitée qui pourrait être celle de l'auteur et de ses éventuels complices. Il est impossible pour les magistrats et les enquêteurs de connaître à l'avance les données dont ils auront besoin pour élucider les enquêtes qu'ils mènent. Enfin, il est impossible de déterminer à l'avance quelles personnes feront l'objet d'investigations[30], à charge comme à décharge. Ainsi, « plus que le dispositif national, ce sera peut-être la méthodologie d'enquête qui devra être revue[31] ».
Par ailleurs, cette possibilité d'accéder aux données de connexion permet d'identifier les auteurs mais aussi et surtout de matérialiser des infractions, de démontrer des liens de complicité ou des coactions[32], de déterminer si les faits ont été commis avec des circonstances aggravantes.

En outre, comme nous venons de le voir, la CJUE n'envisage l'accès aux données de connexion conservées que dans le cadre de la lutte contre la criminalité grave. Or, cette notion de gravité n'est pas explicitée dans l'arrêt et la jurisprudence antérieure de la CJUE relative aux données de connexion. En droit français, cette notion de gravité est déterminée en fonction de l'échelle des peines. Ainsi, un crime est par essence nécessairement grave. Or, s'agissant des délits, la liste des infractions potentiellement concernées par un

30. MOLINS, François. La protection des citoyens européens dans un monde ultra-connecté. Fondation Robert Schuman, *Question d'Europe*, n° 510, 8 avril 2019.
31. NICAUD, Baptiste. CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données. *AJ Pénal*, 2020, p. 531.
32. *op.cit.* note 30.

accès prohibé aux données de connexion est extrêmement longue.

C'est le cas, par exemple, des infractions pouvant être exclusivement commises par la voie des communications électroniques : infractions relatives à la vie privée[33], cyberharcèlement[34], provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance à une ethnie, une nation, une race ou à une religion déterminée[35], la provocation à la haine ou à la violence à raison du sexe ou de l'orientation sexuelle, de l'identité de genre ou du handicap et provocation à des discriminations les concernant[36].

Ces infractions sont-elles graves ? La sanction prévue pour celles-ci varie entre un an et deux d'emprisonnement. L'application stricte de cet arrêt de la CJUE empêcherait donc le recours aux données de connexion pour enquêter sur des infractions de haine en ligne. Or, ces données sont absolument essentielles pour élucider de tels faits. Ainsi, « l'inquiétude pèse tant sur les procédures en cours que sur l'avenir des moyens d'enquêtes[37]» pour élucider ces infractions.

Enfin, l'arrêt de la CJUE faisant suite à une question préjudicielle[38], il appartient à la juridiction nationale qui a saisi la CJUE de résoudre l'affaire, conformément à la décision de la CJUE. En outre, cette décision lie les autres juridictions nationales des pays de l'Union

33. Articles 226-1 et suivants du Code pénal.
34. Article 222-33-2-2 du Code pénal.
35. Article 24 de la loi du 29 juillet 1881 relative à la liberté de la presse.
36. *Ibid.*
37. *op.cit.* note 31, p. 26.
38. Article 267 du Traité sur l'Union européenne.

européenne qui seraient saisies d'un problème similaire. La combinaison des arrêts Quadrature du Net et H.K/Prokuratuur est donc susceptible de remettre profondément en cause les méthodes actuelles d'enquêtes judiciaires[39] [40].

Nonobstant les questions de la conservation et de l'accès à des fins pénales aux données de connexion, la CJUE vient préciser les modalités d'accès à ces données et, notamment, s'agissant du contrôle préalable de cet accès. Ce faisant, elle remet en question les prérogatives du Parquet français et, par extension, certaines prérogatives du juge d'instruction.

II. L'exclusion du ministère public dans le contrôle préalable de certains actes d'enquêtes : vers un nouveau paradigme dans la procédure pénale française ?

Il s'agit ici d'examiner la troisième question posée par la Cour suprême estonienne et la réponse apportée par la CJUE. En effet, au regard de l'article 15, paragraphe 1, de la directive 2002/58 et de l'arrêt Tele2 du 21 décembre 2016, le ministère public est-il compétent pour autoriser cet accès ? Par sa réponse, la CJUE remet en cause certaines prérogatives du ministère public français (A) et, par là même, certaines du juge d'instruction (B).

---

39. DAOUD, Emmanuel, BELLO, Imane, PECRIAUX, Océane. Données de connexion et sauvegarde de la sécurité nationale : l'exception confirme la règle. *Dalloz IP/IT*, 2021, p. 46.

40. *op.cit.* note 31, p. 56.

A) Une remise en cause du Parquet français au travers du ministère public estonien

Pour analyser la possibilité pour le ministère public estonien d'autoriser cet accès, la CJUE va analyser ses caractéristiques. Ainsi, il est « tenu d'agir de manière indépendante », il doit « examiner les éléments à charge et à décharge lors de la procédure d'instruction, l'objectif de cette procédure [étant] la collecte d'éléments de preuve ainsi que la réunion des autres conditions nécessaires à la tenue d'un procès », il « représente l'action publique lors du procès et (…) serait donc également partie à la procédure ». Enfin, il « est organisé de manière hiérarchique »[41].

Tout d'abord, la CJUE va contrôler le respect de l'exigence de proportionnalité dans l'accès aux données. Elle relève ainsi que la loi estonienne autorise au Parquet estonien un accès général à toutes les données sans préciser l'objectif poursuivi[42]. Elle en conclut ainsi que ces dispositions ne respectent pas l'exigence de proportionnalité[43]. Ensuite, la CJUE va ajouter un point fondamental qui impactera certainement le Parquet français. Elle indique « que l'accès des autorités nationales compétentes aux données conservées [doit être] subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité [doit intervenir] à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de

41. Point 47. Voir également CRICHTON Cécile, Précisions sur l'accès aux métadonnées lors du procès pénal, *Dalloz actualité*, 5 mars 2021.
42. Points 49 et 50.
43. *Ibid.*

prévention, de détection ou de poursuites pénales[44] ».

Elle précise que la juridiction ou l'entité de contrôle « [doit disposer] de toutes les attributions et [doit présenter] toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès[45] ». Dès lors, cette juridiction ou entité de contrôle doit avoir « une position de neutralité vis-à-vis des parties à la procédure pénale[46] ».
Dans la mesure où le ministère public estonien dirige l'enquête mais est également susceptible d'exercer l'action publique, la CJUE en conclut que celui-ci ne peut être considéré comme indépendant : il n'a pas la qualité de tiers à la procédure et notamment vis-à-vis des enquêteurs qui demandent l'accès aux données et il peut faire l'objet d'une influence extérieure[47]. Enfin, la CJUE insiste pour rappeler qu'un contrôle de l'accès postérieur n'est pas suffisant, car il doit intervenir dans les plus brefs délais, « préalablement à tout accès, sauf cas d'urgence dûment justifié[48] ».

Forts de ces éléments, examinons la situation du Parquet français.

---

44. Point 51. Voir également arrêt du 6 octobre 2020. La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, point 189.
45. Point 52.
46. Point 54.
47. Points 54-57.
48. Point 58.

Aux termes de la loi, la police judiciaire est exercée sous la direction du procureur de la République[49]. Il exerce l'action publique dans le respect du principe d'impartialité[50], il ne prend donc pas parti dans les enquêtes. Toutefois, c'est lui qui dispose du principe de l'opportunité des poursuites[51] et peut, le cas échéant, mettre en œuvre l'action publique et requérir une condamnation[52]. Enfin, le procureur de la République est placé sous l'autorité du procureur général près la cour d'appel[53].

Or, sur ces points, la CJUE a clairement tranché[54] : le droit de l'Union s'oppose à une législation nationale qui donne compétence au ministère public qui dirige l'enquête judiciaire et exerce, le cas échéant, l'action publique ultérieurement, pour autoriser l'accès aux enquêteurs aux données de connexion.

En droit français, dans le cadre de l'enquête de flagrance, le procureur de la République ou l'officier de police judiciaire, et l'agent de police judiciaire sous le contrôle de ce dernier, peuvent, par réquisition, récupérer les données de connexion intéressant une enquête en cours[55]. Au cours de l'enquête préliminaire, le procureur ou l'officier ou l'agent de police judiciaire, peuvent, sur autorisation du procureur de la République également récupérer ces données, toujours par réquisition[56]. Dans la loi, le contrôle préalable n'existe que dans le cadre de l'enquête préliminaire. En pratique, il existe

49. Articles 12 et 41 du Code de procédure pénale.
50. Article 31 du Code de procédure pénale.
51. Article 40 du Code de procédure pénale.
52. Article 40-1 du Code de procédure pénale.
53. Articles 35 à 37 du Code de procédure pénale.
54. Point 60 2).
55. Article 60-1 du Code de procédure pénale.
56. Article 77-1-1 du Code de procédure pénale.

aussi en enquête de flagrance dans la mesure où il s'agit de réquisitions émises sous frais de justice.

Ainsi, aucun tiers à la procédure, tel un juge des libertés et de la détention, n'intervient pour autoriser cet accès. Seul le procureur de la République est susceptible d'exercer un tel contrôle. Or, comme nous l'avons vu, du fait de son positionnement, il y a d'une part un problème de contrôle préalable tel qu'exigé par la CJUE mais également un problème d'indépendance au sein même de l'enquête dans la mesure où c'est le procureur qui exerce le cas échéant l'action publique à l'issue de l'enquête qu'il dirige.

En conclusion, le Parquet français est clairement menacé par l'arrêt de la CJUE du 2 mars, tant en raison de son positionnement dans la procédure qu'en raison de ses attributions propres.

B) Une remise en cause par ricochet du juge d'instruction ?

À première vue, le juge d'instruction ne semble pas impacté par cet arrêt de la CJUE qui ne traite que du ministère public. Pour autant, certains points de l'arrêt le concernent.

Celui-ci ne représente pas l'action publique. Son rôle est d'instruire à charge et à décharge[57]. Il procède ainsi à tous les actes d'enquête qu'il juge utiles à la manifestation de la vérité. Il peut procéder lui-même à ces actes ou les déléguer aux officiers de police judiciaire par le biais de commissions rogatoires[58]. À cet effet, les officiers de police judiciaire exercent, dans les limites de la commission

57. Article 81 du Code de procédure pénale.
58. Article 151 du Code de procédure pénale.

rogatoire, tous les pouvoirs du juge d'instruction[59].

S'agissant des données de connexion, le juge d'instruction ou l'officier de police judiciaire commis par lui peut, par réquisition, récupérer les données de connexion intéressant une enquête en cours[60]. Ce pouvoir précis va alors rentrer en contradiction avec l'arrêt de la CJUE. Celle-ci explique en substance que celui qui exerce le contrôle préalable doit être un tiers par rapport à celui qui demande l'accès aux données de connexion. L'autorité de contrôle ne doit donc pas être impliquée dans la conduite de l'enquête pénale[61].

Or, lorsque le juge d'instruction requiert en vertu de l'article 99-3 du Code de procédure pénale, aucune entité ne contrôle préalablement sa réquisition. Seule une nullité nécessairement postérieure peut le cas échéant être soulevée[62]. Surtout, le juge d'instruction est impliqué dans l'enquête, car c'est justement son rôle d'informer à charge et à décharge[63]. La CJUE indique que le droit de l'Union « s'oppose à une réglementation nationale donnant compétence au ministère public dont la mission est de diriger la procédure d'instruction pénale (…) pour autoriser l'accès d'une autorité publique aux données [de connexion] aux fins d'une instruction pénale[64] ». Nous pouvons donc en déduire que l'article 99-3 du Code de procédure pénale semble contraire au droit de l'Union.

---

59. Article 152 du Code de procédure pénale.
60. Article 99-3 du Code de procédure pénale.
61. Point 54.
62. Article 170 du Code de procédure pénale.
63. Article 81 du Code de procédure pénale.
64. Point 59.

Le raisonnement pourrait également s'appliquer aux interceptions de correspondances bien que non concernées par cet arrêt. En effet, si en enquête de flagrance et en enquête préliminaire, celles-ci sont autorisées par le juge des libertés et de la détention[65], dans le cadre de l'information, le juge des libertés et de la détention n'intervient pas pour les autoriser[66]. Il serait paradoxal que les données de connexion fassent l'objet d'un traitement plus strict que les données de contenu, objets des interceptions. Pour ces raisons, le juge d'instruction est également menacé par ricochet par cet arrêt de la CJUE.

À cet égard, il convient de s'interroger si la jurisprudence de la CJUE n'incite pas les États membres à tendre vers la création d'un juge de l'enquête : magistrat non impliqué dans la procédure qui serait uniquement chargé, à la demande des enquêteurs ou du procureur de la République ou du juge d'instruction pourtant indépendant, d'autoriser certains actes attentatoires à des droits ou libertés.

65. Article 706-95 du Code de procédure pénale.
66. Article 100 du Code de procédure pénale.

Général d'armée (2S) Marc watin-Augouard

Cour de cassation, Chambre criminelle, n° 20-84.004, arrêt n° 236 du 2 mars 2021, M.A...X ; et autre(s)

Ne relève pas de la procédure de géolocalisation en temps réel (art. 230-32 du Code de procédure pénale – CPP) la localisation d'une personne en dehors du territoire national qui ne s'appuie pas sur un itinéraire ou un positionnement obtenu en temps réel ou qui résulte de l'exploitation de fadettes.

La PJ de Metz identifie un groupe organisé, impliqué dans l'acheminement et la diffusion d'importantes quantités de produits stupéfiants dans le secteur de la Moselle-Est. Les personnes sont mises en examen des chefs de transport, détention, offre ou cession, acquisition et emploi d'une substance ou plante classée comme stupéfiant, de participation à un groupement formé ou une entente établie en vue de la préparation d'un ou plusieurs délits punis de dix ans d'emprisonnement, et de non-justification de ressources, et placées en détention provisoire. Les mis en examen contestent la régularité des opérations de géolocalisation menées en dehors du territoire national, sur les territoires marocains, espagnols et allemands, sans autorisation préalable ou concomitante de ces États.

La chambre de l'instruction ne donne pas suite à leur demande, considérant qu'une mesure de localisation opérée à l'étranger ne saurait s'analyser en une mesure de géolocalisation, faute pour les procès-verbaux d'exploitation de cette mesure de faire état d'une indication précise de lieu.

Pour justifier l'arrêt de la chambre de l'instruction, la Cour de cassation relève que :

- même si les heures de franchissement aller-retour des frontières sont mentionnées, il ne saurait être considéré qu'il y a géolocalisation ;
- la plupart des pièces ne comportent aucune indication précise de lieu, dès lors que l'intéressé franchit la frontière, les procès-verbaux se bornant à indiquer qu'il se rend sur le territoire allemand. L'absence de toute indication sur l'itinéraire ou de la localisation en temps réel sur le territoire étranger exclut la qualification de géolocalisation ;
- la seule indication du pays étranger, d'où les appels paraissent avoir été passés ou reçus provisoirement sans plus ample précision de lieu, ne saurait s'analyser en une mesure de géolocalisation. La seule mention de la date et de l'heure d'arrivée au Maroc d'un des protagonistes ne provient pas d'une opération de localisation en temps réel sur son territoire mais de l'exploitation des fadettes de sa ligne ;
- l'indication d'un déplacement en Espagne « effectué visiblement en avion » ne saurait s'analyser en une mesure de géolocalisation, aucune autre précision n'étant apportée.

Note sur la géolocalisation en temps réel

La géolocalisation en temps réel se distingue de la géolocalisation en temps différé et de la surveillance[67]. Elle a été autorisée par la loi

67. La surveillance des personnes ou des biens est une technique d'enquête qui est mise en œuvre dans le « monde réel » (art. 706-80 CPP).

du 28 mars 2014[68] qui est venue combler le vide juridique consécutif à deux arrêts de la Cour de cassation du 22 octobre 2013[69] tirant les conclusions de la jurisprudence de la Cour européenne des droits de l'Homme[70].

Avant la loi du 28 mars 2014, aucun texte spécifique ne venait encadrer son usage. Dans le cadre d'une information judiciaire, le recours à l'article 81 du CPP semblait autoriser le juge d'instruction à procéder à tous les actes d'information qu'il jugeait « utiles à la manifestation de la vérité ». S'agissant des enquêtes préliminaires ou de flagrance, le Parquet s'appuyait sur l'article 41 du CPP, selon lequel « le procureur de la République procède ou fait procéder à tous les actes d'enquête nécessaires à la recherche et à la poursuite des infractions à la loi pénale », et les articles 60-2 et 77-1-1 dudit Code (réquisition judiciaire concernant des données informatiques).

Dans une délibération du 19 décembre 2013, la Commission nationale de l'informatique et des libertés (CNIL) a rappelé que « l'utilisation de dispositifs de géolocalisation est particulièrement sensible au regard des libertés individuelles, dans la mesure où ils permettent de suivre de manière permanente et en temps réel des personnes, aussi bien dans l'espace public que dans des lieux privés. Le recours à la géolocalisation en temps réel – poursuit-elle – s'apparente à une interception du contenu des communications électroniques prévues aux articles 100 et suivants du Code de procédure pénale, qui font notamment référence à la transcription des correspondances émises par la voie des communications et imposent d'identifier la liaison à intercepter ».

Si la Cour de cassation a validé la géolocalisation dans le cadre d'une

68. Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.
69. Cass.crim, 22 octobre 2013, bull.crim 2013, n° 196 et 197.
70. CEDH, 2 septembre 2010, n° 35623/05, *Uzun c/Allemagne*.

instruction relative à un trafic de stupéfiants, parce qu'elle est mise en œuvre sous le contrôle d'un juge (Cass.crim, 22 novembre 2011, Mohamed X et autres), elle a cependant, à l'occasion des deux arrêts précités, remis en cause cette pratique pour les enquêtes conduites sous la direction du Parquet. Elle était, en effet, contraire à la jurisprudence de la Cour européenne des droits de l'Homme statuant sur la conformité de la géolocalisation à l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. La Cour n'a pas contesté le bien-fondé de la géolocalisation, « nécessaire dans une société démocratique », mais, constatant que la géolocalisation est une ingérence dans la vie privée – protégée par l'article 8§1 de ladite Convention – elle a exigé l'intervention d'un juge pour en contrôler la procédure. Or, il est désormais acquis que le procureur de la République n'est pas considéré comme un magistrat indépendant[71].
Les arrêts de la Cour de cassation ont provoqué un véritable « séisme », dans la mesure où toutes les géolocalisations en cours, dans le cadre d'une enquête préliminaire ou d'une enquête de flagrance, ont été interrompues, sans préjudice des nullités pouvant être prononcées.

La loi du 28 mars 2014 a créé les articles 230-32 à 230-44 du CPP qui ont posé le principe d'un recours à la géolocalisation, en temps réel, d'une personne sans son consentement, d'un véhicule ou d'un objet, à l'insu de son propriétaire ou de son possesseur[72]. Pour le Conseil

71. CEDH, arrêt *Mdevedyev c/ France*, 29 mars 2010 et *Moulin c/France*, 23 novembre 2011.
72. La géolocalisation en temps réel peut aussi être mise en œuvre dans le cadre d'une recherche des causes de la mort ou de la disparition (art. 74, 74-1 et 80-4 du CPP) ou de la recherche d'une personne en fuite (art. 74-2 du CPP).

constitutionnel[73], « la mise en œuvre de ce procédé n'implique pas d'acte de contrainte sur la personne visée ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son ; l'atteinte à la vie privée qui résulte de la mise en œuvre de ce dispositif consiste dans la surveillance par localisation continue et en temps réel d'une personne, le suivi de ses déplacements dans tous lieux publics ou privés ainsi que dans l'enregistrement et le traitement des données ainsi obtenues ».

Selon les termes de cette loi (modifiée par la loi n° 2019-222 du 23 mars 2019), la géolocalisation peut être autorisée pour les besoins des procédures relatives aux infractions punies d'au moins trois ans d'emprisonnement au lieu de cinq (art. 230-32 CPP)[74]. Le juge d'instruction peut l'autoriser pour une durée de quatre mois renouvelable. Dans le cadre d'une enquête préliminaire ou de flagrance, la géolocalisation peut être mise en œuvre sur décision du procureur de la République pour une durée de quinze jours (criminalité organisée) ou de huit jours (autres cas). À l'issue, après autorisation du juge des libertés et de la détention, elle peut être prolongée pour une durée d'un mois renouvelable.

La géolocalisation est aussi possible dans le cadre des enquêtes ou informations judiciaires en recherches des causes de la mort et des blessures (art. 74 et 80-4 du CPP), des enquêtes ou informations judiciaires en recherches des causes de la disparition (art. 74-1 et 80-4 du CPP), des enquêtes en recherches des personnes en fuite (art. 74-2 du CPP).

---

73. Décision n° 2014-693 DC du 25 mars 2014.

74. Par similitude, l'article 67 bis-2 du Code des douanes, qui autorise la géolocalisation dans la cadre des enquêtes douanières, prévoit un seuil d'emprisonnement de 3 ans.

