LA VEILLE JURIDIQUE

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

N° 91 | Novembre 2020

EDITO

Cette veille est la dernière que j'ai le plaisir de vous présenter en qualité de directeur du CREOGN. Le 3 décembre 2020, en effet, au lendemain de la commémoration de la victoire d'Austerlitz, je vais « tirer ma révérence », eu égard à mon âge. Je suis désormais juridiquement trop âgé pour assurer de telles responsabilités. Mais rassurez-vous, je pars serein et heureux du travail accompli durant presque 9 années, avec une équipe dont je mesure chaque jour la qualité et sans laquelle le CREOGN ne se serait pas hissé au niveau qui est aujourd'hui reconnu. Que tous mes compagnons de route depuis 2012 soient ici chaleureusement remerciés, notamment mes directeurs adjoints Philippe Durand, Laurent Vidal,

(Suite page 2)

CREOGN
CENTRE DE RECHERCHE

Edito

Stéphane Descorsiers et Dominique Schoenher, dont la patience a été sans limite ! Je ne saurais oublier madame Netzer, dont l'implication dans la production de cette veille a été une garantie de qualité et de ponctualité.

À mes remerciements, j'associe bien sûr les Professeurs – dont Frédéric Debove, Claudia Ghica-Lemarchand et Xavier Latour, coauteurs de cette veille, ou François Dieu – qui m'ont aidé à inscrire le CREOGN dans l'écosystème universitaire, dans le cadre des enseignements, mais aussi par l'organisation de colloques. Les auteurs non universitaires, Elisabeth Rolin et Ludovic Guinamant, ne sont pas oubliés dans mes pensées.

Je suis heureux de voir arriver le général Daoust, nouveau directeur, ancien patron du Pôle judiciaire de la gendarmerie nationale (PJGN), après avoir commandé l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN). Avec lui, le CREOGN va poursuivre son orientation sur l'étude des nouvelles technologies et de leurs conséquences sur notre vie quotidienne, la sécurité et la défense, accentuant ainsi sa marque en favorisant la convergence des « sciences dures » et des sciences humaines et sociales.

Au même moment s'opérera le passage de flambeau entre le colonel (ER) Philippe Durand, ancien directeur adjoint du Centre, rédacteur en chef de la Revue de la gendarmerie nationale et Matthieu Frachon, journaliste, réserviste opérationnel. Ayant exercé un travail de bénédictin, en allant souvent au-delà du « contrat » par l'implication bienveillante de son épouse, relectrice bénévole, Philippe Durand peut être fier de la qualité de la Revue et de son rayonnement croissant. Qu'ils soient, lui et son épouse, remerciés à la hauteur de leur engagement ! Je souhaite la

Edito

bienvenue à son successeur que je connais suffisamment pour avoir une totale confiance dans la poursuite d'une publication créée… en 1929.

Je quitte mes fonctions, mais je n'abandonne pas ma responsabilité de rédacteur en chef de la veille juridique. L'âge n'entraîne pas nécessairement la nécrose du cerveau. J'espère pouvoir faire la démonstration du maintien de ma curiosité, de mon émerveillement, de ma volonté de servir encore une gendarmerie qui m'a tant donné et un CREOGN qui a fait le bonheur de mes « vieux jours » professionnels.

Restez fidèles au CREOGN !

Bonne lecture de cette veille juridique !

Par le général d'armée (2S) Marc WATIN-AUGOUARD

SOMMAIRE

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

Droit de l'espace numérique

VEILLE NUMÉRIQUE

Lieutenant Océane GERRIET

La CJUE : un premier pas vers la consécration du principe de neutralité du Net

CJUE - Grande chambre - Arrêt C-807/18 et C-39/19 - 15 septembre 2020 - Telenor Magyarorzag Zrt

Dans un arrêt rendu le 15 septembre 2020, la Cour de justice de l'Union européenne (CJUE) statue pour la première fois sur la réglementation relative à un Internet ouvert. Elle considère qu'une politique commerciale ne doit pas porter atteinte à ce principe et que l'analyse de son impact doit se faire à l'échelle globale du marché. En outre, elle rappelle que les cas de mesures permettant de réguler le trafic et, de surcroît, de le ralentir, sont strictement et limitativement définies par la réglementation, de sorte que les préférences purement commerciales ne sont pas au nombre de celles-ci. Le traitement égal et non discriminatoire du trafic d'Internet s'oppose donc à des offres de la part d'un fournisseur d'accès qui privilégient certains services et opèrent des blocages ou des ralentissements sur d'autres.