Le Conseil constitutionnel déclare conformes à la Constitution les dispositions de la loi du 23 mars 2019, en considérant, selon les mêmes termes, que sa décision du 23 mars 2014, que « la géolocalisation, mesure de police judiciaire, n'implique pas d'acte de contrainte sur la personne visée, ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son ». En autorisant le recours à la géolocalisation lorsque les nécessités de l'enquête l'exigent pour un crime ou un délit puni d'une peine d'au moins trois ans d'emprisonnement, le législateur n'a pas porté atteinte aux exigences constitutionnelles.

La circulaire CRIM/2014-7/G-1.04.2014 du 1er avril 2014 précise que deux techniques de géolocalisation en temps réel sont mises en œuvre dans le cadre d'une procédure pénale :

– le suivi dynamique d'un terminal de télécommunications ;
– le suivi dynamique par un système (balise) placé sur un moyen de transport[75] ou sur tout autre objet, soit par sa propre technologie (par exemple un smartphone, une tablette, un véhicule par son GPS), soit par l'intermédiaire d'une balise.

Toute personne (et pas uniquement la personne soupçonnée) peut être concernée, dès lors que la mesure relève des « nécessités de

75. Cass.crim, (n° 15-87755), 7 juin 2016, George sX..., Juan Y... « MM. X... et Y... ne sauraient se faire un grief de ce que la chambre de l'instruction a rejeté leur requête par les motifs repris au moyen, dès lors qu'en dehors du recours, par les autorités publiques, à un procédé déloyal, non démontré, ni même allégué, en l'espèce, un mis en examen est irrecevable à contester la régularité de la géolocalisation en temps réel d'un véhicule volé et faussement immatriculé sur lequel il ne peut se prévaloir d'aucun droit. »

l'enquête ».

Le territoire national, limite géographique

L'article 230-32 spécifie bien l'application géographique de la géolocalisation à « l'ensemble du territoire national ». Au-delà des frontières, une mesure de coopération est nécessaire. Les données issues d'une géolocalisation mise en œuvre sur le territoire national et s'étant poursuivie sur le territoire d'un autre État ne peuvent, lorsque cette mesure n'a pas fait l'objet d'une acceptation préalable ou concomitante de celui-ci au titre de l'entraide pénale, être exploitées en procédure qu'avec son autorisation. Dans un arrêt du 9 février 2016[76], la Cour de cassation a statué sur la pose de dispositifs de géolocalisation sur une Renault Clio et une Audi A2, utilisées par les personnes soupçonnées de trafic de stupéfiants, permettant de constater les déplacements de ces véhicules en France, en Belgique et aux Pays-Bas. Ces opérations de géolocalisation ne sont pas légales dès lors que « les demandes d'entraide pénale internationales indispensables à l'utilisation et à l'exploitation de ces données en procédure ne se trouvent pas au dossier de l'information ».

Le calendrier commande

Compte tenu de l'atteinte aux libertés individuelles qu'entraîne la géolocalisation en temps réel, les conditions de forme sont rigoureuses, s'agissant notamment de la prise en compte de la chronologie.

76. Cass.crim, (n° 15-85.070), 9 février 2016, M. X.

Ainsi, le 29 septembre 2020, la Chambre criminelle de la Cour de cassation[77] considère que la pose d'une balise de géolocalisation par un enquêteur agissant en urgence doit faire l'objet d'une information immédiate du procureur de le République ou du juge d'instruction. Dans le cadre d'une information judiciaire, des enquêteurs procèdent un matin, à 3h20, à la pose d'un dispositif de géolocalisation sur un véhicule. Ils agissent en vertu des dispositions de l'article 230-35 du CPP. Ils avisent le juge d'instruction à 9h30. Le véhicule fait également l'objet de mesures de sonorisation. Ces dispositifs combinés permettent l'interpellation et la mise en examen de l'auteur. Celui-ci demande à la Cour l'annulation de la mesure de géolocalisation jugée conforme par la chambre de l'instruction.

La Cour considère qu'en cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, et dans les cas mentionnés aux articles 230-33 et 230-34 du CPP, un officier de police judiciaire peut prescrire ou mettre en place les opérations de localisation en temps réel, par tout moyen technique, d'un véhicule sans le consentement de son propriétaire ou possesseur, à la condition qu'il en informe immédiatement, par tout moyen, le procureur de la République ou le juge d'instruction. « Mais l'OPJ doit en informer immédiatement, par tout moyen, le procureur de la République ou le juge d'instruction ». Cette immédiateté se justifie parce qu'elle permet le contrôle effectif du juge sous lequel est placée la mesure de géolocalisation qui constitue une ingérence dans la vie privée. Elle doit être interprétée strictement. Ainsi, « méconnaît l'article 230-35 du code de procédure pénale et viole l'article 8 de la Convention

77. Cour de cassation – Chambre criminelle – (20-80.915) - Arrêt n° 1715 du 29 septembre 2020.

européenne des droits de l'homme, la chambre de l'instruction qui a déclaré régulière la mesure de géolocalisation quand il résultait de ses constatations que les enquêteurs ont procédé à la pose du dispositif de géolocalisation le 28 février 2019 à 3 heures 20 et que le juge d'instruction n'en a été informé que le 28 février 2019 à 9 heures 30, soit 6 heures 10 plus tard ».
Dans un arrêt du 19 février 2019[78], la Cour de cassation offre un autre exemple de son interprétation « à la minute près » des textes.

En l'espèce, les policiers ont sollicité du procureur de la République la mise en place d'un dispositif de suivi en temps réel d'une véhicule. L'autorisation a été accordée le 22 mars 2017 pour une durée maximale de dix-sept jours consécutifs. Le dispositif a été mis en place le 29 mars 2017 à 23 heures 51. Le 13 avril 2017, les enquêteurs ont sollicité une prolongation de la géolocalisation qui a été autorisée le 14 avril 2017 par le juge des libertés et de la détention pour une durée d'un mois à compter de sa mise en place effective. Cette affaire permet à la Cour de préciser que :

- s'agissant d'une mesure qui porte atteinte à la vie privée, toute journée durant laquelle le dispositif a été fonctionnel, même pendant une période de temps minime, doit être prise en compte dans la computation des délais. Même si la mise en place n'a été effective le 29 mars 2017 que durant quelques minutes, cette journée doit être considérée comme la première du délai de quinze jours autorisé par le procureur de la République ;
- le dispositif pouvait donc être encore exploité durant encore quatorze jours pleins de sorte que l'autorisation était valable

78. Cour de cassation – Chambre criminelle – (18-84.671) – Arrêt n°165 du 19 février 2019.

jusqu'au 12 avril 2018 à minuit. La prolongation n'en a été autorisée par le juge des libertés et de la détention que le 14 avril 2017. Celle-ci est intervenue avant 10 heures 32. L'article 230-33 du CPP n'exige pas une continuité entre l'expiration du délai durant lequel la mesure est autorisée par le procureur de la République et la délivrance de l'autorisation du juge des libertés et de la détention faisant courir, à partir de ce moment, un nouveau délai ;

• l'ordonnance du juge des libertés et de la détention mentionne dans son dispositif que la prolongation est autorisée pour une durée d'un mois « à compter de sa mise en place effective », c'est-à-dire le 29 mars 2017. Toute exploitation de celle-ci postérieure au 28 avril 2017 à minuit est donc irrégulière. L'article 230-33 ne précise pas que la prolongation part de la date initiale, mais l'ambiguïté doit être interprétée dans un sens favorable à la protection des libertés publiques.

Sont donc affectés de nullité tous les actes d'exploitation de la géolocalisation correspondant à la période comprise entre le 13 avril 2017 à minuit et le 14 avril 2017 à 10 heures 32.

Capitaine/Docteur Thibaut HECKMANN

Royal Courts of Justice, [2021] EWCA Crim 128, arrêt du 5 février 2021, cas EncroChat

Les données récoltées par la gendarmerie française, dans le cadre de l'affaire EncroChat, sont jugées recevables par les tribunaux britanniques. Ainsi, les juges britanniques ont décidé que l'implant actif français ne constituait pas une interception judiciaire et ne contrevenait pas aux dispositions légales énoncées dans la loi britannique de 2016 sur les pouvoirs d'investigation.

EncroChat était l'un des plus grands services de communications chiffrées au monde avec environ 60 000 utilisateurs (20 % de Britanniques), dont les fonctionnalités étaient essentiellement exploitées par les criminels. Le service de messagerie EncroChat a été découvert par l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) en 2017 lors d'expertises judiciaires contre le crime organisé. L'enquête s'est accélérée le 10 avril 2020 par la constitution d'une Équipe commune d'enquête (ECE) entre les autorités judiciaires françaises, néerlandaises et britanniques, sous l'égide d'Eurojust, avec le soutien d'Europol. Finalement, le renseignement et la collaboration technique internationale ont abouti à l'accès aux messages déchiffrés des utilisateurs d'EncroChat grâce à la mise en place d'un dispositif technique actif sur les téléphones d'EncroChat dont les serveurs se trouvaient en France. Le logiciel (implant) leur a permis de lire plusieurs millions de messages chiffrés et d'enregistrer les mots de passe de chiffrement des téléphones. Les forces de l'ordre du monde entier

ont ainsi pu procéder à près de 1 100 arrestations, à la saisie de plus de 35 tonnes de drogues et plus de 169 millions d'euros. En droit français, la technique développée par la gendarmerie répond au cadre juridique de la captation de données informatiques constituant une technique spéciale d'enquête prévue par l'article 706-102-1 du Code de procédure pénale : « Il peut être recouru à la mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur [...], telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques ». Cette mesure est strictement encadrée au cours de l'information judiciaire par le juge d'instruction après avis du procureur de la République (article 706-95-12 du Code de procédure pénale). Ainsi, les données récoltées par la gendarmerie française dans le cadre de l'affaire EncroChat sont recevables par les tribunaux français.

EncroChat et le droit britannique

Les autorités françaises ont évoqué, en conférence de presse, avoir développé un dispositif technique, appelé « implant », qui leur a permis d'accéder à des informations cruciales qui ont ensuite été partagées avec la *National Crime Agency* (NCA) du Royaume-Uni. La NCA, dans le cadre de l'opération Venetic, a ainsi pu collecter des milliers de messages avant que la faille de sécurité ne soit connue et que le réseau EncroChat ne mette fin à son service. Décrite par le directeur des enquêtes de la NCA comme « l'opération la plus vaste jamais menée contre le crime organisé », l'opération française a déjà

abouti à 750 arrestations au Royaume-Uni et à la saisie de plus de 55 millions de livres sterling. Cependant, en vertu du droit britannique, les preuves interceptées lors du transfert de message ne peuvent pas être utilisées devant les tribunaux et doivent être utilisées uniquement à des fins de renseignement[79], après l'autorisation d'un Secrétaire d'État et du juge[80].

La position de la défense

Les avocats de quatre accusés ont fait appel de la validité du dispositif technique utilisé par la France et ont demandé à ce que toutes les données récoltées dans le cadre de l'affaire EncroChat soient jugées irrecevables par les tribunaux britanniques[81]. L'argument principal était que le dispositif français constituait une interception des données entre le téléphone et le serveur d'EncroChat. Cependant, l'*Investigatory Powers Act* de 2016 autorise formellement que le contenu des communications obtenues directement et/ou physiquement sur un téléphone ou un ordinateur soit utilisé comme preuve devant un tribunal[82]. L'article reste valable dans le cas où le contenu est extrait physiquement du téléphone (par exemple dans le cas de l'expertise réalisée après la saisie du téléphone) mais également dans le cas où un logiciel est installé sur le téléphone, permettant ainsi l'extraction indirecte des données[83].

---

79. *Part 2, Interception of communication, Investigatory Powers Act 2016, Parliament of the United Kingdom, 29 November 2016.*
80. *« The act introduced a double lock that requires interception warrants to be authorised by a secretary of state and approved by a judge ».*
81. R v Director of Public Prosecutions [2020] EWHC 2967 Admin.
82. Part 5, Equipment Interference, Investigatory Powers Act 2016, Parliament of the United Kingdom, 29 November 2016.
83. *« Equipment interference warrants may authorise both physical interference [...]*

La Cour d'appel met un terme au débat

Ainsi, le 5 février 2021, l'arrêt de la Cour d'appel dans l'affaire A & Others [2021] EWCA Crim 128 a été rendu et permet de mettre un terme au débat. L'arrêt a effectivement rejeté les arguments pour mettre fin à l'utilisation des données obtenues à partir du réseau de communication EncroChat dans les procédures judiciaires. En termes simples, les juges ont affirmé que les données obtenues par les forces de l'ordre françaises et néerlandaises ne constituaient pas une interception mais une intervention directe sur le téléphone et ne contrevenaient donc pas aux dispositions légales énoncées dans la loi de 2016 sur les pouvoirs d'investigation. Les juges ont décidé que, dans un premier temps, les données étaient en réalité stockées temporairement en clair dans la mémoire des appareils puis que les données étaient chiffrées par le téléphone avant d'être transmises chiffrées sur le serveur d'EncroChat. Les juges indiquent que le logiciel permettait de copier les messages du téléphone avant leur chiffrement (directement depuis la mémoire du téléphone) et que ces messages étaient envoyés non chiffrés sur un serveur de la gendarmerie française. Les juges rappellent que, dans ce cas, il ne s'agit pas d'une interception pendant l'envoi (ce que n'autorise pas la loi britannique) et que cela ne constitue donc pas une interception. Les juges précisent que cela se justifie d'autant plus que, lors de la transmission proprement dite, le message est chiffré et donc non exploitable par la gendarmerie française. De plus, ils affirment que les métadonnées obtenues par la gendarmerie (par exemple le nom de l'utilisateur) étaient uniquement présentes dans

and remote interference (e.g. installing a piece of software on to a device over a wired and/or wireless network in order to remotely extract information from the device ».

la mémoire du téléphone et non lors de la transmission, ce qui démontre que les données ont été récupérées dans la mémoire du téléphone et non lors de leur transmission. Dans l'arrêt rendu, les juges comparent le processus à celui de l'envoi d'une lettre : « Le processus consiste à rédiger la lettre (rédaction du message non chiffré), à la mettre dans une enveloppe (chiffrement), à apposer un timbre (destinataire) puis à placer la lettre dans la boîte postale (envoi sur le serveur d'EncroChat) ». Ainsi, seule la récupération du message lors de sa transmission implique une interception mais pas les premiers éléments du processus. L'implant français récupérant le message avant son envoi, cela ne peut constituer une interception en droit britannique. Les juges ont donc conclu que les communications transmises au Royaume-Uni n'ont pas été obtenues pendant leur transmission, mais pendant leur stockage dans la mémoire du téléphone. L'arrêt permet également de préciser que l'interception ne peut être retenue que si elle a lieu directement lors de la transmission des données provenant d'un signal radio, d'un câble ou d'une fibre optique mais pas si les données sont copiées à partir de la mémoire de l'appareil cible. Actuellement, de nombreuses affaires fondées sur des preuves obtenues par les autorités françaises sont jugées devant les tribunaux britanniques ; toutes les contestations judiciaires quant à la légalité de la manière dont ces preuves ont été obtenues par les forces de l'ordre ont été rejetées grâce à l'arrêt de la Cour d'appel dans l'affaire [2021] EWCA Crim 128.

Général d'armée (2S) Marc Watin-Augouard

Tribunal judiciaire de Paris, ordonnance de référé du 4 mars 2021, Présidente de la Commission nationale de l'informatique et des libertés (CNIL)/ Orange, Free, Bouygues Telecom, SFR

Faute de pouvoir agir sur l'hébergeur, l'éditeur ou l'auteur d'un fichier contenant des données médicales à caractère personnel, diffusées de manière illicite, le juge des référés, en application de la Loi pour la confiance dans l'économie numérique (LCEN), enjoint aux fournisseurs d'accès à Internet (FAI) de bloquer l'accès à un service de communication au public en ligne «***.gg ».**

Une violation concernant des données personnelles et médicales de près de 500 000 patients a été révélée au mois de février 2021. Ces données particulièrement sensibles au sens de l'article 9 du Règlement général sur la protection des données (RGPD) ont été illégalement collectées et rassemblées dans un fichier informatique rendu accessible en ligne. Dès la connaissance de cette violation, les services de la Commission nationale de l'informatique et des libertés (CNIL) ont procédé à une opération de contrôle en ligne, en application de la décision n° 2021-028C du 24 février 2021 de sa présidente. Il est apparu qu'un forum de discussion partageait par un lien de téléchargement direct un fichier hébergé sur un serveur tiers et contenant les données concernées. Ce fichier contient 491 840 lignes qui correspondent chacune à une personne bien identifiée. Sur chaque ligne sont mentionnés :

– son nom d'usage (éventuellement accompagné de son nom patronymique) et son prénom ;

– sa date de naissance ;
– son numéro de téléphone fixe et/ou de son portable ;
– son numéro de sécurité sociale (NIR) ;
– son adresse postale et son adresse électronique.

D'autres données sont également publiées : nom et coordonnées du médecin traitant, date de la dernière visite médicale, nom de l'assuré social dont le patient est ayant droit, groupe sanguin, facteur rhésus, existence ou non d'une affection de longue durée. S'ajoutent des commentaires non dénués de données à caractère personnel.

La CNIL tente d'intervenir auprès de l'hébergeur, de l'éditeur et de l'auteur, mais sans succès, situés à l'étranger ou inconnus. Elle se tourne alors vers le juge des référés. L'article 21 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose que : « En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er de la présente loi, le président de la commission peut en outre demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés ».

Le référé est prévu par l'article 6.I-8 de la loi n 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique : « L'autorité judiciaire peut prescrire en référé ou sur requête, à toutes personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ou, à défaut, à toute personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, toutes

mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne. » Par référé d'heure à heure en date du 1er mars 2021, la CNIL demande au juge d'enjoindre la SA Orange, la SAS Free, la SA SFR et la SA Bouygues Telecom de mettre en œuvre ou de faire mettre en œuvre, sans délai et de manière définitive et illimitée, toutes mesures les plus adaptées et les plus efficaces de surveillance ciblées de nature à assurer le blocage effectif du fichier « full fr ********.7z » ou, à défaut, du service de communication au public en ligne « *****.gg » sur les réseaux des défendeurs ou, à défaut, l'adresse URL « https://*****.gg/********.7z ».

Pour faire cesser l'atteinte grave et immédiate aux droits et libertés des personnes, le juge des référés enjoint les sociétés visées *supra* de mettre en œuvre ou de faire mettre en œuvre, sans délai et pour une période de 18 mois à compter de la présente décision, toutes mesures les plus adaptées et les plus efficaces de surveillance ciblées de nature à assurer le blocage effectif, sur leurs réseaux, du service de communication au public en ligne « *****.gg » qui correspond à un nom de domaine national de premier niveau réservé à l'île de Guernesey. Faute de pouvoir obtenir le retrait du fichier, devant le mutisme de l'hébergeur, la société Cloudflare, dont le siège social est à San Francisco, la procédure de blocage est la seule possible.

Tribunal judiciaire de Paris, ordonnance de référé du 25 février 2021, Mme X./ Twitter International Company

La plaignante a créé une chaîne sur la plateforme YouTube ayant vocation à partager les moments de loisirs de sa famille et dont ses

enfants sont les protagonistes principaux. En juillet 2020, elle est alertée de la création d'un hashtag sur la plateforme Twitter, afin de dénoncer une prétendue emprise nocive et une instrumentalisation par elle de ses enfants mis en scène dans les vidéos publiées. Un compte intitulé « X.@X. », accessible à l'adresse URL « https://twitter.com/X. », participe à cette dénonciation sur les réseaux sociaux et incite à sa diffusion la plus large, comme en atteste un procès-verbal de constat d'huissier en date du 21 septembre 2020.
Afin d'interrompre le délai court de prescription, Mme X. dépose une plainte avec constitution de partie civile du chef de diffamation publique envers un particulier, en date du 23 octobre 2020, auprès du doyen des juges d'instruction du tribunal judiciaire de Paris. Craignant un risque de dépérissement de la preuve, eu égard à l'état d'avancement du dossier devant le magistrat, elle saisit le tribunal par voie de référé sur la base des articles 145 du Code de procédure civile et 6- I.2, 6-I.8 et 6.II alinéas 1 et 3 de la loi n° 2004-575 du 21 juin 2004 (LCEN).

Art 145 CPC (référé expertise)
« S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. »

Art 6-I.2 LCEN
« Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des

destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère manifestement illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible. »

Art 6-I. LCEN

« L'autorité judiciaire peut prescrire en référé ou sur requête, aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ou, à défaut, à toute personne dont l'activité est d'offrir un accès à des services de communication au public en ligne, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne. »

Art.6. II al 1 et 3

« Les personnes mentionnées aux 1 et 2 du I (*ndlr* : voir art. 6-I ci-dessus) détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification

prévues au III.
L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa. »

La plaignante demande que Twitter soit enjoint à lui fournir l'ensemble des données d'identification en sa possession et notamment les IP de connexion, les ports sources de connexion, les nom et prénom, la dénomination sociale, les adresses postales associées, les adresses de courrier électronique associées et les numéros de téléphone utilisés lors de la création du compte Twitter « X. », accessible à l'adresse URL incriminée ainsi que l'ensemble des données d'identification associées aux publications litigieuses, accessibles à d'autres URL. Le décret du 25 février 2011[84] précise la liste des données collectées par les hébergeurs pour chaque opération de création de contenu (article 1er) et la durée de conservation requise (article 3), celle-ci étant d'un an à compter de la résiliation du contrat souscrit lors de la création d'un compte ou de la fermeture de celui-ci pour ce qui concerne les données fournies lors de la souscription du compte considéré.
Twitter conteste la procédure suivie en considérant que le référé vient s'ajouter à une ouverture d'information. Le tribunal rejette cette objection : « Le motif légitime, en l'espèce, dont peut se prévaloir Mme X., consiste à établir la preuve de l'identité du possesseur de compte Twitter, éventuels auteurs des dommages dont elle se dit victime. Il lui appartient, qu'il s'agisse de responsabilité civile ou pénale, d'exposer le fait personnel de

84. 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.

l'auteur, pour lequel elle entend voir dévoiler l'anonymat. […] Le dépôt d'une plainte avec constitution de partie civile du chef de diffamation publique, auquel il a été procédé en l'espèce le 23 octobre 2020, permettant d'empêcher la prescription de l'action publique, n'exclut pas, en soi, la possibilité de solliciter une mesure d'instruction sur le fondement de l'article 145 du Code de procédure pénale, dès lors que l'intervention du juge d'instruction ne se limite nullement à la recherche de l'auteur des propos litigieux et qu'est établie l'existence d'un motif légitime tenant, notamment, à la durée de conservation des données d'identification ».
Sur la communication des données, le tribunal , afin de garantir la proportionnalité de la mesure ordonnée, limite la demande d'identification aux seules données utiles à la réunion des éléments susceptibles de commander la solution du litige potentiel, eu égard aux données que l'hébergeur est amené à collecter en application des dispositions de l'article 1er du décret du 25 février 2011, soit :
– les types de protocoles et l'adresse IP utilisés pour la connexion au service ;
– au moment de la création du compte, l'identifiant de cette connexion ;
– la date de création du compte ;
– les nom et prénom ou la raison sociale du titulaire du compte ;
– les pseudonymes utilisés ;
– les adresses de courrier électronique ou de comptes associés.

On notera que la conservation des données de connexion est un sujet qui oppose la France à la Cour de justice de l'Union européenne. Cette juridiction a récemment encore (arrêt du 6 octobre 2020, Quadrature du Net contre gouvernement français – voir *La veille juridique* n° 91, novembre 2020, p. 13-29), condamné l'obligation généralisée et indifférenciée de collecte et de

conservation des données, confirmant ainsi sa jurisprudence Tele2 (arrêt du 21 décembre 2016). Fort de cet arrêt, Free vient de saisir le Conseil d'État.

AVRIL
2021

CREOGN
CENTRE DE RECHERCHE
DE L'ECOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Général d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE ADMINISTRATIVE

Conseil d'État, ordonnance de référé du 12 mars 2021, Association Interhop et autres / Doctolib

Le traitement des rendez-vous pour la vaccination anti-Covid-19 par le site Doctolib, bien qu'hébergé par une société filiale d'une société américaine, n'est pas contraire au Règlement général sur la protection des données (RGPD).

Pour faciliter et accélérer la campagne de vaccination contre la Covid-19, le ministère des Solidarités et de la Santé a confié la gestion de prise de rendez-vous de vaccination à trois sociétés différentes, parmi elles Doctolib. Cette société héberge ses données auprès de la société de droit luxembourgeois AWS Sarl, filiale de la société américaine Amazon Web Services Inc. La société AWS est certifiée « hébergeur de données de santé » en application de l'article L. 1111-8 du Code de la santé publique.
Les données qu'elle traite sont hébergées dans des datacenters situés en France et en Allemagne. Le contrat conclu entre la société Doctolib et AWS ne prévoit pas le transfert de données pour des raisons techniques aux États-Unis. Par ailleurs, Doctolib et AWS ont conclu un *addendum* au contrat sur le traitement des données qui instaure une procédure précise en cas de demandes d'accès par une autorité publique aux données traitées pour le compte de Doctolib et qui prévoit notamment la contestation de toute demande ne respectant pas la réglementation européenne. Enfin, pour interdire l'accès aux données par des tiers, Doctolib a également sécurisé les données hébergées par la société AWS par une procédure de

chiffrement reposant sur un tiers de confiance situé en France.
Malgré ces précautions, plusieurs associations ont saisi le juge référé du Conseil d'État en vue d'ordonner la suspension du partenariat avec la société Doctolib, concernant l'hébergement des données de santé auprès d'une société américaine, au motif qu'il serait incompatible avec le RGPD (art. 44 à 48). Pour étayer leur demande, elles se sont appuyées sur le Règlement mais aussi sur la jurisprudence de la Cour de justice de l'Union européenne (arrêt Grande chambre C-311/18 du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems*).
S'agissant du RGPD, les données traitées par la plateforme Doctolib seraient, selon les requérants, susceptibles de donner une indication précise sur l'état de santé de la personne et constituent des informations directement identifiantes. Ils ajoutent que les potentielles demandes d'accès aux données personnelles par les autorités américaines ne peuvent faire l'objet d'aucune opposition concrète par les sociétés américaines, que ces accès sont massifs, indiscriminés et non minimisés, et qu'elles ne peuvent faire l'objet de contrôles ou de droit d'opposition auprès d'autorités indépendantes. Ce traitement est donc, selon eux, incompatible avec le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les requérants soulignent que, du fait de sa qualité de filiale d'une société de droit américain, la société AWS pourrait faire l'objet de demandes d'accès à certaines données de santé par les autorités américaines, dans le cadre de programmes de surveillance fondés sur l'article 702 de la loi américaine FISA (*Foreign Intelligence Surveillance Act*) ou sur l'*Executive Order* (E.O.) 12333. Pour invalider le *Privacy Shield*, la Cour de justice de l'Union européenne (CJUE) avait relevé que les activités de la NSA fondées sur l'E.O. 12333 ne

font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels.

Le FISA, du 25 octobre 1978, autorise, sous le contrôle de l'*United States Foreign Intelligence Surveillance Court* (FISC), les programmes de surveillance de type PRISM ou UPSTREAM, certifiés chaque année par l'*Attorney General* et le Directeur du renseignement national (DNI). Le programme PRISM oblige les fournisseurs de service Internet à fournir à la NSA toutes les communications envoyées et reçues par un « sélecteur », une partie d'entre elles étant également transmise au FBI et à la *Central Intelligence Agency* (CIA) (agence centrale de renseignement). En ce qui concerne le programme UPSTREAM, les entreprises de télécommunications exploitant la « dorsale » de l'Internet (réseau de câbles sous-marins, terrestres, commutateurs et routeurs) doivent autoriser la NSA à copier et à filtrer les flux de trafic Internet pour recueillir des communications envoyées par un ressortissant non américain visé par un « sélecteur », reçues par lui ou le concernant. Ces flux concernent aussi bien les métadonnées que les contenus.

L'*Executive Order* n° 12333 permet à la NSA d'accéder à des données « en transit » vers les États-Unis, en accédant aux câbles sous-marins (notamment ceux qui relient l'Europe aux États-Unis), de les recueillir et de les conserver avant qu'elles n'arrivent aux États-Unis, échappant ainsi aux règles de contrôle du FISA. Les activités fondées sur l'E.O. 12333 ne sont pas régies par la loi. Alors que les ressortissants de l'Union européenne disposent de voies de recours dans le cadre du FISA, lorsqu'ils ont fait l'objet d'une surveillance électronique illégale à des fins de sécurité nationale, il n'en est pas ainsi dans le cadre de l'E.O 12333. Les activités de la NSA fondées sur l'E.O. 12333 ne font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels.

Le Conseil d'État donne tort aux associations requérantes : « Les données litigieuses comprennent les données d'identification des personnes et les données relatives aux rendez-vous mais pas de données de santé sur les éventuels motifs médicaux d'éligibilité à la vaccination, les personnes intéressées se bornant, au moment de la prise de rendez-vous, à certifier sur l'honneur qu'elles entrent dans la priorité vaccinale, qui est susceptible de concerner des adultes de tous âges sans motif médical particulier. […] le niveau de protection des données de prise de rendez-vous dans le cadre de la campagne de vaccination contre la Covid-19 ne peut être regardé comme manifestement insuffisant au regard du risque de violation du règlement général de protection des données invoqué par les requérants ».

JURISPRUDENCE JUDICIAIRE

Cour de cassation, Chambre criminelle (n° 20-85.556), arrêt n° 392 du 30 mars 2021, M. A... X...

La mention du nom du magistrat figurant dans la réquisition informatique établie pour saisir la Plateforme nationale des interceptions judiciaires (PNIJ), qui suit le visa des articles qui imposent son autorisation et serait sans objet si celle-ci n'avait pas été donnée préalablement, a la même valeur qu'une mention expresse en procédure par procès-verbal de l'enquêteur.

Cet arrêt un peu technique illustre l'encadrement juridique des interceptions judiciaires, dans le cadre d'une enquête.
À l'occasion d'une enquête préliminaire relative à un trafic de stupéfiants, les enquêteurs ont adressé des réquisitions à la PNIJ. La chambre de l'instruction ayant rejeté la demande de la personne

mise en examen qui invoquait l'irrégularité de la procédure, la Cour de cassation est saisie.

À l'appui de son pourvoi, la personne en cause produit un moyen selon lequel les réquisitions faites en enquête préliminaire aux opérateurs de télécommunication qui prennent la forme d'une consultation de la PNIJ nécessitent l'autorisation préalable du Parquet. Or, selon le requérant, la preuve de cette autorisation ne ressort pas du document généré lors de l'envoi de la réquisition à la PNIJ, à l'occasion de laquelle l'officier de police judiciaire doit mentionner le magistrat en charge de la procédure. C'est donc en violation manifeste des articles 77-1-1, 77-1-2 et 230-45 du Code de procédure pénale, et de l'article 593 du même Code, que la chambre de l'instruction a refusé d'annuler les réquisitions réalisées par ce biais, en considérant que l'autorisation du Parquet résulte de l'édition « du document généré pour chaque réquisition ainsi adressée à la PNIJ ».

LA PNIJ

Article 230-5 du CPP

« I. - Un décret en Conseil d'État, pris après avis public et motivé de la Commission nationale de l'informatique et des libertés, détermine les missions et les modalités de fonctionnement de la plateforme nationale des interceptions judiciaires.

Sauf impossibilité technique, les réquisitions et demandes adressées en application des articles 60-2, 74-2, 77-1-2 ,80-4, 99-4, 100 à 100-7, 230-32 à 230-44, 706-95 et 709-1-3 du présent code ou de l'article 67 bis-2 du code des douanes sont transmises par l'intermédiaire de la plate-forme nationale des interceptions judiciaires qui organise la centralisation de leur exécution.

Les dispositions du présent code relatives au placement des enregistrements sous scellés fermés et à l'établissement d'un

procès-verbal lorsqu'il est procédé à leur destruction ne sont pas applicables aux données conservées par la plateforme nationale des interceptions judiciaires.
Le décret mentionné au premier alinéa du présent I fixe également les modalités selon lesquelles les données ou correspondances recueillies en application des articles 230-32 à 230-44, 706-95-20 et 709-1-3 du présent code sont, sauf impossibilité technique, centralisées et conservées par la plate-forme nationale des interceptions judiciaires.
II. - La plateforme nationale des interceptions judiciaires est placée sous le contrôle d'une personnalité qualifiée, assistée par un comité qui comprend parmi ses membres un député et un sénateur. Les missions, la composition, l'organisation et le fonctionnement du comité sont précisés par décret en Conseil d'Etat. »

Décret n° 2017-614 du 24 avril 2017 portant création d'un service à compétence nationale dénommé « Agence nationale des techniques d'enquêtes numériques judiciaires » et d'un comité d'orientation des techniques d'enquêtes numériques judiciaires

« Article 1
Il est créé un service à compétence nationale relevant du garde des sceaux, ministre de la justice, dénommé "Agence nationale des techniques d'enquêtes numériques judiciaires". Ce service est rattaché au secrétaire général du ministère de la justice

L'agence est placée sous l'autorité d'un directeur, chef de service. L'agence peut bénéficier du concours d'agents détachés ou mis à sa disposition par d'autres ministères, notamment ceux dont les services recourent à la plate-forme nationale des interceptions judiciaires.

Article 2
L'Agence nationale des techniques d'enquêtes numériques judiciaires met en œuvre la plate-forme nationale des interceptions judiciaires prévue au chapitre VI du titre IV du livre Ier du code de procédure pénale.

[…] »

Le requérant reproche l'absence de procès-verbal indiquant le destinataire de la demande et la nature des informations demandées , conformément aux dispositions de l'article R 15-33-71 du Code de procédure pénale. Il ajoute qu'une autorisation du Parquet d'ouvrir une enquête préliminaire ne vaut pas autorisation pour chaque réquisition susceptible d'être sollicitée par l'officier de police judiciaire durant cette enquête.
La Cour lui donne tort et rejette son pourvoi :
– en mentionnant dans le cadre « Magistrat » des formulaires de réquisition le nom d'un vice-procureur de la République, l'enquêteur a indiqué agir en conformité avec les prescriptions du Code de procédure pénale, c'est-à-dire avec l'autorisation préalable de ce magistrat, dont il doit être rappelé qu'elle n'est soumise à aucun formalisme ;
– cet accord résulte également des instructions de ce magistrat telles que rapportées dans le procès-verbal d'investigation (D13), avant les pièces relatant les premières investigations réalisées en exécution de ces instructions ;
– il était permis au procureur de la République d'autoriser de façon générale, sur le fondement de l'article 39-3 du Code de procédure pénale, dans le cadre de l'enquête préliminaire qu'il avait ordonnée, les enquêteurs à procéder à des réquisitions auprès de la PNIJ ;

Article 39-3 du CPP

« Dans le cadre de ses attrributions de direction de la police judiciaire, le procureur de la République peut adresser des instructions générales ou particulières aux enquêteurs. Il contrôle la légalité des moyens mis en œuvre par ces derniers, la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits, l'orientation donnée à l'enquête ainsi que la qualité de celle-ci.

Il veille à ce que les investigations tendent à la manifestation de la vérité et qu'elles soient accomplies à charge et à décharge, dans le respect des droits de la victime, du plaignant et de la personne suspectée. »

– l'édition de la réquisition informatique vaut le procès-verbal exigé par l'article R. 15-33-71 du Code de procédure pénale ;

Article R 15-33-71 du CPP

« Toute demande de mise à disposition fait l'objet de la part de l'officier de police judiciaire d'un procès-verbal indiquant le destinataire de la demande et la nature des informations demandées.

Dans le cas prévu par l'article 77-1-2, le procès-verbal mentionne l'accord préalable du procureur de la République qui peut être donné par tout moyen. »

– la mention du nom du magistrat figurant dans la réquisition informatique établie pour saisir la PNIJ, qui suit le visa des articles qui imposent son autorisation et serait sans objet si celle-ci n'avait pas été donnée préalablement, a la même valeur qu'une mention expresse en procédure par procès-verbal de l'enquêteur.

Lieutenant Océane GERRIET

La carte nationale d'identité numérique : une réalité pour une pluralité d'enjeux

La mise en œuvre de la carte nationale d'identité électronique (CNIe) nécessite de modifier le décret n° 55-1397 réglementant la CNI pour prévoir, notamment, l'intégration du composant électronique et le fichier des cartes identités et des passeports couramment nommé « fichier TES » (fichier des titres électroniques sécurisés) qui collecte ces données. Dans une délibération n° 2021-22 du 11 février 2021, la Commission nationale de l'informatique et des libertés (CNIL) donne son aval, tout en se montrant réservée sur les interconnexions avec d'autres fichiers et émet des recommandations sur la sécurité du traitement.

« Multipass ! » Les fans de science-fiction reconnaîtront la référence au film de Luc Besson qui se déroule au XXII^{e} siècle et où l'héroïne présente ce qui s'apparente à une carte d'identité électronique. Nous ne sommes pas en 2263 et nous y sommes déjà ! Après le déploiement (avec succès) des passeports électroniques dans plus d'une centaine de pays, c'est au tour de la carte nationale d'identité de se « numériser ». L'idée d'une CNIe n'est pas nouvelle puisqu'elle est débattue depuis les années 2000. D'une part, il y a l'impérieuse nécessité de lutter contre les risques d'usurpation et de détournement d'identité. À l'heure du numérique où la donnée est devenue le nouvel or noir et où les fuites de données sont de plus

en plus courantes[1], les données d'identité n'ont jamais été aussi exposées. D'autre part, et bien que cela ne soit pas mentionné dans le décret, derrière la CNIe se joue aussi le développement de **l'identité numérique**[2]. En effet, à l'heure où l'administration renforce sa dématérialisation et où les citoyens ont recours à de multiples comptes sur des plateformes sociales ou commerciales, l'enjeu de transparence et de sécurité de l'identité numérique n'a jamais été aussi fort[3]. Le règlement 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit eIDAS) du 23 juillet 2014 est venu poser une première pierre, et pas des moindres, visant à garantir la sécurité des systèmes d'identification et d'authentification numériques. C'est ce règlement qui a mené au développement de FranceConnect (un système d'identification et d'authentification offrant un accès universel aux administrations en ligne), permettant de se connecter à certains services de l'État à l'aide de quelques identifiants (notamment les impôts) et à ALICEM (application téléphonique permettant de prouver son identité sur Internet grâce à son passeport et à la reconnaissance faciale).

En tous les cas, pour en revenir à la CNIe, c'est bien le règlement 2019/1157 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union (…) du 20 juin 2019 qui impose aux États membres de mettre en place des documents d'identité biométriques sécurisés comprenant photos et empreintes digitales.

---

1. En 2020, la CNIL déclarait qu'il y avait eu plus de 2 000 notifications de violation de données. Mais on a encore en mémoire les fuites de plusieurs millions de données chez Facebook en 2018, chez Uber en 2016, etc.

2. EYNARD, Jessica (dir.). *L'identité numérique : quelle définition pour quelle protection ?* Larcier, 2020, 212 p.

3. Sur ce point, lire le rapport de mission parlementaire sur l'identité numérique.

Pour l'Europe, ces données diminuent le risque de fraude et renforcent *de facto* la liberté des citoyens de l'Union en permettant leur circulation. Bien évidemment, ces données doivent être sécurisées et le règlement pose ainsi des normes minimales afin de garantir une « Union plus sûre ».

Ce règlement entrant en vigueur le 2 août 2021, la France devait donc rapidement transposer ces dispositions, ce qui est chose faite avec le décret n° 2021-279 du 13 mars 2021. Que modifie-t-il concrètement ?

Dans un premier temps, il vient modifier la réglementation relative à la CNI. Cette dernière liste les données collectées sur le titre d'identité et prévoit désormais la présence d'un composant électronique qui comprend ces données (y compris donc la photographie et l'empreinte digitale des doigts qui devient obligatoire sauf pour les mineurs de 12 ans), à l'exception de la signature, du code de lecture automatique[4] et du numéro du support. En outre, le décret prévoit que la CNIe comportera un cachet électronique visible comportant certaines informations (nom, prénom, sexe, nationalité, lieu et date de naissance, type de document, numéro du titre et date de délivrance). De quoi s'agit-il exactement ? Il s'agit d'un code à barres 2D (comme un QR Code) qui encodera certaines données précitées. Enfin, le décret aligne la durée de validité des titres pour fixer celle de la CNIe à 10 ans.

Dans un second temps, il vient modifier la réglementation relative

4. Qui permet de lire automatiquement les informations suivantes : le nom de famille, le ou les prénom(s), la date de naissance, le sexe et la nationalité du titulaire, le type de document, l'État émetteur, le numéro du titre et sa date de fin de validité.

au fichier TES et c'est sur ce point que la question est plus délicate. En effet, en 2016, la Quadrature du Net avait déjà attaqué le fichier TES, estimant que la collecte de ces données d'identités biométriques alliée à la reconnaissance faciale générait une « surveillance généralisée de la population »[5]. Mais le Conseil d'État[6] avait rejeté leurs prétentions en rappelant notamment qu'aucun dispositif de reconnaissance faciale n'était déployé. Ce n'est pas donc pas par hasard que **la CNIL rappelle et souligne que TES est un « fichier singulier », d'une « ampleur inégalée » et « sensible », eu égard aux « données biométriques qu'il contient »**. Sur ce point, si elle ne conteste pas le besoin légitime d'avoir recours à ce type de données pour fiabiliser l'authentification des personnes, elle rappelle que **ces données doivent être conservées « sur un support dont la personne a l'usage exclusif »**. C'est d'ailleurs la position de principe du règlement européen dans son considérant 18. Or, ce n'est pas ce qui est prévu avec leur collecte dans TES. Sur ce point, la CNIL rappelle également qu'elle était opposée à la collecte de ces données dans un traitement centralisé pour les passeports électroniques, ce qui n'a pas empêché le gouvernement d'y procéder et le Conseil d'État de valider le principe, tant pour les passeports[7] que pour la CNI[8]. Dès lors, elle estime que cette collecte ne peut être admise que dans la mesure où « des exigences impérieuses en matière de sécurité ou d'ordre public le justifient ».