Il était une fois, dans une galaxie pas si lointaine, le premier arrêt de la CJUE concernant la neutralité du Net… Depuis longtemps, les rebelles luttent pour faire consacrer et appliquer le principe de

neutralité qui se veut comme un véritable corollaire de la **liberté** et de la démocratie. Tandis que le côté obscur de la force cherche, ici et là, à tester les limites de la réglementation.

En vérité, il est temps de quitter cette version imagée et exagérée de l'histoire qui n'a que pour objectif de vous soutirer un sourire en cette période très sombre et d'aborder l'arrêt rendu par la CJUE ce 15 septembre 2020, qui est très important, car le premier rendu à propos du règlement (UE) 2015/2120 du Parlement européen et du conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert.

Les faits sont les suivants : une société de télécommunication norvégienne (TELENOR) dispose de nombreuses filiales, dont une en Hongrie qui est mise en cause par l'Autorité nationale hongroise des communications et des médias (ANCM). Cette dernière estime que deux des offres de TELENOR ne respectent pas l'obligation de traitement égal et non discriminatoire prévu par le règlement et, plus particulièrement, **son article 3** dont les dispositions visent à *« garantir l'accès à un Internet ouvert »*. En l'espèce, cette société (fournisseur d'accès à Internet – FAI –) proposait deux offres permettant pour l'une, l'accès à des applications de musique et pour l'autre, l'accès à des applications de communication en proposant un volume de données restreint. Une fois ce volume consommé, des mesures de ralentissement du débit étaient mises en place, à l'exception de certaines applications bénéficiant d'un « tarif nul » qui ne débitaient aucune donnée et n'étaient nullement ralenties après expiration du forfait.

L'ANCM a prononcé deux décisions de non-conformité de ces offres à l'article 3 du règlement et a exigé que la société y mette fin. Cette dernière a levé le contentieux devant la Cour de Budapest qui a estimé que les dispositions du règlement revêtent une importance majeure, que les questions soulevées sont nouvelles et doivent être renvoyées à la CJUE à titre préjudiciel.

Ces questions avaient trait à l'interprétation dudit article et, plus précisément, à l'articulation de ses 3 premiers paragraphes. Pour mémoire, le **paragraphe 1** consacre l'étendue du droit à un accès à un Internet ouvert puisqu'il souligne que *« les utilisateurs finaux »* ont le *« droit d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où [ils se trouvent], [où se trouve le fournisseur] quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet »*. Ensuite, le **paragraphe 2** précise que les *« accords portant sur les conditions commerciales et techniques entre le FAI et l'utilisateur »* ainsi que *« les pratiques commerciales mises en place par les FAI »* ne doivent pas limiter les droits prévus au paragraphe 1. Enfin, le **paragraphe 3** rappelle aux FAI qu'ils doivent traiter *« tout le trafic de façon égale et sans discrimination, restriction ou interférence »* quels que soient l'expéditeur, le destinataire, l'équipement utilisé et le contenu. Toutefois, il prévoit également la possibilité de mettre en œuvre *« des mesures raisonnables de gestion du trafic non discriminatoire, transparente et proportionnée »* reposant *« sur des différences objectives entre les exigences*

techniques en matière de qualité de service » qui ne doivent durer que le temps strictement nécessaire à l'objectif poursuivi et ne doivent pas, dans la mesure du possible *« bloquer, ralentir, modifier, restreindre, perturber, dégrader ou traiter de manière discriminatoire les contenus »*, sauf si cela est nécessaire dans un temps strictement contraint dans 4 cas strictement définis (se conformer à un acte législatif qui contraint le FAI, se conformer à une décision judiciaire ou à une autorité publique dotée de pouvoir *ad hoc*, préserver l'intégrité et la sûreté du réseau ou prévenir une congestion imminente du réseau).

Les questions soulevées étaient donc les suivantes :

1. Les principes énoncés à l'article 3 évoquent *« les utilisateurs finaux »*, de sorte qu'un accord commercial conclu entre un FAI et un seul utilisateur final entraînant une différenciation doit-il être interprété comme étant conforme à l'**article 3§2** ?
2. Si non, faut-il interpréter l'**article 3§2** à la lumière de l'**article 3§1** en évaluant l'impact des mesures sur les droits des utilisateurs finaux ?
3. Est-ce que l'obligation imposée par l'**article 3§3** (traiter le trafic de manière égale et sans discrimination ni restriction) est absolue en ce sens que *« toute mesure de gestion de trafic »* prévue à l'**article 3§3** établissant une différenciation dans les contenus proposés, y compris par la voie d'un accord commercial, est interdite ?
4. Si oui, est-ce que la simple constatation de mesures de

gestion discriminatoire (article 3§3) suffit à faire constater la non-conformité au règlement sans avoir besoin d'examiner la conformité du litige aux §1 et §2 ?

D'une part, et comme l'indique le 6e considérant du règlement, l'utilisateur final ne peut exercer ses droits que **par l'intermédiaire** d'un FAI, ce qui souligne *de facto* le rôle fondamental que doit jouer ce dernier puisqu'il doit permettre l'effectivité des droits garantis. En outre, la Cour rappelle le champ d'application de l'article 3§2 qui concerne aussi bien les accords conclus entre un FAI et son utilisateur sur les *« conditions commerciales et techniques du service »* telles que le prix, le volume de données ou le débit, *« **que les pratiques commerciales** mises en place »* permettant de proposer des services variés adaptés aux préférences de chacun. Le terme *« pratique commerciale »* est suffisamment éloquent puisque la juridiction rappelle qu'il peut s'agir d'offres de service et de prix parfois adaptés à la population concernée. En tous les cas, ni l'un ni l'autre ne doivent faire obstacle *« à la garantie d'un accès à un Internet ouvert »* ou contourner d'une manière ou d'une autre les garanties mises en place. En outre, la Cour précise le sens à donner au terme *« **utilisateur** »*. Pour mémoire, ce terme est défini par la Directive cadre 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre ») comme l'ensemble des personnes utilisant ou demandant un service de communication électronique. Elle définit également l'utilisateur final comme un utilisateur qui ne fournit pas de réseaux de communication publics ou de services de communications électroniques accessibles au public en ligne. En l'espèce, elle

souligne que **l'utilisateur final** concerne aussi bien les consommateurs particuliers que les consommateurs professionnels, ce qui multiplie de fait l'impact des politiques commerciales choisies.

C'est pourquoi, la Cour s'intéresse ensuite à l'impact de la pratique commerciale menée par TELENOR. Il ne s'agit pas d'interférer avec un accord en particulier mais bien d'analyser, en l'espèce, **la pratique commerciale dans son ensemble et son impact sur le marché**. Ici, les offres groupées proposées par la société constituent bien une pratique commerciale relevant du champ du §2. Cette pratique commerciale a bien pour objectif de conduire à la conclusion d'accords et il est évident que plus le nombre de clients est élevé, plus *« l'incidence de ces accords est susceptible, compte tenu de son ampleur, d'engendrer une limitation importante de l'exercice des droits »* des utilisateurs. Dès lors, en proposant des offres qui privilégient certaines applications ne connaissant aucune restriction de débit et aucune consommation de données, le FAI participe à la « [raréfaction] de l'utilisation des autres applications (…) compte tenu des mesures par lesquelles [il en rend l'accès] techniquement plus difficile voire impossible ». **Par conséquent**, la Cour constate une incompatibilité de la politique commerciale de la société et, plus précisément, de ces deux offres groupées, aux dispositions de l'**article 3§2 et §1**.