---

5. Le fichier TES, prémisse à la reconnaissance faciale de masse, arrive devant le Conseil d'État [en ligne]. *La Quadrature du Net*. 26 septembre 2018. Disponible sur : https://www.laquadrature.net/2018/09/26/audience_tes/

6. CONSEIL D'ÉTAT, 10ème - 9ème chambres réunies, n° 404996, 18 octobre 2018, Inédit au recueil Lebon [en ligne]. Légifrance. Disponible sur : https://www.legifrance.gouv.fr/ceta/id/CETATEXT000037507135/

7. CE, Ass., 26 oct. 2011, n° 317827.

8. *Op. cit.* note 5.

La CNIL analyse ainsi **les finalités poursuivies** par le traitement TES. Elle constate un élargissement (« lutter contre l'usurpation d'identité ») mais qui n'est que le prolongement logique des finalités initiales (« permettre l'instruction des demandes relatives à ces titres et prévenir et détecter leur falsification et leur contrefaçon »). Elle souligne néanmoins qu'il convient de respecter strictement cette finalité en s'assurant que l'accès à ces données sensibles soit réservé au porteur du titre.

Ensuite, **s'agissant de la durée de conservation**, la CNIL rappelle que d'autres pays européens ont fait le choix de la CNIe et de ne pas détenir une telle base centralisée. Mieux encore, ces pays ont fait le choix de ne pas conserver les données biométriques plus de 90 jours après la délivrance ou le refus de délivrance du titre et ce, conformément aux recommandations du règlement européen. Or, la France fait le choix par défaut de détenir un tel traitement et de conserver ces données pendant 10 ans. Si l'autorité de régulation salue le passage de 15 à 10 ans de la durée de conservation, elle regrette que les justifications motivant le titre électronique (diminuer le risque de fraude) n'entraînent pas, *de facto*, une réduction plus forte de la durée de conservation. Cependant, elle prend acte des nouveaux risques générés et rappelle que le Conseil d'État a déjà validé ce type de durée[9]. Néanmoins, elle souligne que les différentes subtilités sur les durées de conservation sont complexes et appelle de ses vœux à une meilleure lisibilité du dispositif, notamment lors de l'information des personnes concernées. En effet, **le décret prévoit la possibilité pour les personnes concernées de demander à ce que l'image de ses empreintes ne soit pas conservée dans le fichier TES plus de 90**

9. *Op. cit.* notes 5 et 6, p. 102.

jours à compter de la date de délivrance ou de refus de délivrance du titre. Si cette information est bien communiquée aux personnes concernées, la CNIL constate qu'elles ne sont pas informées de la conservation d'une copie papier de ces données pour 15 ans. Enfin, afin de garantir le respect du choix des personnes, elle exige une suppression automatique (et non manuelle à ce jour) des données biométriques du traitement.

Dans un autre paragraphe, la CNIL revient sur les **différentes interconnexions** prévues par TES. **Sur l'interconnexion avec le fichier de vérification des titres (DOCVERIF)**, elle rappelle que TES transmet déjà des données à DOCVERIF mais de manière limitée et notamment en fonction du statut du titre (perdu, volé ou invalidé). Désormais, les données transmises font fi de ce critère au motif que la vérification de l'authenticité du titre et de la personne concernée nécessite la collecte de plus d'informations. La CNIL met en garde le ministère de ne pas créer « une base miroir » de TES dans DOCVERIF qui poursuit, lui, des finalités bien distinctes (« contrôle des titres ») et ne prévoit pas, en l'état, la collecte de ces nouvelles données. Le ministère va donc devoir rapidement se mettre en conformité sur ce point. **Sur l'interconnexion avec les logiciels de rédaction de procédure pénale de la police nationale et de la gendarmerie nationale (LRPPN/LRPGN)**, elle rappelle que sa mise en œuvre est fixée à la fin d'année 2021 et vise à recueillir les informations du titre lors de la rédaction d'une déclaration de vol. La CNIL ne remet pas en cause l'utilité « opérationnelle » de cette interconnexion, d'autant qu'elle vise également à fiabiliser les

10. Ce fichier européen vise à permettre une politique commune de gestion des flux au sein de l'espace Schengen, notamment pour garantir la sécurité publique et comprend, à ce titre, les identités des personnes signalées.

données transmises au Système d'information Schengen (SIS)[10]. Néanmoins, une nouvelle fois, elle constate l'élargissement des données transmises (avant, il n'y avait que le numéro du titre et son statut) et s'interroge sur la justification évoquée (vérifier que le plaignant est bien le titulaire légitime) alors qu'elle constate dans le même temps la transmission des signalements à SIS. Enfin, elle constate que, si la photographie n'est pas enregistrée dans la procédure, le ministère devra apporter plus de garanties quant au respect de ce critère.

Enfin, la CNIL se montre pointilleuse **sur la sécurité du traitement**. Premièrement, elle souligne qu'un système de chiffrement a été mis en place mais regrette que les moyens de déchiffrement soient détenus par le ministère de l'Intérieur et l'Agence nationale des titres sécurisés (ANTS). Afin de garantir que ce traitement ne soit pas utilisé comme base d'identification et afin de renforcer sa sécurité, elle recommande de scinder en deux le système de chiffrement, comme recommandé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Deuxièmement, elle appelle alors l'ANTS à étudier la possibilité de conserver les empreintes digitales sous forme de gabarits[11]. Troisièmement, elle exige que le ministère relève le niveau d'exigence attendu pour la sécurité lorsqu'il passe des contrats de prestation. Quatrièmement, et dans le prolongement de ses interrogations sur les interconnexions, elle souhaite que les audits de sécurité intègrent

11. Sur son site, la CNIL définit le gabarit biométrique comme « les mesures qui sont mémorisées lors de l'enregistrement des caractéristiques morphologiques (empreinte digitale, forme de la main, iris...), biologiques (ADN,urine, sang...) ou comportementales (démarche, dynamique de tracé de signature...) de la personne concernée ». Il est dit « maîtrisé » quand sa conservation est inexploitable en l'absence d'intervention ou d'action de la personne concernée.

cette dimension. Enfin, et pour faire écho à la position qu'elle a adoptée dans d'autres traitements, elle rappelle que la durée de conservation des traces et journaux techniques est de 6 mois, sauf à démontrer que certains risques justifient une conservation plus longue.

Pour conclure, la CNIL n'oppose pas de résistance majeure à la CNIe et au fichier TES. Elle émet mêmes des recommandations plus générales sur l'identité numérique qui n'est pas « l'objet du projet de décret soumis » mais qui répond à des besoins et problématiques sous-jacents. Comme le souligne le rapport d'information parlementaire de juillet 2020 relatif à l'identité numérique, cette notion « n'est pas simple à définir », car « à la fois sociologique et technique ». Nous évoquions en introduction le règlement eIDAS qui définit des procédures d'authentification et d'identification sécurisées, au nombre desquelles figure la signature électronique. Est-ce que notre future CNIe deviendra un de ces moyens ? Si le décret présenté par le ministère de l'Intérieur n'y fait pas référence, la CNIL précise que le ministère l'a informée vouloir intégrer ce dispositif dans ALICEM et FranceConnect. À ce titre, la CNIL souligne qu'il faudra être vigilant en développant, à l'instar de l'Allemagne, des dispositifs d'identification sélectifs divulguant plus ou moins de données selon le service en cause (elle cite l'exemple de la justification de l'âge pour jouer à un jeu d'argent qui ne nécessite pas de divulguer toutes les données présentes sur le titre). Elle note également qu'il faudra veiller aux problématiques d'inclusion numérique à l'heure où tous les Français ne sont pas encore familiers de ces usages, voire ne disposent pas

12. Voir, sur ce point, les constats de la mission « société numérique » et le plan national adopté en conséquence : https://societenumerique.gouv.fr/plannational/

d'équipements[12]. Des initiatives existent déjà, comme le démontrent le « pass numérique » permettant à certains publics de se former et le renforcement des enseignements numériques dans l'enseignement secondaire. Ainsi, derrière notre future CNIe se dessine sans aucun doute une partie de notre future identité numérique qui se veut plus sûre et sécurisante.

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS
DE LA GENDARMERIE NATIONALE

MAI
2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Capitaine Matthieu AUDIBERT

Conservation des données de connexion Comment le Conseil d'État a sauvé la majorité des enquêtes judiciaires

Conseil d'État, French Data Network et autres, 21 avril 2021, n° 3930922

La décision rendue le 21 avril 2021 par le Conseil d'État est certainement l'une des plus importantes de ces dernières années. Rendue en Assemblée du contentieux[1], elle vient clore (temporairement ?) un chapitre ouvert depuis 2014 s'agissant de la question ô combien sensible de l'équilibre entre protection de la vie privée et recherche et poursuite des auteurs d'infractions pénales.

Depuis 2014, la Cour de justice de l'Union européenne (CJUE) poursuit l'encadrement des dispositifs juridiques liés à la conservation et à l'accès, à des fins pénales, aux données de localisation et de trafic (données de connexion) des utilisateurs[2]. En effet, au travers de ses différents arrêts[3], la CJUE a posé plusieurs grands principes qui mettaient à mal le régime juridique français de

1. Formation de jugement la plus solennelle du Conseil d'État et réservée aux affaires les plus importantes.

2. AUDIBERT, Matthieu. La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ? cf. *supra* p. 46-64.

3. Arrêt du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., C-293/12 et C-594/12 ; arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15 ; arrêt du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a., C-511/18, C-512/18 et C-520/18 ; arrêt du 2 mars 2021, Prokuratuur, C-746/18.
numérique (LCEN).

conservation des données de connexion[4] au regard de la Charte des droits fondamentaux de l'UE. Le droit français prévoit ainsi un cadre juridique précis organisant la conservation généralisée et indifférenciée des données techniques de connexion et des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne[5]. Ces données sont conservées pendant une année[6].

Par ailleurs, il convient de souligner que l'arrêt Quadrature du Net rendu le 6 octobre 2020 par la CJUE faisait suite à plusieurs questions préjudicielles posées par le Conseil[7].

Que nous apporte cette décision ?

Particulièrement sensible à maintenir le régime juridique actuel, le Gouvernement demandait au Conseil d'État de déclencher un contrôle « *ultra vires* ». De quoi s'agit-il ?
Le Gouvernement invitait ainsi le Conseil à contrôler puis à constater que la CJUE avait dépassé les limites de ses compétences

---

4. LASSALLE, Maxime. Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE. *Recueil Dalloz*, 2021, p. 406.
5. AUDIBERT, Matthieu. La conservation des données, le droit français et la Cour de justice de l'Union européenne, quelles conséquences pour les enquêtes judiciaires ? [en ligne] *La veille juridique du Centre de recherche de l'École des officiers de la gendarmerie nationale*, novembre 2020, p. 15-29. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/veille-juridique/novembre-2020
6. Article L. 34-1 III du Code des postes et des communications électroniques. Article 6 II de la loi n° 2004-575 du 21 juin 2004, loi pour la confiance dans l'économie numérique (LCEN).
7. Conseil d'État, 26 juillet 2018, n° 394922, 397844 et 397851.

avec celles relevant des États membres au regard des traités. Ce faisant, le Conseil était invité à écarter la jurisprudence de la CJUE, ce qui aurait constitué un bouleversement majeur dans l'ordre juridique communautaire. Ce type de contrôle a déjà été mis en œuvre en Allemagne[8].

Toutefois, le Conseil a refusé le contrôle « *ultra vires* » demandé par le Gouvernement et a ainsi évité la guerre des juges[9]. Il s'est en revanche appuyé sur le droit constitutionnel français puis sur l'arrêt Quadrature du Net pour contourner certains principes dégagés par la CJUE dans ses différents arrêts, un bel exercice d'équilibrisme[10].

À cet effet, le Conseil introduit sa décision en affirmant avec solennité la primauté de la Constitution[11]. Elle est la norme suprême en droit national. Le Conseil en tire comme conséquence qu'il lui revient de vérifier que l'application du droit communautaire ne remet pas en cause des exigences constitutionnelles qui ne seraient pas garanties de façon équivalente par le droit de l'Union.

Il s'agit en réalité d'une forme de clause de sauvegarde fondée sur la primauté de la Constitution dans la hiérarchie des normes. Ainsi, quand il est reproché à un acte réglementaire de ne pas respecter le

---

8. JOOP, Olivier. Guerre des cours ou dialogue de sourds ? L'arrêt de la Cour constitutionnelle fédérale allemande relative au programme PSPP de la Banque centrale européenne, *RTD Eur.*, 2021, p. 110.

9. DE MONTECLER, Marie-Christine. Conservation des données : la guerre des juges n'aura pas lieu. *Dalloz Actualité*, avril 2021.

10. REES, Marc. Comment le Conseil d'État a sauvé la conservation des données de connexion [en ligne]. NextINpact, 22 avril 2021. Disponible sur : https://www.nextinpact.com/article/45613/comment-conseil-detat-a-sauve-conservation-donnees-connexion

11. Point 4.

droit de l'Union, alors le moyen soulevé en défense peut être écarté lorsque son acceptation aurait pour conséquence de bloquer une garantie constitutionnelle inexistante dans le droit communautaire[12]. Dans ce cas, le Conseil va alors contrôler la conformité du texte réglementaire non au droit communautaire, mais directement à la Constitution[13].

Dans son mémoire, le Gouvernement invoquait ainsi la sauvegarde des intérêts fondamentaux de la nation, la prévention des atteintes à l'ordre public, les atteintes à la sécurité des personnes et des biens, la lutte contre le terrorisme, ainsi que la recherche des auteurs d'infractions pénales[14]. Celles-ci « constituent des objectifs de valeur constitutionnelle, nécessaires à la sauvegarde de droits et de principes de même valeur, qui doivent être conciliés avec l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir et le respect de la vie privée[15] ».

Néanmoins, et c'est toute l'habilité remarquable de cette décision, le Conseil d'État ne met pas en œuvre cette clause de sauvegarde, certainement pour ne pas ouvrir un front avec la CJUE.

En effet, il va s'appuyer sur l'arrêt Quadrature du Net pour, *in fine*, préserver la conservation et l'utilisation des données de connexion dans le cadre de la majorité des enquêtes judiciaires.

Dans son arrêt Quadrature du Net[16], la CJUE énonce que la

12. Point 5.
13. Points 5 à 8.
14. Point 9.
15. *Ibidem*.

conservation généralisée et indifférenciée des données de connexion est permise au titre de la sécurité nationale.

Ainsi, le Conseil relève que « le droit de l'Union européenne permet d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et de localisation autres que les adresses IP aux seules fins de sauvegarde de la sécurité nationale lorsqu'un État est confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, sur injonction d'une autorité publique, soumise à un contrôle effectif d'une juridiction ou d'une autorité administrative indépendante, chargée notamment de vérifier la réalité de la menace, pour une période limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace [17]».

Ce faisant, le Conseil juge illégale l'obligation de conservation généralisée et indifférenciée des données de connexion (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins liés à la poursuite des infractions pénales. Il rappelle ainsi que le droit de l'Union s'oppose à ce que soit imposée aux opérateurs la conservation généralisée et indifférenciée des données de trafic et de localisation autres que les adresses IP, y compris aux fins de lutte contre la criminalité grave.

Néanmoins, il relève que cette conservation généralisée et indifférenciée aujourd'hui imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale,

---

16. Arrêt du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a., C-511/18, C-512/18 et C-520/18, points 134 à 139.
17. Point 31.

comme cela est requis par la CJUE[18]. Il relève notamment « que la France est confrontée à une menace pour sa sécurité nationale (…). Cette menace est non seulement prévisible mais aussi actuelle. Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Deux nouveaux attentats ont déjà été déjoués en 2021. Le plan Vigipirate a été mis en œuvre au niveau "Urgence attentat" entre le 29 octobre 2020 et le 4 mars 2021 puis au niveau "Sécurité renforcée - risque attentat" depuis le 5 mars 2021, attestant d'un niveau de menace terroriste durablement élevé sur le territoire[19]. »

Il impose à ce sujet au gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace[20].

Pour la poursuite des infractions pénales, le CE énonce que la solution suggérée par la CJUE dans son arrêt Quadrature du Net de « conservation ciblée[21] » en amont des données n'est ni matériellement possible, ni opérationnellement efficace[22]. En effet, il n'est pas possible de prédéterminer les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu où elle sera commise[23].

Pour contourner les infaisabilités opérationnelles des solutions proposées par la CJUE, le Conseil suggère de recourir à la méthode

20. Points 31 et 46.
21. Point 54.
22. Point 57.
23. Point 54.

de « conservation rapide » autorisée par le droit européen[24]. Celle-ci peut s'appuyer sur le stock de données conservées de façon généralisée et indifférenciée pour les besoins de la sécurité nationale et peut être utilisée pour la poursuite des infractions pénales[25]. Autrement dit, le critère lié à la sécurité nationale devient le support juridique autorisant l'accès en judiciaire à ces données, sous deux réserves.

Tout d'abord, cette conservation rapide et cet accès ne peuvent être autorisés que dans le cadre de la criminalité grave. Cela implique de prévoir un seuil de gravité en excluant *de facto* les contraventions et certains délits pour lesquels les enquêteurs ne pourront plus requérir les opérateurs, les crimes étant nécessairement graves. En outre, selon la jurisprudence de la CJUE, cet accès ne pourra être autorisé que par une autorité administrative indépendante ou un juge indépendant qui doit avoir la qualité d'un tiers par rapport aux enquêteurs[26]. Ce juge ne doit pas être impliqué dans la conduite des investigations et doit avoir une position de neutralité vis-à-vis des parties à la procédure pénale[27].

Le recours au critère lié à la sécurité nationale permet donc de sauvegarder l'accès aux données de connexion dans le cadre des enquêtes judiciaires. Pour autant, cette solution ne peut être que

---

24. Points 55 et 56. Cette méthode de « conservation rapide » est prévue par la Convention du Conseil de l'Europe sur la cybercriminalité dite Convention de Budapest du 23 novembre 2001 (articles 16 et 17) à laquelle la France est partie.

25. Point 57.

26. CJUE, 2 mars 2021, aff. C-746/18, Prokuratuur.

27. AUDIBERT, Matthieu. La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ? Cf. *supra*, p. 46-64.

temporaire. Le Conseil rappelle, en effet, que l'existence et la persistance de cette menace liée à la sécurité nationale doivent faire l'objet d'un examen périodique sous le contrôle du juge administratif[28]. Si cette menace liée à la sécurité nationale disparaît, la conservation des données à ce titre et l'accès pour les enquêtes judiciaires disparaîtront.
En réalité, cette solution permet certainement de conserver, en partie, le régime actuel, pour avancer sur le projet de règlement E-evidence[29].

À court terme, le Conseil d'État enjoint le Gouvernement à procéder à l'abrogation du dispositif réglementaire[30] de conservation des métadonnées dans un délai de six mois[31]. À moyen et long terme, des modifications substantielles de notre procédure pénale doivent également être envisagées.

Ces modifications concerneront vraisemblablement cinq articles du Code de procédure pénale.
S'agissant de l'accès aux métadonnées conservées au titre de la sécurité nationale, il faudra envisager de modifier les articles 60-1, 77-1-1 et 99-3 du Code de procédure.
Au titre du principe de proportionnalité[32], cette obligation de

---

28. Point 31.
29. CONSEIL EUROPÉEN, Un meilleur accès aux preuves électroniques pour lutte contre la criminalité [en ligne]. Dernière mise à jour le 20 octobre 2020. Disponible sur : https://www.consilium.europa.eu/fr/policies/e-evidence/
30. Article R. 10-13 du Code des postes et des communications électroniques. 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.
31. Point 46.

conservation n'est imposée aux opérateurs que « pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales susceptibles de présenter un degré de gravité suffisant pour justifier l'ingérence dans les droits protégés » par la Charte des droits fondamentaux de l'Union. Le Conseil d'État précise que « seules de telles infractions [peuvent] légalement justifier l'accès des services d'enquêtes aux données conservées par les opérateurs[33] ». Or, les articles précités prévoient actuellement la possibilité pour les services d'enquêtes d'accéder à ces données pour l'ensemble des contraventions, délits et crimes.

Cette possibilité est en contradiction avec la position du Conseil d'État qui subordonne l'accès aux « données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie[34]».

Enfin, il sera certainement nécessaire de modifier l'article 60-2 du Code de procédure pénale pour actualiser la méthode dite de « conservation rapide » des données, laquelle n'est actuellement prévue que pour « le contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs[35] ».

Après le Conseil d'État, la position de la Chambre criminelle de la Cour de cassation, qui va certainement être amenée à se prononcer sur ces questions, devra être examinée avec la plus grande attention.
En effet, au regard de l'arrêt de la CJUE Prokuratuur du 2 mars

32. Points 39 et 57.
33. *Ibid*.
34. Point 57.
35. Article 60-2 alinéa 2 du Code de procédure pénale.

2021, quelle est l'autorité qui doit préalablement autoriser cet accès ? Au regard de son positionnement, quelle place pour le procureur de la République ? Le juge d'instruction peut-il voir ses pouvoirs d'enquête menacés ? Enfin, les juges des libertés et de la détention doivent-ils être cette autorité ?

Lieutenant Océane GERRIET

Le bigdata au service de l'État : « qui est pris, qui croyait prendre » ou quand les fraudeurs vont devenir payeurs !

L'article 154 de la loi n° 2019-1479 de finances pour 2020 a prévu, pour une durée de 3 ans, l'expérimentation d'un traitement de données permettant de collecter et d'exploiter les « contenus librement accessibles sur les plateformes en ligne » au profit de l'administration fiscale et de l'administration des douanes et droits indirects. Le décret de mise en œuvre est paru, quant à lui, le 11 février 2021. Ce dispositif, déjà validé le 27 décembre 2019 par le Conseil constitutionnel, n'a pas fait l'objet de réserves majeures lors de la seconde délibération de la Commission nationale de l'informatique et des libertés (CNIL) rendue le 10 décembre 2020. Cependant, elle a fourni une analyse restrictive de la notion de « contenu librement accessible » qui restreint d'autant les possibilités de l'outil aux seuls contenus ne nécessitant pas de se connecter notamment via un compte sur la plateforme en amont.

Vous avez déclaré disposer de peu de ressources ? Ou encore, être domicilié en Franche-Comté ? Alors quid de vos selfies #Instagram sur les plages de Menton ou au volant de votre Audi TT flambant neuve ? L'administration fiscale a décidé de traquer les fraudeurs en les prenant à leur propre jeu en glanant des informations rendues librement accessibles par ces derniers sur Internet et plus précisément sur les « **plateformes en ligne** ». Par plateforme en ligne, Bercy entend viser celles mentionnées au 2° de l'article L. 111-7 du Code de la consommation, soit les plateformes de « mise en

relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service ». En somme : les réseaux sociaux, les sites de e-commerce, les sites de petites annonces et bien d'autres… Le fait d'exploiter Internet pour lutter contre les fraudes n'est pas nouveau mais c'est le moyen qui est novateur. Les nouvelles technologies offrent de nouvelles perspectives, tant pour les citoyens que pour les pouvoirs publics. Ainsi, afin d'« améliorer la détection de la fraude et le ciblage des contrôles », l'administration a voulu s'armer d'un outil lui permettant de faciliter le travail de ses agents pour ce type de recherche, voire de l'automatiser en s'appuyant sur une méthode redoutable : le **datamining**. Autrement nommé « l'exploration de données », il s'agit d'un processus automatique ou semi-automatique visant à analyser de grandes quantités de données et d'établir des corrélations à l'aide d'algorithmes, voire d'intelligence artificielle (comme c'est le cas de Bercy).

Le décret d'application est scindé en deux temps : d'une part, le traitement mis en œuvre dans le cadre de la phase d'apprentissage et de conception de l'outil puis, d'autre part, le traitement qui sera mis en œuvre pour la phase d'exploitation. Sur ce point, il est intéressant de souligner que la CNIL rappelle que le régime juridique applicable est distinct. En effet, la **phase d'apprentissage** a pour finalité de « développer un outil de collecte et d'analyse » et « d'identifier les indicateurs » permettant de caractériser des « manquements et infractions recherchées ». Cette phase ne cherche pas à rechercher, constater et poursuivre des manquements (= ce qui relèverait de la directive Police/Justice) mais bien à **développer un outil** qui permettra d'y répondre. Ainsi, et quand bien même il s'agit d'une phase de « développement », l'outil va

brasser des données personnelles et relève du Règlement général sur la protection des données (RGPD)[1]. Par contre, la **phase de mise en œuvre** qui consistera à utiliser cet outil pour **rechercher et constater des manquements et des infractions** relèvera de la directive Police/Justice qui prévoit des exigences encore plus élevées pour la sécurité du traitement.

Concernant la phase d'apprentissage, Bercy va collecter des données sur un échantillon précis, composé de certaines entreprises et personnes physiques préalablement identifiées. Ce travail sur échantillon va lui permettre de **créer les indicateurs qui seront utiles pendant la phase d'exploitation**. Premièrement, s'agissant des indicateurs, il rappelle qu'ils ne comportent aucune donnée personnelle puisqu'ils vont représenter des mots clés, expressions, etc. Deuxièmement, s'agissant des données collectées, Bercy précise que le traitement a vocation à recueillir « les données d'identification ». Cette mention est plutôt large mais à l'image de tout ce qui est susceptible d'être publié en ligne tels un écrit, une image, une photographie, un son ou une vidéo. En outre, et par essence, le décret prévoit qu'elles peuvent comporter des données sensibles comme, par exemple, des messages évoquant une situation médicale ou une opinion politique, voire encore des photos révélant une orientation sexuelle, etc. Sur ce point, il souligne les garanties mises en œuvre par l'administration vis-à-vis du traitement de ce type de données puisqu'elles ne sont pas conservées si elles ne sont pas strictement nécessaires.

1. Sur la question de la prise en compte de la problématique des données personnelles au stade du développement, voir le Guide RGPD pour les développeurs mis au point par la CNIL. Disponible sur : https://www.cnil.fr/fr/la-cnil-publie-un-guide-rgpd-pour-les-developpeurs

De manière générale, la CNIL conforte les durées de conservation fixées par Bercy. Pour la phase d'apprentissage, elle salue également le fait d'avoir réduit la taille de l'échantillon au strict nécessaire et d'avoir fixé une **durée de conservation très limitée** (5 jours pour les données sensibles, 30 jours pour les autres). Tandis que, pour la phase d'exploitation, qui n'est plus limitée à un échantillon de données, la durée de conservation est fixée par défaut à 30 jours mais comprend deux exceptions. D'une part, elle peut aller jusqu'à 1 an maximum si la donnée collectée permet de concourir à la constation des infractions et, d'autre part, peut perdurer au-delà de ce délai pour les besoins d'une procédure pénale ou douanière. La CNIL regrette néanmoins que Bercy n'aille pas jusqu'au bout de son raisonnement. En effet, le ministère précise que la phase de conception va lui permettre de déterminer des indicateurs mais aussi d'affiner les données qui lui sont nécessaires de collecter. Or, le décret prévoit d'ores et déjà les données collectées pour la phase d'exploitation du traitement et fige ainsi cette liste (de manière large) avant même le retour d'expérience que peut apporter la phase d'apprentissage. En réalité, rien n'empêchera Bercy de modifier son décret mais cela prendra du temps.

Ensuite, les **données collectées par l'outil développé par Bercy seront transmises aux services en charge de la lutte contre les fraudes**, aussi bien du côté de la Direction générale des finances publiques (DGFIP) que de la Direction générale des douanes et des droits indirects (DGDDI). D'une part, cela permet de conforter le fait que les données recueillies grâce à une intelligence artificielle ne donnent pas lieu à une décision automatisée mais bien à **une analyse par un humain**. L'outil ne révèle que des probabilités de fraude, à charge pour l'agent d'en vérifier la véracité. D'autre part, la

DGFIP et la DGDDI disposent chacune d'un traitement de données spécifiques pour la poursuite de leurs missions de lutte contre les fraudes, de sorte que cette transmission va donc générer une collecte de nouvelles données qui n'étaient pas initialement prévues par les décrets de mise en œuvre de ces traitements. Le ministère a donc également saisi la CNIL d'un projet de décret modificatif.

Enfin, l'intérêt principal d'un tel outil est de pouvoir collecter toutes les **données « librement accessibles » et manifestement rendues publiques sur les plateformes en ligne, mais faut-il encore s'entendre sur le champ d'une telle notion**. Pour Bercy, il s'agit d'une donnée publiée « sans paramètre de confidentialité spécifique ou avec un paramétrage de confidentialité public ». Néanmoins, la CNIL estime que cette notion est trop large et s'appuie sur la décision rendue par le Conseil constitutionnel en 2019.

Premièrement, ce dernier estime qu'est « librement accessible » un contenu qui ne nécessite pas la saisie d'un mot de passe ou une inscription à un site. Sur ce point, la CNIL a censuré Bercy en exigeant une modification du décret. En effet, elle rappelle qu'il n'est pas possible, via l'outil automatisé, de créer des comptes pour pouvoir accéder aux contenus. En outre, si la CNIL reconnaît que Bercy peut utiliser des API (*Application Programming Interface*) afin que lui soient mises à disposition des données de certaines plateformes ou des techniques d'extraction de données, ces deux techniques nécessitent la création de comptes (administrateur pour l'un, utilisateur pour l'autre). Ainsi, cela ne doit pas permettre pour autant la collecte de données qui n'auraient pas été accessibles sans la possession d'un compte sur la plateforme en question ou de la

saisie d'un mot de passe. Cette approche, particulièrement protectrice de la liberté des citoyens, limite néanmoins l'intérêt d'un tel outil visant à lutter plus efficacement contre les fraudes, puisqu'elle exclut *de facto* de nombreux contenus présents sur certaines plateformes, telles que Facebook, qui nécessitent *a minima* la création d'un compte. Deuxièmement, le Conseil constitutionnel a eu l'occasion de préciser ce qu'il fallait entendre par contenu « manifestement rendu public ». À la lumière de cette approche, la CNIL s'est interrogée sur les contenus concernant une personne donnée mais « rédigés par des tiers » ou encore des commentaires rédigés par la personne concernée sur une plateforme de e-commerce sur laquelle elle n'a aucune prise sur la confidentialité. Pour résumer, un contenu « **manifestement** » rendu public signifie qu'il faut une intention volontaire de la personne concernée à divulguer son contenu publiquement. La CNIL conclut donc à l'impossibilité de collecter les commentaires rédigés par les tiers et va plus loin en exigeant des garanties techniques permettant d'éviter cette collecte. Troisièmement et dernièrement, il est toujours intéressant de souligner qu'aucun système de reconnaissance faciale n'est prévu dans ce traitement.

Force est de constater que si la réglementation relative à la protection des données personnelles s'avère très protectrice (et c'est heureux, d'autant plus que l'Europe est pionnière en la matière), elle restreint d'autant les moyens d'action des autorités souhaitant avoir recours à des procédés automatisés ou à des technologies particulièrement innovantes comme l'IA. Mais face à l'ingéniosité des contrevenants comme des fraudeurs, face aux nouveaux vecteurs facilitant les actes délictuels, n'est-ce pas le rôle de l'État de développer des moyens adéquats pour y répondre ? Même s'il est difficile d'en connaître avec certitude le montant, on estime que le coût de la fraude fiscale oscille entre 20 et 100

milliards d'euros[2]. Or, l'impôt est une condition *sine qua non* du fonctionnement de l'État et, plus important encore, permet de préserver notre système social, particulièrement protecteur des individus. Ainsi, s'il est du pouvoir de tout État d'en assurer la levée, il est également de son devoir d'en garantir l'efficacité.

2. Combien la fraude fiscale coûte-t-elle à la France chaque année ? [en ligne*europe 1.fr*, 7 janvier 2019. Disponible sur : https://www.europe1.fr/economie/combien-la-fraude-fiscale-coute-t-elle-a-la-france-chaque-annee-3833942https://www.europe1.fr/economie/combien-la-fraude-fiscale-coute-t-elle-a-la-france-

Général d'armée (2S) Marc Watin-Augouard

ACTUALITÉ NUMÉRIQUE

L'agence du numérique de défense est créée

L'arrêté du 23 avril 2021 porte création de l'Agence du numérique de défense (AND).

Le 1er décembre 2020, la ministre des Armées Florence Parly a annoncé la création de l'AND en soulignant que « le numérique occupe une place croissante au cœur des capacités opérationnelles et fonctionnelles du ministère des Armées. Ce sont plusieurs milliers d'agents civils et militaires et près de 1 500 systèmes d'information et de communication qui concourent directement ou indirectement aux missions du ministère ». La ministre ajoute « qu'il est urgent de simplifier notre manière de faire pour une meilleure efficacité opérationnelle. Le ministère des Armées est pionnier en la matière et entend bien le rester. Plus que jamais, un numérique solide, fiable et efficace est un gage de résilience ».

Après une préfiguration de quatre mois, l'arrêté du 23 avril 2021 donne naissance à ce service à compétence nationale rattaché au délégué général pour l'armement. Elle est dirigée depuis le 5 mai 2021 par l'Ingénieur général de l'armement de 1re classe (IGA) Dominique Luzeaux, ancien directeur adjoint « Plans » de la Direction interarmées des réseaux d'infrastructure et des systèmes d'information de la Défense (DIRISI).

Cette agence doit contribuer aux enjeux de supériorité opérationnelle et de maîtrise de l'information au sein du ministère en révisant en profondeur l'organisation du numérique pour faire face aux défis croissants liés à la transformation du ministère. Elle doit, dans un cadre budgétaire contraint, permettre d'encore mieux

utiliser les différents budgets et effectifs du ministère pour répondre aux enjeux de transformation numérique.
Elle s'inscrit dans un écosystème numérique déjà riche, avec la Direction générale du Numérique (DGNUM), la DIRISI et le Commandement de la cyberdéfense (COMCYBER). Proximité par le milieu numérique qui les rapproche, mais différenciation par les missions exercées.
La DGNUM, rattachée directement à la ministre, a un rôle stratégique de pilotage et de coordination. La DIRISI, l'opérateur du ministère, intervient sur les réseaux, les applications et toutes les infrastructures du système d'information (SI). Elle administre et exploite, ce qui signifie qu'elle garantit le bon fonctionnement de l'IT (*information technology* ou technologie de l'information) au service des forces comme des services, et elle est également acheteur IT pour le ministère ainsi que pour certains contrats interministériels. Quant à COMCYBER, il est « l'ANSSI » du ministère et met en œuvre les actions opérationnelles conduites par les forces.
Selon l'article 2 de l'arrêté, l'agence a pour missions :

– de conduire, pour le compte des états-majors, directions et services, et tout au long de leur cycle de vie (conception, réalisation, déploiement et retrait), les projets numériques complexes ou à fort enjeu. La complexité s'analyse d'un point de vue technique, lorsqu'ils associent plusieurs porteurs qui peuvent avoir des attentes différentes, sont financés sur plusieurs lignes différentes ;
– de fédérer et mutualiser les capacités existantes en matière de conduite de projets numériques et de diffuser les meilleures pratiques ;
- d'assurer un rôle de conseil des armées, des directions et des services sur la définition de leurs besoins numériques et de veiller à

l'optimisation des ressources humaines et financières qu'ils leur consacrent ;
– de contribuer à la mise en œuvre de la politique industrielle du ministère des Armées dans le domaine des technologies numériques des systèmes d'information, en lien avec la DGNUM et la Direction générale de l'armement (DGA). L'agence va faciliter en priorité l'accès à la commande publique des TPE-PME, notamment par des groupements, pour favoriser l'innovation technologique ou la rupture dans les usages.

Un comité d'orientation et de pilotage de l'agence du numérique de défense, présidé par le délégué général pour l'armement et réunissant les représentants des états-majors, directions et services, oriente et évalue les activités de l'agence.
L'Agence a ses propres personnels, mais elle exerce une autorité fonctionnelle sur les chefs des projets dont la responsabilité lui est confiée, ainsi que sur le personnel qui leur est subordonné dans la conduite de ces projets (art. 3).

L'Europe renforce sa cybersécurité

L'année 2020 a été riche en termes d'annonces de l'Union européenne relatives à la transformation numérique. En février-mars 2020, au moment où la crise de la Covid-19 accapare les esprits, la Commission publie trois communications : *Façonner l'avenir numérique de l'Europe* (COM (2020) 0067), *Une stratégie européenne pour les données* (COM (2020) 0066), *Livre blanc sur l'intelligence artificielle - une approche européenne de l'excellence et de la confiance* (COM (2020) 0065). Quelques jours plus tard, le 10 mars, *Une nouvelle stratégie industrielle pour une Europe verte et numérique* (COM (2020) 102) fixe les grandes lignes d'une ambition

résumée par Thierry Breton : « Gérer les transitions verte et numérique et éviter les dépendances à l'égard de l'extérieur dans un nouveau contexte géopolitique exige un changement radical qui doit commencer dès à présent ». Depuis, trois rapports non contraignants du Parlement européen relatifs à l'intelligence artificielle (20 octobre 2020) et l'énoncé par ce dernier des lignes directrices pour l'utilisation militaire et non militaire de l'intelligence artificielle (IA), en particulier dans des domaines comme l'armée, la justice et la santé (20 janvier 2021), sont venus enrichir le corpus relatif à l'Europe du numérique. Malheureusement, la crise de la Covid-19 a modifié le centre de gravité des priorités. Depuis quelques jours, une certaine reprise est observée, avec la publication de plusieurs documents structurants qui ont une incidence directe sur la stratégie de cybersécurité.

La création du Centre de compétences en matière de cybersécurité

L'approbation du règlement relatif au Centre de compétences en matière de cybersécurité par le Conseil de l'Union européenne (UE), le 20 avril 2021, devrait être suivie par l'adoption définitive du texte par le Parlement européen.

Le Centre de compétences en matière de cybersécurité sera basé à Bucarest. Il réunira les principales parties prenantes européennes, notamment des entreprises, des organisations universitaires et de recherche et d'autres associations de la société civile concernées, afin de constituer une communauté de compétences en matière de cybersécurité destinée à renforcer et diffuser l'expertise dans ce domaine dans toute l'Union. Il a pour objectif de renforcer la sécurité de l'Internet ainsi que d'autres réseaux et systèmes

d'information critiques en mettant en commun les investissements dans la recherche, les technologies et le développement industriel en matière de cybersécurité.
Le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité travaillera en coopération avec un réseau de centres nationaux de coordination désignés par les États membres. Il affectera notamment les financements liés à la cybersécurité issus du programme Horizon Europe et du programme pour une Europe numérique (voir *infra*). Le centre sera établi pour la période allant de l'entrée en vigueur du règlement au 31 décembre 2029. Il sera ensuite liquidé, à moins que son mandat ne soit prolongé à la suite d'une évaluation et, éventuellement, d'une proposition législative de la Commission. Les activités du nouveau Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité compléteront les missions de l'ENISA (*The European union Agency for Cyberscurity*).

Le programme pour une Europe numérique

Le règlement (UE) 2021/694 du Parlement européen et du Conseil du 29 avril 2021 fixe l'enveloppe financière du programme pour une Europe numérique pour la période 2021-2027. Ce programme est structuré en cinq objectifs spécifiques qui correspondent à des domaines politiques clés :

– calcul à haute performance ;
– intelligence artificielle ;
– cybersécurité et confiance ;
– compétences numériques avancées ;
– déploiement et meilleure utilisation des capacités numériques –

Interopérabilité.

Les pôles européens d'innovation numérique doivent servir de points d'accès aux toutes dernières capacités numériques, parmi lesquelles le calcul à haute performance (CHP), l'IA, la cybersécurité, ainsi qu'à d'autres technologies innovantes existantes comme les technologies clés génériques, également disponibles dans les ateliers de fabrication collaboratifs ou les laboratoires numériques.
Selon le règlement, « la cybersécurité représente un défi pour l'Union dans son ensemble, que l'on ne peut pas relever dans le seul cadre d'initiatives nationales. La capacité de l'Europe en matière de cybersécurité devrait être renforcée de façon à la doter des moyens nécessaires pour protéger ses citoyens, ses administrations publiques et ses entreprises contre les cybermenaces. En outre, les consommateurs devraient être protégés lorsqu'ils utilisent des produits connectés qui peuvent être piratés et compromettre leur sécurité. Cette protection devrait être réalisée avec les États membres et le secteur privé, en développant des projets destinés à renforcer les capacités de l'Europe en matière de cybersécurité, en assurant la coordination entre ces programmes et en assurant un large déploiement dans tous les secteurs économiques des solutions de cybersécurité les plus récentes, y compris les projets, services, compétences et applications à double usage, ainsi qu'en agrégeant les compétences dans ce domaine pour atteindre une masse critique et un niveau d'excellence ».
Dans cet esprit, l'objectif spécifique « Cybersécurité et confiance » a pour ambition de :
– soutenir, avec les États membres, le développement et l'acquisition d'équipements, d'outils et d'infrastructures de données de cybersécurité avancés afin d'atteindre un niveau commun élevé de cybersécurité à l'échelon européen, dans le strict respect de la

législation en matière de protection des données et des droits fondamentaux, tout en garantissant l'autonomie stratégique de l'Union ;

– soutenir le développement et la meilleure utilisation possible des connaissances, capacités et compétences européennes en matière de cybersécurité, ainsi que le partage et l'intégration des meilleures pratiques ;

– assurer un large déploiement, dans l'ensemble de l'économie européenne, de solutions de cybersécurité de pointe efficaces, une attention particulière étant portée aux autorités publiques et aux PME ;

– renforcer les capacités au sein des États membres et du secteur privé pour les aider à se conformer à la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI ou NIS), y compris grâce à des mesures visant à favoriser l'adoption de bonnes pratiques en matière de cybersécurité ;

– améliorer la résilience face aux cyberattaques, contribuer à accroître la sensibilisation aux risques et la connaissance des processus de cybersécurité, aider les organismes publics et privés à atteindre les niveaux de base de la cybersécurité, par exemple en déployant le chiffrement de bout en bout des données et des mises à jour logicielles ;

– renforcer la coopération entre les sphères civile et militaire en ce qui concerne les projets, services, compétences et applications à double usage dans le domaine de la cybersécurité, conformément à un règlement établissant le Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité et le Réseau de centres nationaux de coordination (cf. *supra* règlement relatif au Centre de compétences en matière de

cybersécurité).