D'autre part, eu égard aux problèmes d'interprétation soulevés vis-à-vis du **paragraphe 3**, la Cour va confirmer la position de l'Autorité hongroise. Il s'agissait ici d'étayer le principe de traitement égal du trafic et ses exceptions. Premièrement, elle rappelle que les

conditions de mise en place *« de mesures raisonnables de gestion de trafic »* sont précisément définies. En effet, elles doivent être *« **non discriminatoires**, transparentes et proportionnées » **en reposant « sur des différences objectives entre les exigences techniques en matière de qualité de service »***. Outre cela, les FAI doivent s'abstenir de *« bloquer, ralentir, modifier, restreindre, perturber, dégrader ou traiter de manière discriminatoire les contenus »*, sauf si cela est nécessaire et pour une durée limitée, dans un des 4 cas suivants : le FAI doit se conformer à une législation nationale, le FAI doit se conformer à une décision de justice, le FAI doit préserver l'intégrité et la sûreté du réseau ou le FAI doit prévenir une congestion imminente du réseau et atténuer ses effets. En l'espèce, la Cour ne peut que constater que la différenciation mise en œuvre par la société ne repose nullement sur des spécifications techniques objectives en matière de qualité de service mais uniquement sur des considérations commerciales visant à favoriser telle ou telle application. En outre, la société a mis en place des mesures de ralentissement de débit. Or, comme le soulignent les dispositions de l'**article 3§3**, ce type de mesure doit être évité, sauf si elle concerne un des 4 cas définis par le règlement. La CJUE estime par ailleurs que ces exceptions sont *« soumises à une interprétation stricte [et une exigence de proportionnalité] »*. En l'espèce, les mesures mises en place reposent uniquement sur des considérations commerciales qui ne rentrent pas dans le cadre prévu à l'article 3 et encore moins dans une des exceptions prévues.

Partant, il n'est pas nécessaire d'évaluer l'incidence d'une telle

mesure de gestion du trafic sur l'exercice des droits des utilisateurs (**article 3§1**), puisqu'il suffit de constater que ces mesures ne sont pas conformes aux conditions posées par l'article 3§3. En ce sens, et sans qu'il y ait besoin d'analyser leur incidence concrète, les pratiques commerciales menées par la société TELENOR constituent une violation des dispositions de l'**article 3§3**.

Cette décision est importante, car c'est la première fois que la CJUE statue sur le règlement portant sur la neutralité du Net et renforce, indubitablement, cet objectif. En effet, eu égard à une telle interprétation, il peut paraître plus aisé pour les autorités chargées de réguler ces pratiques d'apporter la preuve d'une violation de la loi puisqu'elles n'ont pas besoin de démontrer une atteinte effective au droit d'un ou des utilisateurs. Cet arrêt vient donc mettre un frein à de telles pratiques et rappelle aux FAI la lourde responsabilité qui est la leur. Bien entendu, les États ont un rôle à jouer en assurant leur rôle de « gendarmes ». Pour mémoire, l'article L. 36-11 du Code des postes et des communications électroniques permet à l'Autorité de régulation des communications électroniques et des Postes (ARCEP) d'initiative, ou à la demande, de constater, mettre en demeure et sanctionner les manquements commis par les *« exploitants de réseau, des fournisseurs de services de communications électroniques, des fournisseurs de services de communication au public en ligne ou des gestionnaires d'infrastructures d'accueil »* à différentes réglementations, dont le règlement 2015/2120. Sur ce point, il convient de souligner que les sanctions peuvent être pécuniairement lourdes puisqu'elles peuvent atteindre jusqu'à 3 %

du chiffre d'affaires. En tout état de cause, cet arrêt apparaît comme un pas en avant vers un cyberespace libre et neutre, ce qui aurait sans doute eu de quoi ravir John Perry Barlow qui avait, en 1996, lors du Forum de Davos, rédigé *La déclaration d'indépendance du cyberespace*. En effet, outre l'idée d'un espace sans frontière, il s'agissait également de permettre à cet espace d'être libre, libre de toute forme de pouvoir. Or, on comprend aisément que, si la neutralité d'Internet est un enjeu démocratique, il n'en va pas de même des intérêts du secteur économique pour lequel le cyberespace est un marché très lucratif. Nul doute que ce n'est que le début du contentieux en la matière…

Général d'armée (2S) Marc WATIN-AUGOUARD

Cour de justice de l'Union européenne – Grande chambre – Affaires C-551/18 et C-552/18 – Arrêt du 6 octobre 2020 – Quadrature du Net, French Data Network et autres / Premier ministre, garde des Sceaux, ministre de la Justice et autres

La directive « vie privée et communications électroniques » s'applique à des réglementations nationales imposant aux fournisseurs de services de communications électroniques de procéder, aux fins de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, à des traitements de données à caractère personnel, tels que leur transmission à des autorités publiques ou leur conservation.