L'enveloppe financière pour l'exécution du programme pour la période du 1er janvier 2021 au 31 décembre 2027 est établie à 7 588 000 000 euros en prix courants (1 649 566 000 EUR) pour l'objectif spécifique « Cybersécurité et confiance ».

L'engagement de l'UE est essentiel mais ne saurait remplacer l'ardente obligation de chaque État membre à renforcer sa propre stratégie de cybersécurité. L'augmentation exponentielle des cyberattaques, observée depuis un an, conduit certains observateurs à « découvrir » ce que le FIC annonce depuis 2007 : « La cybercriminalité est la criminalité du XXIe siècle ». Pour lutter contre ce phénomène, l'idée de « bouclier » européen a été avancée. En vérité, il faut réaliser la « tortue romaine », chaque État devant avoir son propre bouclier, tandis que l'UE favorise l'uniformité et la cohérence de l'ensemble.

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS
DE LA GENDARMERIE NATIONALE

JUIN
2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Général d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE EUROPÉENNE

Cour de justice de l'Union européenne (Grande chambre) – Affaire C-645/19 du 15 juin 2021, Facebook Ireland Ltd, Facebook Inc., Facebook Belgium / Gegevensbeschermingsautoriteit (Autorité de protection de données)

Le Règlement général sur la protection des données (RGPD) autorise, sous certaines conditions, une autorité de contrôle d'un État membre à exercer son pouvoir de porter toute prétendue violation du RGPD devant une juridiction de cet État et d'ester en justice en ce qui concerne un traitement transfrontalier de données, alors qu'elle n'est pas « l'autorité chef de file » pour ce traitement.

Le 11 septembre 2015, le président de la Commission de la protection de la vie privée (CPVP devenue Autorité de protection des données – APD) intente une action en cessation à l'encontre de Facebook Ireland, de Facebook Inc. et de Facebook Belgium devant le tribunal de première instance néerlandophone de Bruxelles. Le motif de la saisine est une « violation grave et à grande échelle, par Facebook, de la législation en matière de protection de la vie privée ». Est reprochée au réseau social la collecte d'informations sur le comportement de navigation des détenteurs d'un compte Facebook ainsi que des non-utilisateurs des services Facebook au moyen de différentes technologies, telles que les cookies, les modules sociaux (par exemple, les boutons « J'aime » ou

« Partager ») ou encore les pixels. Ces éléments permettent au réseau social concerné d'obtenir certaines données d'un internaute consultant une page d'un site Internet les contenant, telles que l'adresse de cette page, l'adresse IP du visiteur de ladite page ainsi que la date et l'heure de la consultation concernée.
Par jugement du 16 février 2018, le tribunal de première instance néerlandophone de Bruxelles juge que le réseau social n'informe pas suffisamment les internautes belges de la collecte des informations concernées et de l'usage de ces informations. Le consentement donné par les internautes à la collecte et au traitement desdites informations est considéré comme non valable.
Le 2 mars 2018, Facebook Ireland, Facebook Inc. et Facebook Belgium font appel devant la Cour d'appel de Bruxelles en faisant valoir que seule l'autorité de protection de données irlandaise est habilitée à se prononcer sur son traitement des données.
La Cour d'appel sursoit à statuer et adresse à la Cour de justice de l'Union européenne (CJUE) une demande de décision préjudicielle sur la question de savoir si l'APD dispose de la qualité pour agir, au sens du RGPD, contre Facebook Belgium. La question posée se résume ainsi : l'autorité de contrôle d'un État membre peut-elle exercer son pouvoir de porter toute violation du RGPD devant la juridiction de cet État ou d'ester en justice en ce qui concerne ce traitement transfrontalier, alors qu'elle n'est pas « autorité chef de file » ?

Le RGPD (art. 56, paragraphe 1) institue, en effet, pour les traitements transfrontaliers, un mécanisme du « guichet unique » fondé sur une répartition des compétences entre une « autorité de contrôle chef de file » et les autres autorités nationales de contrôle concernées. L'article 56, paragraphe 2, et l'article 66 du RGPD consacrent les exceptions au principe de la compétence

décisionnelle de « l'autorité de contrôle chef de file ». Dans ces conditions, l'APD peut-elle agir contre Facebook Belgium, dès lors que c'est Facebook Ireland qui a été identifiée comme responsable du traitement des données concernées ? Selon Facebook, seul le Commissaire irlandais à la protection des données serait compétent pour intenter une action en cessation, sous le contrôle des juridictions irlandaises.

La compétence de l'autorité nationale n'est pas exclue par le mécanisme de « guichet unique »

Pour la CJUE, « le mécanisme de « guichet unique » ne saurait en aucun cas aboutir à ce qu'une autorité de contrôle nationale, en particulier « l'autorité de contrôle chef de file », n'assume pas la responsabilité qui lui incombe, en vertu du RGPD, de « contribuer à une protection efficace des personnes physiques contre des atteintes à leurs droits fondamentaux, sous peine d'encourager la pratique d'un forum shopping, notamment de la part des responsables de traitement, visant à contourner ces droits fondamentaux et l'application effective des dispositions de ce règlement les mettant en œuvre ». La compétence de « l'autorité de contrôle chef de file » pour adopter une décision constatant qu'un tel traitement méconnaît les règles relatives à la protection des droits des personnes physiques à l'égard du traitement de données à caractère personnel figurant dans le RGPD constitue la règle, tandis que la compétence des autres autorités de contrôle concernées pour adopter une telle décision, même à titre provisoire, constitue l'exception. Ainsi, une autorité de contrôle d'un État membre qui a le pouvoir de porter toute violation du RGPD à l'attention d'une juridiction de cet État membre et, le cas échéant, d'ester en justice, peut exercer ce pouvoir en ce qui concerne un

traitement de données transfrontalier, alors qu'elle n'est pas l'« autorité de contrôle chef de file », pour autant que ce soit dans l'une des situations où le règlement lui confère une compétence pour adopter une décision constatant que ledit traitement méconnaît les règles qu'il contient ainsi que dans le respect des procédures de coopération et de contrôle de la cohérence prévues par ce règlement. L'exception est prévue par le RGPD (art. 56, paragraphe 2) qui dispose qu'une autorité de contrôle qui n'est pas « l'autorité de contrôle chef de file » est compétente pour traiter une réclamation introduite auprès d'elle, relative à un traitement transfrontalier de données à caractère personnel ou une infraction éventuelle à ce règlement, si son objet concerne uniquement un établissement dans l'État membre dont elle relève ou affecte sensiblement des personnes concernées dans cet État membre uniquement. Ce pouvoir ne requiert pas que le responsable du traitement ou le sous-traitant pour le traitement transfrontalier de données à caractère personnel contre qui cette action est intentée dispose d'un établissement principal ou d'un autre établissement sur le territoire de cet État membre, pour autant que l'action en justice vise un traitement de données effectué dans le cadre des activités de cet établissement.

Facebook Belgium est indissociablement lié au traitement effectué par Facebook Ireland

Dans le cas d'espèce, le siège social du groupe Facebook est situé en Irlande. Facebook Ireland est le responsable exclusif de la collecte et du traitement des données à caractère personnel pour l'ensemble du territoire de l'Union. L'établissement situé en Belgique a été créé, à titre principal, pour permettre au groupe d'entretenir des relations avec les institutions de l'Union et, à titre accessoire, pour

promouvoir les activités publicitaires et de marketing du même groupe, destinées aux personnes résidant en Belgique. La CJUE relève que Facebook génère une partie substantielle de ses revenus grâce, notamment, à la publicité qui y est diffusée et que l'activité exercée par l'établissement situé en Belgique est destinée à assurer, dans cet État membre, même si ce n'est que de manière accessoire, la promotion et la vente d'espaces publicitaires qui servent à rentabiliser les services Facebook. Par ailleurs, l'activité exercée à titre principal par Facebook Belgium, consistant à entretenir des relations avec les institutions de l'Union et à constituer un point de contact avec ces dernières, vise notamment à établir la politique de traitement des données à caractère personnel par Facebook Ireland. Donc, les activités de l'établissement du groupe Facebook situé en Belgique doivent être considérées comme étant indissociablement liées au traitement des données à caractère personnel en cause au principal, dont Facebook Ireland est le responsable s'agissant du territoire de l'Union. Partant, un tel traitement doit être regardé comme étant effectué « dans le cadre des activités d'un établissement du responsable du traitement ». Ce traitement entre bien dans le champ d'action du RGPD. L'autorité de protection des données belge peut donc exercer son contrôle à l'égard de l'établissement responsable du traitement.

La nécessaire coopération de la part de « l'autorité chef de file »

La CJUE rappelle que le mécanisme de « l'autorité chef de file » exige une coopération étroite, loyale et efficace entre les autorités de protection de données concernées par un traitement transfrontalier, afin d'assurer une protection cohérente et homogène des règles relatives à la protection des données à

caractère personnel et ainsi préserver son effet utile. Cependant, dans l'exercice de ses compétences, « l'autorité de contrôle chef de file » ne saurait s'affranchir d'un dialogue indispensable ainsi que d'une coopération loyale et efficace avec les autres autorités de contrôle concernées. De ce fait, dans le cadre de cette coopération, « l'autorité de contrôle chef de file » ne peut ignorer les points de vue des autres autorités de contrôle concernées et toute objection pertinente et motivée formulée par l'une de ces dernières autorités a pour effet de bloquer, à tout le moins temporairement, l'adoption du projet de décision de « l'autorité de contrôle chef de file ». Est directement visée l'autorité irlandaise, souvent critiquée par ses pairs européens, dont la lenteur s'explique sans doute par la faiblesse de ses moyens rapportée au nombre d'entreprises ayant leur établissement stable dans cet État (dont Facebook, WhatsApp, Instagram, Apple, Google). L'autorité irlandaise serait donc le point de passage obligatoire pour contrôler les traitements transfrontaliers des 500 millions de consommateurs européens, comme le souligne Monique Goyens, la très redoutée directrice générale du Bureau européen des unions de consommateurs.

JURISPRUDENCE JUDICIAIRE

Cour de cassation – Chambre criminelle – (n° 20-85.853) – Arrêt n° 699 du 8 juin 2021

Est une atteinte à un système de traitement automatisé de données la suppression, en toute connaissance de cause, de la minute numérisée d'un jugement et des mentions informatiques relatives au dossier concerné, à l'insu d'un autre utilisateur dudit système.

Un greffier près le tribunal de commerce d'Agen a été dénoncé auprès du Parquet par un associé qui lui a reproché d'avoir fait disparaître un jugement dans l'historique informatique du greffe et dans le minutier. Il est cité devant le tribunal correctionnel du chef de suppression de données résultant d'un accès frauduleux à un Système de traitement automatisé de données (STAD). Il est déclaré coupable par cette juridiction qui n'a pas retenu l'accès frauduleux mais la suppression frauduleuse de données. Après appel, la procédure vient devant la Cour de cassation.

Dans ses moyens, la personne condamnée conteste l'existence d'une atteinte à un STAD en rappelant l'arrêt du 7 janvier 2020[1]. À cette occasion, la Cour avait considéré que les atteintes aux systèmes de traitement automatisé de données, prévues aux articles 323-1 à 323-3 du Code pénal, ne sauraient être reprochées à la personne qui, bénéficiant des droits d'accès et de modification des données, procède à des suppressions de données, sans les dissimuler à d'éventuels autres utilisateurs du système. Or, l'auteur du pourvoi fait valoir qu'il bénéficiait des droits d'accès et de modification des données et que « la condition supplémentaire posée par l'arrêt du 7 janvier 2020 et tenant à une absence de dissimulation à d'éventuels autres utilisateurs du système ne pose pas de difficulté, les faits ayant été commis au vu et au su de Mme [Z], commis-greffière assermentée ».

La Chambre criminelle a déjà jugé, à propos d'une affaire concernant la Chambre de commerce et d'industrie (CCI) du Puy-en-Velay Yssingeaux[2], que le seul fait de modifier ou de supprimer, en violation de la réglementation en vigueur, de telles données, caractérise le délit, sans qu'il soit nécessaire que ces modifications

1. Crim. 7 janvier 2020, pourvoi n° 18-84.755.
2. Crim., 8 décembre 1999, pourvoi n° 98-84.752.

ou suppressions émanent d'une personne n'ayant pas un droit d'accès au système, ni que leur auteur soit animé de la volonté de nuire. Mais si l'arrêt du 7 janvier 2020 précité écarte toute incrimination, dès lors que les opérations de suppression sont effectuées par le seul titulaire des droits d'accès et de modification des données, sans dissimulation à d'éventuels autres utilisateurs du système, la Cour, dans son arrêt du 8 juin 2021, considère que les modifications ou suppressions de données sont nécessairement frauduleuses dès lors qu'elles ont été sciemment dissimulées à au moins un autre utilisateur d'un tel système, même s'il n'est pas titulaire de droits de modification.

Cour de cassation – Chambre criminelle (20-86.343) – Arrêt n° 779 du 22 juin 2021

Encourent la cassation la saisie et l'exploitation de terminaux informatiques, lors d'une visite domiciliaire, alors qu'il n'a pas été découvert de documents ou de données sur place, et que la seule présence de terminaux informatiques ne peut être regardée comme révélant par elle-même l'existence de données relatives à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne.

L'état du droit

La loi du 30 octobre 2017[3] renforçant la sécurité intérieure et la lutte contre le terroriste (loi SILT) a introduit, dans le Code de la sécurité intérieure (art. L. 229-1 à L. 229-6) – CSI –, des mesures

3. Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

inspirées de celles de la loi du 3 avril 1955 relative à l'état d'urgence. Sur demande du préfet et après autorisation par le juge des libertés et de la détention du tribunal judiciaire de Paris[4], des visites domiciliaires et des saisies peuvent être réalisées (art. L. 229-1) « aux seules fins de prévenir la commission d'actes de terrorisme et lorsqu'il existe des raisons sérieuses de penser qu'un lieu est fréquenté par une personne dont le comportement constitue une menace d'une particulière gravité pour la sécurité et l'ordre publics et qui soit entre en relation de manière habituelle avec des personnes ou des organisations incitant, facilitant ou participant à des actes de terrorisme, soit soutient, diffuse, lorsque cette diffusion s'accompagne d'une manifestation d'adhésion à l'idéologie exprimée, ou adhère à des thèses incitant à la commission d'actes de terrorisme ou faisant l'apologie de tels actes ».

L'article L. 229-5 dispose « qu'aux seules fins de prévenir la commission d'actes de terrorisme, si la visite révèle l'existence de documents, objets ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée, il peut être procédé à leur saisie ainsi qu'à celle des données contenues dans tout système informatique ou équipement terminal présent sur les lieux de la visite soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la visite ».

4. Cette centralisation s'explique par la compétence nationale de ce tribunal en matière de terrorisme.

L'arrêt contesté

Dans le cas d'espèce, sur la demande d'un préfet, le juge des libertés et de la détention du tribunal judiciaire de Paris a, par ordonnance du 20 octobre 2020, autorisé des opérations de visite et saisie au domicile de l'auteure du pourvoi. À cette occasion, les gendarmes ont notamment saisi un téléphone et un ordinateur portables. Sur requête du préfet du 23 octobre 2020, le juge des libertés et de la détention, par ordonnance du 24 octobre 2020, a autorisé l'exploitation des données contenues dans les terminaux informatiques saisis. Tel est l'acte de procédure qui est porté devant la Cour de cassation, après un appel sans succès devant le Premier président de la Cour d'appel de Paris.

Sur la forme, l'auteure du pourvoi soutient que les opérations de visite et saisie ont été menées par une unité de gendarmerie territorialement incompétente. La Cour de cassation juge ce moyen irrecevable au motif que le recours formé sur le fondement de l'article L. 229-5 du CSI, qui ne porte que sur la régularité de la saisie, ne saurait avoir pour effet de permettre la discussion du déroulement des opérations de visite et de saisie lorsque le recours, sur le fondement des dispositions de l'article L. 229-3, II, du même Code n'a pas été exercé. L'incompétence territoriale ne pouvait être valablement soulevée qu'à l'occasion d'un recours contre le déroulement des opérations de visite et saisie, permis par l'article L. 229-3, II, du CSI, qui n'a pas été exercé.
Sur le fond, la Cour de cassation rappelle que la saisie ou la copie de documents et données informatiques contenus dans les terminaux informatiques, ordinateurs ou téléphones découverts sur les lieux, lors d'opérations de visite autorisées, en application de l'article L. 229-1 du CSI, n'est possible que lorsque ladite visite révèle

l'existence d'éléments relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne.

Pour justifier sa décision, la Cour d'appel a relevé que « le juge retient un ancrage ancien et solide de Mme X dans la mouvance islamiste, son adhésion sans faille à cette idéologie, son utilisation des réseaux sociaux pour approuver les attentats de janvier 2015, son utilisation à cette période d'un profil Facebook très évocateur, largement utilisé pour faire figurer des photos d'elle revêtue du niqab dissimulant le visage, son utilisation de ce moyen de communication pour diffuser des vidéos de propagande de Daech, son lien avec des individus acquis à la cause pro-jihadiste, son projet de partir en Syrie, son utilisation du réseau Périscope, en janvier 2018, pour diffuser une vidéo dans laquelle elle prônait des actes de violences contre la France, les contacts qu'elle a établis au cours de l'été 2018 avec un terroriste algérien assigné à résidence, le fait qu'elle ait fait l'objet d'un arrêté portant mesure individuelle de contrôle administratif et de surveillance jusqu'en mai 2020, son rejet des lois et valeurs républicaines ainsi que sa haine des institutions, encore démontrés par son comportement récent ». Le Premier président de la Cour d'appel a ajouté que les moyens de communication par le réseau d'Internet semblent être largement utilisés par la requérante pour véhiculer son idéologie islamiste et pour être en lien avec des individus engagés dans cette mouvance terroriste. Pour ce magistrat, la découverte à un domicile des éléments tels qu'un téléphone et un ordinateur portables dans ce contexte est suffisante et permet de révéler l'existence de documents ou données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics.

La Cour de cassation revient à une lecture littérale de l'article L. 229–5 du CSI : « Alors qu'il n'a pas été découvert de documents ou de

données sur place, et que la seule présence de terminaux informatiques ne peut être regardée comme révélant par elle-même l'existence de données relatives à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne, le premier président de la cour d'appel a méconnu le texte susvisé et les principes ci-dessus énoncés ».

CYBERSÉCURITÉ : ACTUALITÉ EUROPÉENNE

En décembre 2020, la Commission et le Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité ont présenté la stratégie de cybersécurité de l'Union européenne (UE).
Le 23 juin, la Commission a proposé la création d'une unité conjointe de cybersécurité afin d'intensifier la réaction aux incidents majeurs de sécurité qui ont des répercussions sur les services publics ainsi que sur la vie des entreprises et des citoyens dans l'ensemble de l'UE. Cette proposition est une concrétisation de la stratégie de cybersécurité de l'UE qui contribue à une économie et à une société numériques sûres.

L'unité conjointe de cybersécurité constitue une avancée importante vers l'achèvement du cadre européen de gestion des crises en matière de cybersécurité. Elle répond à un « besoin de partager » plus engageant que le seul « besoin d'en connaître ». Elle doit réunir les ressources et l'expertise dont disposent l'UE et ses États membres afin de prévenir et de dissuader les incidents et crises de cybersécurité massifs et d'y réagir.
Il s'agir de fédérer au sein d'une plateforme virtuelle et physique de solidarité et d'assistance les communautés de cybersécurité (civile,

répressive, diplomatique et militaire) du domaine de la cybersécurité, ainsi que les partenaires du secteur privé. Les participants fourniront des ressources opérationnelles pour l'assistance mutuelle au sein de l'unité conjointe de cybersécurité qui permettra de partager les meilleures pratiques, ainsi que des informations en temps réel sur les menaces qui pourraient apparaître dans leurs domaines respectifs. La Commission apportera les investissements nécessaires à la création de l'unité conjointe de cybersécurité, essentiellement à travers le programme pour une Europe numérique.

L'unité conjointe de cybersécurité sera créée selon un processus progressif et transparent en quatre étapes, avec l'adhésion pleine et entière des États membres et des différentes entités actives dans ce domaine. Il s'agit de faire en sorte que l'unité conjointe de cybersécurité entre dans sa phase opérationnelle d'ici au 30 juin 2022 et qu'elle soit entièrement mise en place un an plus tard, d'ici au 30 juin 2023. Elle sera localisée à proximité du bureau de l'Agence de l'Union européenne pour la cybersécurité (ENISA) et du bureau de la CERT-EU, à Bruxelles.

Pour Thierry Breton, commissaire au marché intérieur, « l'unité conjointe de cybersécurité est un élément essentiel de notre protection contre la complexité et le nombre croissants des cybermenaces. Nous avons défini des étapes et un calendrier précis qui nous permettront, de concert avec les États membres, d'améliorer concrètement la coopération, dans l'UE, en matière de gestion des crises, de détecter les menaces et d'y réagir plus rapidement. L'unité conjointe de cybersécurité est le bras opérationnel du cyberbouclier européen ».

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS
DE LA GENDARMERIE NATIONALE

SEPTEMBRE 2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Général d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE CONSTITUTIONNELLE

Conseil Constitutionnel – Décision n° 2021-924 QPC du 9 juillet 2021, la Quadrature du Net

La transmission d'informations aux services de renseignement par les autorités administratives n'est pas conforme à la Constitution, car le législateur n'a pas prévu les garanties suffisantes pour encadrer une action qui concerne le plus souvent des données à caractère personnel. L'échange d'informations entre services de renseignement est, en revanche, conforme à la Constitution.

Le 19 mai 2021, le Conseil d'État saisit le Conseil constitutionnel d'une question prioritaire de constitutionnalité posée par la Quadrature du Net. Celle-ci conteste la conformité à la Constitution de l'article L. 863-2 du Code de la sécurité intérieure (CSI), dans sa rédaction résultant de la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.

Le droit en cause

L'article L. 863-2 du CSI comprend trois alinéas.
Le premier dispose que les services spécialisés de renseignement du « premier cercle » (art. 811-2 du CSI[1]) et les services du deuxième

1. Direction générale de la sécurité extérieure (DGSE), Direction générale de la sécurité intérieure (DGSI), Direction nationale du renseignement et des enquêtes

cercle (art. 811-4 du CSI[2]) peuvent partager toutes les informations utiles à l'accomplissement de leurs missions définies par le CSI.
Le second alinéa concerne les autorités administratives[3] mentionnées à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Il permet à ces dernières de transmettre aux services mentionnés au premier alinéa, de leur propre initiative ou sur requête de ces derniers, des informations utiles à l'accomplissement des missions de ces derniers.
Le troisième alinéa renvoie à un décret en Conseil d'État le soin de fixer les modalités et les conditions d'application.

L'association requérante reproche au législateur d'avoir méconnu l'étendue de sa compétence et ainsi affecté le droit au respect de la vie privée, la protection des données personnelles, le secret des correspondances ainsi que la liberté d'expression. Elle reproche notamment aux dispositions de l'article incriminé de ne pas définir les informations pouvant être partagées, les catégories de personnes pouvant accéder à ces dernières, les finalités de ce

douanières (DNRED), Direction du renseignement militaire (DRM), Direction du renseignement et de la sécurité de la Défense (DRSD), TRACFIN.

2. Certains services de la police, de la gendarmerie, de l'administration pénitentiaire.

3. Les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du Code de la sécurité sociale et du Code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du Code du travail et les autres organismes chargés de la gestion d'un service public administratif ainsi que les commissions de coordination des actions de prévention des expulsions locatives prévues à l'article 7-2 de la loi n° 90-449 du 31 mai 1990 visant à la mise en œuvre du droit au logement.

partage ainsi que son régime juridique.

La décision des Sages

Les services de renseignement concourent à la défense des intérêts fondamentaux de la Nation

Le Conseil constitutionnel déclare conforme à la Constitution l'alinéa 1er qui prévoit l'échange entre services de renseignement mais censure l'alinéa 2 qui autorise l'échange vers les services de renseignement.
Les services spécialisés de renseignement du « premier cercle » ont pour missions la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils mettent en œuvre des techniques pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation. Les services du « second cercle » peuvent aussi recourir à certaines de ces techniques selon des finalités propres à chacun. Qu'ils appartiennent à l'une ou à l'autre catégorie, les services appelés à partager entre eux les informations sont tous des services concourant à la défense des intérêts fondamentaux de la Nation.

Le partage d'informations entre services est conforme aux exigences constitutionnelles

Le législateur a organisé et sécurisé le partage d'informations entre les services de renseignement afin d'accroître leur capacité opérationnelle. Les dispositions en cause mettent en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts

fondamentaux de la Nation.
S'agissant de l'information, un service de renseignement détenteur ne peut partager que si celle-ci est nécessaire à l'accomplissement des missions du service destinataire. Les informations ainsi partagées sont soumises au respect des règles encadrant les traitements de données à caractère personnel par les services de renseignement et, s'agissant des données recueillies au moyen de techniques de renseignement, des règles mentionnées au livre VIII du CSI. D'autre part, les dispositions contestées ne font pas obstacle au contrôle susceptible d'être exercé, par les autorités compétentes, sur les informations partagées.
En adoptant les dispositions contestées, le législateur a entendu améliorer l'information des services de renseignement. Ce faisant, ces dispositions mettent en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation.

La communication d'informations aux services de renseignement n'est pas encadrée par le législateur

La transmission d'informations peut avoir lieu à la seule initiative d'autorités administratives, dont les missions peuvent être sans lien avec celles des services de renseignement. Les informations communiquées aux services de renseignement sont toutes les « informations utiles » à l'accomplissement des missions de ces derniers sans que le législateur n'ait précisé la nature des informations concernées. La communication d'informations ainsi autorisée peut porter sur toute catégorie de données à caractère personnel, dont notamment des informations « sensibles » relatives à la santé, aux opinions politiques et aux convictions religieuses ou philosophiques des personnes. Le législateur n'a prévu aucune garantie encadrant ces transmissions d'informations. Le deuxième

alinéa de l'article L. 863-2 méconnaît donc le droit au respect de la vie privée.
L'abrogation de ces dispositions est reportée au 31 décembre 2021. Les mesures prises avant la publication de la présente décision ne peuvent être contestées sur le fondement de cette inconstitutionnalité.

JURISPRUDENCE JUDICIAIRE

Tribunal judiciaire de Paris, 17ème Chambre, jugement du 30 juin 2021, M.X./ 20 Minutes France

Le « droit à l'oubli » n'est pas un droit absolu. Il doit être mis en balance avec la liberté d'information et d'expression, particulièrement protégée s'agissant d'un organe de presse.

Les faits et la procédure

M.X., ancien Président, de décembre 2002 à août 2004, du « Racing Club de Paris », section football du Racing Club de France, a fait l'objet d'une condamnation pénale pour sa gestion du club. Déclaré coupable de complicité d'abus de confiance, de recel de bien obtenu à l'aide d'un abus de confiance, d'abus de biens sociaux, il a été condamné, le 12 juin 2009, par le tribunal correctionnel de Nanterre à deux ans d'emprisonnement avec sursis et à une amende de 20 000 euros. Par un arrêt rendu le 16 février 2011, la Cour d'appel de Versailles a infirmé partiellement le jugement en première instance[4]. Le 15 juin 2009, un article a été publié sur le site Internet

4. La Cour d'appel a reconnu M. X. coupable de délits d'abus de confiance et de recel et ordonné l'exclusion de sa condamnation du bulletin n° 2 de son casier judiciaire, sa peine d'emprisonnement avec sursis étant ramenée à un an et l'amende portée à 30 000 euros.

du journal *20 Minutes*, intitulé *Il détournait de l'argent pour un club*. M. X. constate que l'article est toujours présent dans la rubrique des actualités locales de la vie parisienne et n'est pas répertorié ni identifié en archives du journal en ligne, qu'il véhicule une information périmée du fait de l'arrêt de la Cour d'appel de Versailles ayant partiellement infirmé le jugement dont il est fait état. M. X. met alors en demeure la société 20 Minutes de supprimer l'article poursuivi ou, à tout le moins, de l'anonymiser ainsi que de faire le nécessaire dans les 72 heures pour qu'il ne soit plus indexé par les moteurs de recherche en application des articles 17 et 21 du Règlement général sur la protection des données (RGPD). Il appuie sa démarche sur le fait que les données personnelles traitées sont obsolètes, périmées et dénuées de pertinence pour les lecteurs, compte tenu de l'ancienneté des faits (plus de 15 ans). Il reproche aussi au journal de ne pas faire mention de la relaxe partielle et de la réduction de la peine d'emprisonnement dont il a bénéficié. Une mise à jour de l'article, le 15 novembre 2019, est la seule réponse du média. Le plaignant assigne la société 20 Minutes devant le tribunal judiciaire de Paris.

Les arguments des parties

M. X. s'appuie sur les articles 17 et 21 du RGPD[5], sur les articles 51 et 56 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, éclairés par la jurisprudence de la Cour de justice du l'Union européenne (CJUE). Il considère que la mention de sa condamnation relève des données sensibles de la personne et qu'au regard de la particulière gravité de l'ingérence dans ses droits au

5. Règlement Européen sur la Protection des Données personnelles (UE) n° 2016/679 du 27 avril 2016.

respect de sa vie privée et à la protection de ses données à caractère personnel, les responsables de traitement devraient justifier en quoi le maintien en ligne de l'article est strictement nécessaire pour protéger la liberté d'information des internautes.
Sur la base de l'article 17 du RGPD (art. 51 de la loi du 6 janvier 1978) qui instaure un « droit à l'oubli », il demande l'effacement de ses données à caractère personnel, considérant qu'elles ne sont pas nécessaires à l'exercice du droit à l'information et à la liberté d'expression. En se référant à l'article 21 (art. 56 de la loi du 6 janvier 1978), il s'oppose au traitement de ses données à caractère personnel sans que soient produits des motifs légitimes et impérieux qui permettraient de passer outre.
Enfin, il réitère sa demande de déréférencement sur l'ensemble des moteurs de recherche et entend se prévaloir subsidiairement de ce que l'exploitant d'un moteur de recherche doit, par principe et conformément à la jurisprudence de la CJUE et de la Cour de cassation, déréférencer les liens traitant des données sensibles d'une personne, telles que ses condamnations pénales, sauf à ce que l'inclusion des liens litigieux dans la liste des résultats s'avère strictement nécessaire à la liberté d'information et d'expression.

La société 20 Minutes France met en avant la liberté d'expression affirmée par l'article 10 de la Convention européenne des droits de l'Homme (CEDH), liberté qui ne peut être restreinte que lorsqu'existe un besoin social impérieux. Elle ajoute que le droit à l'effacement et le droit d'opposition ne s'appliquent pas lorsque le traitement en cause de données est nécessaire à l'exercice de la liberté d'expression, comme il résulte des dispositions du considérant 65 et de l'article 17-3 du RGPD ainsi que des dérogations prévues à l'article 80 de la loi Informatique et Libertés[6].

6. Traitement de données à caractère personnel aux fins de journalisme et

La position du tribunal

Le tribunal judiciaire de Paris arbitre en faveur de la liberté de l'information. Le RGPD (considérants 4 et 65) « vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques » ; « le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité ». Le RGPD concilie le « droit à l'oubli » (art. 17) avec le droit au respect de la vie privée, le droit à la liberté d'expression et d'information garanti par l'article 10 de la Convention de sauvegarde des libertés fondamentales et des droits de l'Homme (CEDH)[7].

L'article 21 du RGPD prévoit aussi une conciliation avec le droit à la liberté d'expression et d'information. Si le responsable du traitement est un organe de presse, le fait de lui imposer, en application de ce texte, de retirer d'un article les données personnelles, privant ainsi l'article de tout intérêt, serait susceptible d'excéder les restrictions pouvant être apportées à la liberté de la presse.

d'expression littéraire et artistique.

7. Article 11 de la Charte des droits fondamentaux de l'Union européenne.

Une société éditrice de presse n'est pas un moteur de recherche

La SAS 20 Minutes est éditrice de presse et exerce une activité de journalisme consistant à mettre en œuvre la liberté d'expression dans le cadre, notamment, d'articles susceptibles d'être mis en ligne sur son site Internet. Les dispositions relatives au « droit à l'oubli » ne s'appliquent pas, dès lors que le traitement des données personnelles « est nécessaire à l'exercice du droit à la liberté d'expression ». L'activité d'une société éditrice de presse n'est pas assimilable à celle du moteur de recherche dont l'intérêt principal n'est pas de publier l'information initiale sur la personne concernée. Le rôle de ce dernier est de permettre, d'une part, de repérer toute information disponible sur cette personne et, d'autre part, d'établir un profil de celle-ci. La jurisprudence de la CJUE s'applique aux moteurs de recherche et est donc inopérante dans le cas d'espèce[8].

8. Le droit au déréférencement – ou « droit à l'oubli » – est une des conséquences de l'arrêt CJUE du 13 mai 2014, Google Spain et Google (C-131/12). S'il ne fait pas disparaître le document que le plaignant estime contraire à sa vie privée, il supprime les liens vers les pages web qu'offre le moteur de recherche. L'arrêt CJUE (Grande chambre) du 24 septembre 2019 (C-136/17, GC, AF, BH, ED/ Commission nationale de l'informatique et des libertés – CNIL) a considéré que les informations relatives à une procédure judiciaire doivent être déréférencées si elles ne correspondent plus à la situation actuelle, dès lors qu'il est constaté que les droits de la personne prévalent sur ceux de l'internaute. Toutefois, en cas de maintien justifié par la liberté d'information des internautes, le moteur de recherche doit aménager la liste des résultats « de telle sorte que l'image globale qui en résulte pour l'internaute reflète la situation judiciaire actuelle ».

Le RGPD ne peut être invoqué pour bloquer des articles de presse

Comme le souligne le tribunal, le droit à la protection des données personnelles ne peut faire disparaître à la première demande des contenus de presse publiés sur Internet. La mention des éléments d'identification et l'évocation de condamnations pénales relèvent du droit à l'information du citoyen. La condamnation pénale d'une personnalité officielle ayant présidé un club sportif notoire s'inscrit dans le sujet récurrent des relations entre le sport et l'argent. Sa mention contribue donc à l'information du public. L'ancienneté de l'article contribue à la formation de l'opinion démocratique et permet l'information du lecteur, non seulement à partir de l'actualité, mais aussi sur la base d'informations plus anciennes qui conservent une pertinence au regard du sujet d'intérêt général. La non-inscription de la condamnation pénale sur le B.2 n'a pas pour effet de faire disparaître l'intérêt informatif de l'article de presse. Cet intérêt pour le public serait également compromis par une anonymisation sollicitée par le demandeur, laquelle excéderait les restrictions pouvant être apportées à la liberté de la presse. Pour le tribunal, le maintien en ligne de l'article ne constitue pas une atteinte disproportionnée au droit au respect de sa vie privée. La condamnation pénale évoquée dans l'article a déjà été prononcée en audience publique et a fait l'objet de divers articles de presse. Il n'a pas eu une diffusion importante, puisqu'il apparaît en 4e position d'une recherche Google avec la mention qu'il n'a été ni commenté, ni partagé. Mais avec son recours devant le tribunal, le demandeur va sans doute connaître « l'effet Streisand » dont ce commentaire n'est qu'une des manifestations…

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS
DE LA GENDARMERIE NATIONALE

OCTOBRE 2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Général d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE CONSTITUTIONNELLE

Décision n° 2021-933 QPC du 30 septembre 2021

Sont conformes à la Constitution les dispositions du Code pénal qui répriment le fait, au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui en diffusant, en l'absence d'accord de la personne, tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenus, avec le consentement exprès ou présumé de la personne ou par elle-même.

I. La saisine du Conseil constitutionnel

Le Conseil constitutionnel a été saisi le 30 juin 2021 par la Cour de cassation (Chambre criminelle, arrêt n° 892 du 23 juin 2021) d'une question prioritaire de constitutionnalité. Dans le dossier au fond, une justiciable conteste l'arrêt de la Cour d'appel de Montpellier, chambre correctionnelle, qui l'a condamnée à six mois d'emprisonnement avec sursis, 800 euros d'amende et trois ans d'interdiction des droits civiques, civils et de famille, pour diffusion publique, sans le consentement de la personne, d'enregistrements ou documents à caractère sexuel. Saisie d'un recours contre cette condamnation, la Cour de cassation saisit le Conseil constitutionnel d'une question prioritaire ainsi rédigée : « L'article 226-2-1, alinéa 2, du code pénal méconnaît-il le principe de légalité des délits et des peines et le principe de nécessité des délits, qui en est le corollaire, tels que garantis par les articles 8 de la Déclaration des droits de

l'homme et du citoyen de 1789 et l'article 34 de la Constitution de 1958, faute pour le législateur d'avoir défini ce qu'il entend par paroles ou images à caractère sexuel, faute d'avoir clairement précisé quels faits matériels sont constitutifs de l'infraction, faute d'avoir précisé si les propos et images doivent se rapporter à la vie intime de la personne et dans quelles conditions la personne qui a donné son consentement à leur communication ou les a elle-même communiqués, doit être considérée comme n'ayant pas donné son consentement à leur diffusion, faute enfin d'avoir précisé les éventuelles exceptions à l'application de l'incrimination, lorsque la personne a adressé des paroles et images à caractère sexuel qui n'étaient pas sollicitées ? »

Article 226-2-1

« Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende.

Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1. »

Nota :

L'article 226-1 réprime le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de

celle-ci, l'image d'une personne se trouvant dans un lieu privé.
3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci.
L'article 226-2 punit des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.

Pour soutenir la saisine, la Cour de cassation considère :
– que le texte ne précise pas ce qu'il convient d'entendre par paroles ou images à caractère sexuel, dans quelles conditions un accord à la fixation, à la captation, à l'enregistrement ou à la transmission d'images ou de propos à caractère sexuel exclut un accord à leur diffusion, si l'infraction résulte d'un mode particulier de diffusion ou simplement de la communication à un tiers, comment l'infraction s'articule avec l'article 226-2-1, alinéa 1, du Code pénal qui ne distingue pas selon que les images ou propos à caractère sexuel ont été obtenus dans un cadre public ou privé ;
– que le texte, qui exige le consentement exprès ou présumé de la personne à la réalisation de l'image ou à l'enregistrement de propos à caractère sexuel, apparaît en contradiction avec l'article 226-1 du Code pénal, auquel il se réfère expressément, et qui ne sanctionne, pour sa part, que la fixation, la captation, l'enregistrement et la transmission d'images ou de propos obtenus sans le consentement de la personne.

Ainsi, la Cour s'interroge sur la constitutionnalité de l'article 226-2-1, alinéa 2, du Code pénal, qui ne définit pas de manière claire et précise les éléments constitutifs de l'infraction, au regard

notamment des textes auxquels il fait expressément référence, et est susceptible de méconnaître le principe de légalité des délits et des peines.

II. La décision des Sages

Pour le Conseil constitutionnel, les termes « un caractère sexuel » et « absence d'accord de la personne pour la diffusion » sont suffisamment clairs et précis pour garantir contre le risque d'arbitraire. Il appartient aux juridictions compétentes d'apprécier le caractère sexuel des paroles ou images diffusées ainsi que l'absence de consentement de la personne à cette diffusion. En faisant référence aux enregistrements ou documents obtenus « à l'aide de l'un des actes prévus à l'article 226-1 » du Code pénal, qui recouvrent la captation, la fixation, l'enregistrement ou la transmission de paroles ou d'images, le législateur a uniquement défini les actes matériels ayant permis à l'auteur de leur diffusion d'obtenir ces enregistrements et documents, sans les restreindre aux seuls actes réalisés dans un lieu privé. D'autre part, il n'a pas entendu incriminer un mode particulier de diffusion.

Ces dispositions n'ont pas pour effet de déroger au principe, prévu par l'article 121-3 du Code pénal, selon lequel il n'y a pas de délit sans intention de le commettre.

De ce fait, le grief tiré de la méconnaissance du principe de légalité des délits et des peines doit être écarté. L'article 226-1-2 ne méconnaît pas non plus le principe de nécessité des délits et des peines, ni aucun autre droit ou liberté que la Constitution garantit. Il doit être déclaré conforme à la Constitution.

L'article 226-2-1 du Code pénal est issu de la loi pour la République numérique du 7 octobre 2016. Sa rédaction fait suite à l'arrêt de la Cour de cassation du 16 mars 2016 qui, à propos d'un « revenge

porn » avait constaté, qu'en l'état du droit, n'était pas pénalement réprimé le fait de diffuser sans son accord l'image d'une personne réalisée dans un lieu privé avec son consentement. Cet arrêt a fait l'objet d'une critique de la doctrine qui a reproché « une certaine déconnexion de la justice face à la réalité numérique ». Mais en matière pénale la loi est d'interprétation stricte…

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS
DE LA GENDARMERIE NATIONALE

NOVEMBRE 2021

CREOGN
CENTRE DE RECHERCHE
DE L'ÉCOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Général d'armée (2S) Marc Watin-Augouard

Convention de Budapest
Un deuxième Protocole pour lutter contre la cybercriminalité

Près de 20 ans, jour pour jour, après l'ouverture à la signature de la Convention de Budapest, un deuxième Protocole additionnel vient d'être adopté, le 17 novembre 2021, par le Comité des ministres du Conseil de l'Europe. Cette modification vient à point nommé, eu égard à l'évolution de la cybercriminalité, mais aussi en raison de l'importance croissante de la preuve numérique dans la criminalité classique.