Droit de l'espace numérique

Dans la veille juridique d'octobre 2020 (p. 16-23), nous avons publié une première analyse relative à un arrêt dont les conséquences n'ont sans doute pas été mesurées par les magistrats européens, malgré les nombreuses contributions d'États membres de l'Union.

S'il est vrai que les services de renseignement sont moins impactés par les restrictions que le sont les services enquêteurs (ce qui est un comble, car ces derniers sont placés sous le contrôle direct de magistrats, tout au long d'une procédure transparente et contradictoire), les juges autorisent quelques dérogations permettant d'obtenir la conservation ciblée des données de connexion ainsi que leur conservation rapide, pour lutter contre la « criminalité grave ».

Poser des principes est une chose, s'appuyer sur une sémantique claire en est une autre ! L'arrêt ne définit pas la notion de « criminalité grave ». Est-ce un acte puni d'une peine d'emprisonnement[1], d'une peine assortie d'un quantum « seuil » ?[2]. L'arrêt est silencieux (cf *infra*, p. 24-26).

On notera que les « ouvertures » ne valent que pour le futur et ne permettent pas de remonter dans le passé. Elles sont réactives et non proactives. Bref, la prévention de la criminalité et de la délinquance est sacrifiée sur l'autel de la protection du délinquant. La victime est oubliée, alors qu'elle devrait être au cœur des préoccupations des juges.

Tant que la loi française n'est pas modifiée, le droit actuel

1. Il suffit, par exemple, qu'une peine soit passible d'emprisonnement pour que l'enquête sous pseudonyme soit possible.

2. Deux ans d'emprisonnement permettent, par exemple, le recours aux services du Centre technique d'assistance (CTA) de la Direction générale de la sécurité intérieure (DGSI) pour mettre au clair un message chiffré.

s'applique. Sur les textes réglementaires, le Conseil d'Etat devra trancher. L'arrêt crée une instabilité juridique considérable et néglige le fait que la protection du citoyen contre la criminalité est un objectif à valeur constitutionnelle.
L'analyse faite ci-après par Matthieu Audibert est suffisamment éclairante pour faire prendre conscience des conséquences graves d'un arrêt « hors-sol ».

Capitaine Matthieu AUDIBERT

La conservation des données de connexion
Le droit français et la Cour de justice de l'Union européenne
Quelles conséquences pour les enquêtes judiciaires ?

À l'heure actuelle, le droit français prévoit un cadre juridique précis pour la conservation généralisée et indifférenciée des données techniques de connexion[3] et des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne[4].
L'article L. 34-1 III du Code des postes et des communications électroniques (CPCE) dispose que *« pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales (…), il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines*

3. Article L 34-1 III du Code des postes et des communications électroniques.
4. Article 6 II de la loi n° 2004-575 du 21 juin 2004, Loi pour la confiance dans l'économie numérique (LCEN).

catégories de données techniques. (…)».

Ces données techniques sont détaillées à l'article R. 10-13 du même Code. Ainsi, *« (…) les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales : les informations permettant d'identifier l'utilisateur ; les données relatives aux équipements terminaux de communication utilisés; les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs; les données permettant d'identifier le ou les destinataires de la communication »*. Ce même article prévoit que les opérateurs conservent les données susmentionnées pour les activités de téléphonie mais aussi celles permettant d'identifier l'origine et la localisation de la communication. Cette durée de conservation des données est d'un an à compter du jour de l'enregistrement.

S'agissant des contenus publiés sur Internet, l'article 6 II de la Loi pour la confiance dans l'économie numérique (LCEN) dispose que *« les personnes mentionnées aux 1 et 2 du I [fournisseurs d'accès à internet et hébergeurs] 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 »*.
Le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne vient préciser les données qui doivent être conservées.