La genèse

Depuis le 23 novembre 2001, la Convention a vu croître le nombre d'États l'ayant ratifiée. Au nombre de 66 aujourd'hui, ils ne relèvent pas tous du Conseil de l'Europe, puisqu'on note la présence des États-Unis, du Canada, de l'Australie, du Japon et de pays d'Afrique ou d'Amérique latine. Ne sont pas signataires la Russie, la Chine, Cuba, l'Iran, la Corée du Nord, États dont les territoires sont la base de départ de très nombreuses cyberattaques. L'Irlande n'a pas ratifié la Convention, alors qu'elle héberge les sièges européens des GAFAM (Google, Apple, Facebook, Amazon, Microsoft).

Si le nombre d'États ayant ratifié la Convention semble encore insuffisant, eu égard au caractère planétaire de la cybercriminalité, plus de 20 d'entre eux ont fondé sur elle leur propre loi et plus de cinquante s'en sont inspirés. La Convention bénéficie donc d'un rayonnement international certain. En 2003, la Convention a été complétée par un Protocole additionnel, relatif à l'incrimination des

actes de nature raciste et xénophobe, commis par le biais de systèmes informatiques.

Depuis 2001, l'espace numérique a profondément évolué, notamment sous l'influence du développement du *cloud*. La Convention harmonise les éléments de droit pénal matériel interne des infractions et les dispositions connexes dans le domaine de la cybercriminalité. Elle prévoit les règles de procédures pénales internes nécessaires aux enquêtes et aux poursuites. Celles-ci concernent les infractions qui visent les systèmes informatiques comme celles commises au moyen de ces systèmes. La Convention a aussi pour objectif de faciliter le recueil des preuves numériques nécessaires à la résolution d'infractions qui n'ont pas de lien direct avec le cyberespace. La Convention met en place des mécanismes rapides et efficaces de coopération internationale. Parce qu'elle est neutre au regard des technologies, elle bénéficie d'une certaine stabilité. Mais elle doit évoluer en raison des mutations du cyberespace et de l'évolution des usages.

En vue de compléter ou d'amender la Convention, le Comité de la Convention sur la cybercriminalité (T-CY), en vertu des pouvoirs qu'il tire de l'article 46 de la Convention, a créé, en 2012, un groupe *ad hoc* sur l'accès frontalier aux données et sur les questions de compétence territoriale. En 2015, il a créé un « Groupe sur les preuves dans le nuage », avec pour domaine d'étude l'accès de la justice pénale aux preuves stockées dans le « nuage ». En 2016, ce groupe est arrivé à la conclusion que « la cybercriminalité, le nombre de terminaux, de services et d'utilisateurs (notamment de terminaux et services mobiles) et, partant, le nombre de victimes ont atteint des proportions telles que seule une infime partie de la cybercriminalité ou autres infractions impliquant des preuves électroniques sera jamais enregistrée et donnera jamais lieu à des enquêtes. L'immense majorité des victimes ne peut pas s'attendre à

ce que justice soit rendue ». Ainsi a-t-il mis en évidence la difficulté d'obtention d'un accès efficace aux preuves électroniques et de leur divulgation sous la triple contrainte de « l'informatique en nuage, la territorialité et la compétence ».

Au regard des conclusions du « Groupe sur les preuves dans le nuage », les Parties à la Convention ont conclu qu'il n'était pas nécessaire de modifier la Convention mais d'élaborer un deuxième Protocole additionnel afin de renforcer l'efficacité de l'action de la justice pénale et de préserver l'État de droit. Le T-CY a donc engagé ses travaux entre septembre 2017 et mai 2021, émaillés de nombreuses consultations, notamment dans le cadre des Conférences Octopus sur la cybercriminalité qui se tiennent chaque année à Strasbourg et rassemblent des experts de 80 pays, des organisations internationales, du secteur privé et du monde universitaire.

Les défis à relever

Pour les rédacteurs du Protocole, il convenait de relever les défis liés à la territorialité, notion qui est peu pertinente dans un espace numérique sans frontière. Le stockage des données dans le *cloud* pose de nombreux problèmes aux enquêteurs. Confrontés à la rigidité des demandes d'entraide auprès d'autres États, les rédacteurs ont imaginé un mécanisme plus simple pour émettre des ordres ou des demandes aux fournisseurs de services d'autres Parties afin de produire des informations sur les abonnés et des données relatives au trafic. Par ailleurs, devant les difficultés soulevées par le « Who is ? » permettant d'identifier les personnes ayant enregistré un nom de domaine, ils ont conçu un dispositif permettant d'obtenir auprès des registraires et registres les informations nécessaires. Enfin, ils ont voulu renforcer les capacités

d'action en cas d'urgence.

La preuve numérique objet du Protocole

Le champ du nouveau Protocole est large et dépasse celui des infractions « cyber » au sens strict. Il s'applique aux enquêtes ou procédures pénales spécifiques concernant des infractions pénales « liées à des données et systèmes informatiques ». Il concerne donc non seulement la cybercriminalité, mais toute infraction pénale pour laquelle les preuves se présentent sous forme électronique, les « preuves numériques ». Les pouvoirs, procédures et mesures de coopération créés par le Protocole peuvent être utilisés lorsque l'infraction est commise par le biais d'un système informatique, ou lorsqu'une infraction qui n'a pas été commise par le biais d'un système informatique (par exemple un meurtre) implique des preuves électroniques.

Le Protocole prévoit des garanties au regard notamment du respect de la vie privée et du traitement de données à caractère personnel[1].
Les sept mesures de coopération principales sont contenues dans le chapitre II.
Les premières renforcent la coopération directe avec les fournisseurs et les entités dans les autres Parties. Il s'agit des

1. Ces garanties n'ajoutent rien à celles déjà prévues par l'Union européenne au travers du Règlement général sur les données à caractère personnel (RGPD) et de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

articles dits de « coopération directe », qui permettent aux autorités compétentes d'une Partie de s'engager directement avec des entités privées.

L'identification des détenteurs de noms de domaine (art. 6)

L'obtention des données d'enregistrement d'un nom de domaine est souvent une étape indispensable pour de nombreuses enquêtes criminelles, notamment pour localiser les Parties auxquelles il convient d'adresser des demandes de coopération internationale. Autrefois accessibles à tous, par des outils de recherche connus sous l'acronyme WHOIS (*who is*), certaines parties de l'information sont aujourd'hui d'accès restreint, ce qui produit des effets négatifs sur les missions des services judiciaires et répressifs. Les informations d'enregistrement de noms de domaine ne permettent pas de tirer des conclusions précises concernant la vie privée de quelqu'un. Leur divulgation peut donc être moins intrusive que celle d'autre catégories de données.
Le Protocole remédie à cette difficulté. Pour rattacher les noms de domaine à une personne et à un lieu, les autorités compétentes en matière d'enquête sont habilitées à émettre, auprès d'une entité fournissant des services d'enregistrement de noms de domaine, située sur le territoire d'une autre Partie, une demande d'informations, en vue d'identifier ou de contacter la personne ayant enregistré un nom de domaine.
La Partie sur le territoire de laquelle est située cette entité (registraire, registre) doit prendre les mesures législatives nécessaires pour permettre la divulgation de l'information demandée.

La divulgation directe de données relatives aux abonnés (art. 7)

La procédure d'entraide n'est pas le moyen le plus adapté pour traiter un nombre croissant de demandes de preuves électroniques volatiles. D'où la définition d'un mécanisme simplifié pour émettre des ordres ou des demandes aux fournisseurs de services d'autres parties afin de produire des informations. Cette disposition permet à « un procureur ou à une autre autorité judiciaire, sous la supervision de cette autorité ou sous une autre forme de supervision indépendante » de s'adresser directement à un fournisseur de services sur le territoire d'une autre Partie, par le biais d'une injonction de produire des données spécifiées et stockées relatives à des abonnés[2].

Les procédures renforçant la coopération internationale entre autorités pour la divulgation de données informatiques stockées

Il s'agit tout d'abord des injonctions d'une Partie sur une autre Partie ordonnant à un fournisseur de services établi sur son territoire la production accélérée de données relatives aux

2. « Toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base du contrat ou de l'arrangement de service. »

informations sur les abonnés et au trafic[3] spécifiées et stockées, en la possession ou sous le contrôle du fournisseur de service (art. 8).

Sont également prévues des procédures relatives à une demande d'entraide urgente.
La notion d'urgence correspond aux situations dans lesquelles le risque est grave et imminent, ce qui exclut les cas où le risque pour la vie ou la sécurité d'une personne est passé ou négligeable. Le risque futur, s'il existe, n'est pas immédiat. Sont ainsi évoqués dans le rapport explicatif « la prise d'otage, situation dans laquelle existe un risque crédible et imminent de décès, de blessure grave ou d'un autre préjudice comparable pour la victime ; la persistance des abus sexuels auxquels un enfant est soumis ; les scénarios immédiatement postérieurs à une attaque terroriste, dans lesquels les autorités cherchent à savoir avec qui les attaquants ont été en communication afin de déterminer si de nouvelles attaques sont imminentes, et les menaces pour la sécurité d'infrastructures essentielles s'accompagnant d'un risque grave et imminent pour la vie ou la sécurité d'une personne physique ».
Chaque Partie doit faire en sorte que son « point de contact » 24/7, prévu à l'article 35 de la Convention, puisse transmettre une demande à un Point de contact dans une autre Partie et recevoir une demande de ce dernier pour une assistance immédiate en vue de l'obtention par un fournisseur de services situé sur le territoire de la Partie concernée de la divulgation accélérée de données informatiques stockées spécifiées qui sont en la possession ou sous

3. « Toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent. »

le contrôle dudit fournisseur de services, sans requête d'entraide judiciaire (art. 9).
Chaque Partie peut demander une entraide judiciaire par les moyens les plus rapides lorsqu'elle estime qu'il y a urgence. Une personne de chaque Partie doit être disponible vingt-quatre heures sur vingt-quatre, sept jours sur sept, pour répondre à une demande présentée dans de telles circonstances (art. 10).

Les procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables

La visioconférence ou les équipes communes d'enquête sont d'ores et déjà mises en oeuvre en vertu d'instruments du Conseil de l'Europe (par exemple, le Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, STE n° 182, ci-après le « Deuxième Protocole STE no 182 ») ou d'autres accords bilatéraux et multilatéraux. Cependant, de tels mécanismes ne sont pas appliqués par toutes les Parties à la Convention, et le Protocole vise à combler cette lacune. L'article 11, intitulé « Vidéoconférence », et l'article 12, intitulé « Équipes communes d'enquête et enquêtes communes », prévoient des mesures de coopération internationale qui ne s'appliquent que lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre les Parties requérante et requise.

Les rédacteurs du Protocole ont également examiné d'autres mesures qui n'ont pas été retenues afin de ne pas retarder la publication du texte. En font notamment partie les « enquêtes clandestines à l'aide d'un système informatique » et l'extension du champ des perquisitions. Ces thématiques seront abordées dans un

autre instrument juridique. Compte tenu de l'évolution du numérique, des usages et des mésusages, il est acquis que ce Deuxième protocole sera suivi d'autres initiatives, sauf à laisser le droit dériver face à la croissance qualitative et quantitative de la cybercriminalité.

Loi n° 2021-1485 du 15 novembre 2021 visant à réduire l'empreinte environnementale du numérique en France

La loi est une illustration de la convergence entre la transformation numérique et la transition écologique. Elle s'inspire du rapport d'information établi par deux sénateurs, en date 24 juin 2020[4], soulignant que « le numérique est l'angle mort des politiques environnementales et climatiques ».
Ce rapport s'est appuyé sur une étude comportant des éléments chiffrés sur l'empreinte carbone du numérique en France[5], ses particularités par rapport aux tendances mondiales et son évolution à l'horizon 2040 : « Le numérique constitue en France une source importante d'émissions de gaz à effet de serre (15 millions de tonnes équivalent CO_2), soit 2 % du total des émissions en 2019), qui pourrait s'accroître considérablement dans les années à venir si rien n'était fait pour en réduire l'impact (+ 60 % d'ici 2040, pour atteindre 24 MtCO2eq) ».

4. Rapport d'information n° 555 (2019-2020) de MM. Guillaume Chevrollier et Jean-Michel Houllegatte, fait au nom de la commission de l'aménagement du territoire et du développement durable, déposé le 24 juin 2020 [en ligne]. Disponible sur : https://www.senat.fr/notice-rapport/2019/r19-555-notice.html

5. Étude relative à l'évaluation des politiques publiques menées pour réduire l'empreinte carbone du numérique (juin 2020), réalisée par le cabinet Citizing, Hugues Ferreboeuf et le cabinet KPMG, à la demande de la commission de l'aménagement du territoire et du développement durable du Sénat.

En 2040, selon cette étude, « si tous les autres secteurs réalisent des économies de carbone conformément aux engagements de l'Accord de Paris et si aucune politique publique de sobriété numérique n'est déployée, le numérique pourrait atteindre près de 7 % (6,7 %) des émissions de gaz à effet de serre de la France, un niveau bien supérieur à celui actuellement émis par le transport aérien (4,7 %). Cette croissance serait notamment portée par l'essor de l'Internet des objets (IoT) et les émissions des *data centers*. Le coût collectif de ces émissions pourrait passer de 1 à 12 milliards d'euros entre 2019 et 2040 ».

Le numérique n'est donc pas neutre pour l'environnement et la santé publique. Alors qu'il n'en est qu'à ses balbutiements, il est nécessaire de concilier sa croissance avec les exigences d'un développement durable. La question ne concerne pas seulement la production de CO_2, gaz à effet de serre, mais aussi l'impact sur l'eau, les conséquences environnementales de l'exploitation des terres rares, les répercussions sur la santé des personnes qui recyclent nos déchets numériques dans des conditions non contrôlées, sauf par la criminalité organisée…

La loi du 15 novembre demeure modeste dans ses ambitions. Elle s'articule autour de cinq idées fortes :

– faire prendre conscience aux utilisateurs de l'impact environnemental du numérique ;

– limiter le renouvellement des terminaux ;

– faire émerger et développer des usages du numérique écologiquement vertueux ;

– promouvoir des centres de données et des réseaux moins énergivores ;

– promouvoir une stratégie numérique responsable dans les territoires.

Faire prendre conscience aux utilisateurs de l'impact environnemental du numérique

Cette prise de conscience passe par une formation à la « sobriété numérique » qui doit être enseignée dès le plus jeune âge à l'école ainsi qu'à l'entrée à l'université, à partir de la rentrée 2022 (art. 1 et 2). Les formations d'ingénieur devront également comporter un module relatif à l'écoconception des services numériques et à la sobriété numérique (art. 3). Ces dispositions vont dans le bon sens, mais, comme le propose le Livre blanc de l'Agora du FIC[6], aucune formation diplômante ne devrait être sanctionnée sans une formation *ad hoc* à la cybersécurité, laquelle doit comprendre naturellement un volet environnemental[7].

La connaissance des impacts sur l'environnement sera facilitée par les travaux rendus publics du nouvel Observatoire des impacts environnementaux du numérique qui a pour mission « d'analyser et de quantifier les impacts directs et indirects du numérique sur l'environnement ainsi que la contribution apportée par le numérique, notamment l'intelligence artificielle, à la transition écologique et solidaire ». Cet Observatoire est placé auprès de l'Agence de l'environnement et de la maîtrise de l'énergie ainsi que de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, qui en assurent le secrétariat. Dans le cadre de ses missions, l'Observatoire peut faire appel à des chercheurs et à des personnalités qualifiées.

---

6. « Faire de la cybersécurité la clef de voûte de la souveraineté numérique européenne », proposition n° 2, Avisa Partners-Gendarmerie nationale, 9 septembre 2021 [en ligne]. Disponible sur : https://www.europanova.eu/actualites/faire-de-la-cybersecurite-la-cle-de-voute-de-la-souverainete-numerique-europeenne-

7. L'offre de cybersécurité doit être vertueuse. Les critères environnementaux doivent conditionner les choix et notamment orienter la commande publique.

Limiter le renouvellement des terminaux

L'objectif est d'allonger la durée de vie des produits, car la fabrication des terminaux numériques (smartphones, tablettes, ordinateurs...) représente 70 % de l'empreinte carbone du numérique en France. La loi renforce le délit d'obsolescence programmée, lutte contre l'obsolescence logicielle, favorise les offres reconditionnées, encourage des opérations de collecte nationale accompagnées d'une prime au retour pour les particuliers qui rapportent les équipements dont ils souhaitent se défaire.
La loi complète l'article 55 de la loi n° 2020-105 du 10 février 2020 relative à la lutte contre le gaspillage et à l'économie circulaire par deux alinéas ainsi rédigés :
« À compter du 1er janvier 2023, lors de l'achat public de produits numériques disposant d'un indice de réparabilité, les services de l'État ainsi que les collectivités territoriales et leurs groupements prennent en compte l'indice de réparabilité défini à l'article L. 541-9-2 du code de l'environnement.
« À compter du 1er janvier 2026, lors de l'achat public de produits numériques disposant d'un indice de durabilité, les services de l'État ainsi que les collectivités territoriales et leurs groupements prennent en compte l'indice de durabilité défini au même article L. 541-9-2. »
C'est une manière d'orienter la commande publique vers les produits plus vertueux.

Faire émerger et développer des usages du numérique écologiquement vertueux

L' Autorité de régulation des communications électroniques, des

postes et de la distribution de la presse et le Conseil supérieur de l'audiovisuel, en lien avec l'Agence de l'environnement et de la maîtrise de l'énergie, définissent le contenu d'un référentiel général de l'écoconception des services numériques avec des critères de conception durable afin d'en réduire l'empreinte environnementale. « Ces critères concernent notamment l'affichage et la lecture des contenus multimédias pour permettre de limiter le recours aux stratégies de captation de l'attention des utilisateurs des services numériques. »

Promouvoir des centres de données et des réseaux moins énergivores

La loi renforce les conditionnalités environnementales qui s'appliqueront, à compter de 2022, au tarif réduit de la taxe intérieure de consommation finale d'électricité (TICFE) applicable aux *datacenters*, lesquels doivent pour en bénéficier :
– valoriser la chaleur fatale, notamment à travers un réseau de chaleur ou de froid, ou respecter un indicateur chiffré déterminé par décret sur un horizon pluriannuel en matière d'efficacité dans l'utilisation de la puissance ;
– respecter un indicateur chiffré déterminé par décret sur un horizon pluriannuel en matière de limitation d'utilisation de l'eau à des fins de refroidissement.

Promouvoir une stratégie numérique responsable dans les territoires

Les Plans climat-air-énergie territoriaux (PCAET), outils de planification ayant pour but d'atténuer le changement climatique,

de développer les énergies renouvelables, de veiller à la qualité de l'air et de maîtriser la consommation d'énergie, doivent intégrer l'enjeu de la récupération de chaleur des centres de données. Les communes de plus de 50 000 habitants et les établissements publics de coopération intercommunale à fiscalité propre regroupant plus de 50 000 habitants doivent définir, au plus tard le 1er janvier 2025, une stratégie numérique responsable qui indique notamment les objectifs de réduction de l'empreinte environnementale du numérique et les mesures mises en place pour les atteindre.
Elles élaborent, au plus tard le 1er janvier 2023, un programme de travail qui comporte, notamment, un état des lieux recensant les acteurs concernés et rappelant, le cas échéant, les mesures menées pour réduire l'empreinte environnementale du numérique.
La stratégie numérique responsable fait l'objet d'un bilan annuel dans le cadre du rapport sur la situation en matière de développement durable prévu à l'article L. 2311-1-1 du Code général des collectivités territoriales.

La loi n'est que le « premier chapitre » d'un corpus juridique qui va nécessairement se densifier. Entre l'exploitation de l'argument écologique avancé par ceux qui voudraient entraver le développement du numérique et l'adoption d'un laisser-aller, il y a un équilibre à trouver.

CENTRE DE RECHERCHE DE L'ECOLE DES OFFICIERS DE LA GENDARMERIE NATIONALE

Directeur de publication :	**Colonel Dominique SCHOENHER**
Rédacteur en chef :	**Gal d'armée (2S) Marc WATIN-AUGOUARD**
Rédacteurs :	**Gal d'armée (2S) Marc WATIN-AUGOUARD** **Capitaine Thibaut HECKMANN** **Capitaine Matthieu AUDIBERT** **Lieutenant Océane GERRIET**
Équipe éditoriale :	**Odile NETZER**