Les données visées ici sont appelées données techniques de connexion. En pratique, il s'agit de métadonnées liées aux communications électroniques et de métadonnées liées à la création de contenus sur Internet.

Plusieurs associations, dont la Quadrature du Net, ont contesté devant le Conseil d'État la légalité de la réglementation française rappelée *supra* en attaquant les dispositions réglementaires de celle-ci. Ces associations estiment que ces dispositions réglementaires sont non conformes à la directive 2002/58/CE *ePrivacy* telle qu'interprétée par la CJUE dans son arrêt rendu le 21 décembre 2016 dans l'affaire *Tele 2 Sverige*. Afin de pouvoir statuer, le Conseil d'État a saisi la Cour de justice de l'Union européenne (CJUE) de plusieurs questions préjudicielles[5], qui ont été jointes à des affaires britannique et belge et sur lesquelles la Cour s'est prononcée le 6 octobre 2020.

S'agissant des enquêtes judiciaires, le Conseil d'État a posé les questions préjudicielles suivantes :

- *« L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive [2002/58], ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la [Charte] et les exigences de la*

5. Conseil d'État, 6 septembre 2018, n° 394922.

sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 [TUE] ? »

- « Les dispositions de la directive [2000/31], lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la [Charte], doivent-elles être interprétées en ce sens qu'elles permettent à un État d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et 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, de conserver 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, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale ? »

Saisie de ces questions préjudicielles, la CJUE va alors se livrer à un contrôle de proportionnalité entre, d'une part, l'objectif d'intérêt public poursuivi par la législation française et, d'autre part, l'atteinte au droit des personnes.[6]

6. CRICHTON Céline, Conservation de données à des fins de sécurité nationale et de lutte contre la criminalité : la CJUE rend ses arrêts, *Dalloz actualité*, 13 octobre 2020. Disponible sur : https://www.dalloz-actualite.fr/flash/conservation-de-donnees-des-fins-de-securite-nationale-et-de-lutte-contre-criminalite-cjue-ren#.X79dj2hKiUk

Droit de l'espace numérique

La conservation des données de communication aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique

La Cour note que, s'agissant de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, *« seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux (…), telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation »*[7].
Or, la Cour considère qu'une telle conservation *« excède les limites du strict nécessaire »*. En effet, cette conservation n'est pas justifiée, car elle vise la totalité des utilisateurs pour le seul objectif de lutte contre la « criminalité grave » et de prévention des menaces graves contre la sécurité publique[8].

La Cour énonce ensuite ce qui serait admissible, à savoir une mesure prévoyant *« à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation »*. Celle-ci doit être limitée au strict nécessaire *« en ce qui concerne les catégories de données à conserver, les moyens de communication visées, les personnes concernées ainsi que la durée de conservation retenue »*[9].
La Cour précise deux options envisageables : tout d'abord des

7. Point 140 de l'arrêt.
8. Points 141-143.
9. Point 147.

personnes qui auraient été *« préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné »*[10], enfin une délimitation fondée sur un critère de zone géographique *« lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave »*[11].

La conservation des adresses IP et des données relatives à l'identité civile aux fins de lutte contre la criminalité et de la sauvegarde de la sécurité publique

Sur ce point, la solution de la CJUE est différente par rapport à la conservation généralisée et indifférenciée des données de connexion. En effet, elle estime proportionnée une législation nationale prévoyant la conservation par les fournisseurs de services de communications électroniques de données relatives à l'identité civile de l'ensemble de ses utilisateurs aux fins de la prévention, de la recherche, de la détection et de la poursuite des infractions pénales[12]. Il convient de souligner que, pour la Cour, la notion de gravité de l'infraction ou de la menace est indifférente, la seule connaissance de l'identité des utilisateurs de ces services ne constituant pas une ingérence grave dans leurs droits.

10. Point 149.
11. Point 150.
12. Points 157-159.

Pour la conservation de l'adresse IP, la Cour adopte une position plus restrictive : sa conservation constitue une ingérence grave dans les droits des utilisateurs[13]. À cet égard, reprenant le principe de proportionnalité, la Cour indique que seule sa conservation dans un objectif de lutte contre la criminalité ou de prévention des menaces graves contre la sécurité publique est de nature à justifier une telle ingérence dans les droits et libertés des utilisateurs[14]. Elle reprend ensuite les garanties évoquées précédemment, fondées sur une limitation dans le temps et une conservation strictement nécessaire.

La conservation rapide des données de connexion et de localisation aux fins de lutte contre la « criminalité grave »

Ici, l'hypothèse visée est celle d'une infraction commise et constatée ou, comme le souligne la Cour, dont l'*« existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée »*[15]. La Cour juge ainsi qu'il est possible de prévoir un cadre juridique national permettant d'enjoindre aux fournisseurs de services de communications électronique de conserver ces données[16]. Là encore, cette conservation doit répondre à l'objectif de lutte contre la « criminalité grave » et cette mesure doit être limitée dans le temps.

13. Point 153.
14. Points 154-156.
15. Point 160.
16. Point 163.

Sur ce point, la CJUE évoque la conservation rapide de données informatiques stockées telle que prévue par l'article 17 de la Convention de Budapest[17]. Ce dispositif a fait l'objet d'une transposition partielle en droit français[18], la conservation des données de trafic et de localisation étant prévue par d'autres dispositions de droit national, notamment dans le Code des postes et des communications électroniques.

La conservation généralisée et indifférenciée des données par les fournisseurs d'accès à des services de communication au public en ligne et par les fournisseurs de services d'hébergement

Comme nous l'avons vu précédemment, cette conservation est fondée sur la LCEN et le décret n° 2011-219 du 25 février 2011.
Pour la CJUE, la directive 2000/31/CE du 8 juin 2000 sur le commerce électronique n'est pas applicable au litige[19]. Ici ce sont la directive *ePrivacy* 2002/58/CE et, le cas échéant, le Règlement général sur la protection des données (RGPD) qui sont applicables[20]. Cette directive s'applique aux services d'accès à Internet et aux services de messagerie sur Internet, dès lors qu'ils impliquent entièrement ou principalement la transmission de signaux sur des réseaux de communication électronique[21].

17. Article 17 de la Convention sur la cybercriminalité dite de Budapest du 23 novembre 2001.
18. Article 60-2 alinéa 2 du Code de procédure pénale.
19. Points 197-199.
20. Points 200-201.
21. Points 204-205.

Ainsi, deux options se présentent :

- Si les données en cause sont soumises à la directive *ePrivacy*, la Cour renvoie à sa position, s'agissant de la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation[22];
- Si le traitement de ces données constitue un traitement de données à caractère personnel, c'est le RGPD qui s'applique et ce dernier s'oppose à une réglementation prévoyant que les fournisseurs d'accès à Internet et les hébergeurs soient contraints de conserver de manière généralisée et indifférenciée ces données[23].

Le juge national et l'arrêt de la CJUE

Une question était posée à la Cour concernant la possibilité pour un juge national de différer dans le temps l'application de l'arrêt de la CJUE par rapport au droit national en vigueur. La Cour répond ici, qu'en vertu du principe de primauté, le juge national est chargé d'assurer le plein effet du droit de l'UE *« en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel »*[24].
Ainsi, le juge national ne peut pas limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, s'agissant d'une législation nationale prévoyant la conservation généralisée et

22. Point 203.
23. Points 213-228.
24. Point 215.

indifférenciée des données[25].

La Cour conclut : le juge national doit 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, 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 »*[26].

Après avoir présenté les grandes lignes de cet arrêt, quelles en sont les conséquences pour les enquêtes judiciaires ?

Premier constat : si la CJUE parle dans son arrêt de la possibilité de recourir à une conservation ciblée des données, elle ne l'envisage que pour la « criminalité grave » ou la prévention des menaces graves contre la sécurité publique. Cette notion de gravité n'est pas définie dans la jurisprudence de la CJUE.
En droit français, les infractions sont classées en trois catégories : contravention, délit et crime avec, pour chacune, des échelles de sanctions différentes. On pourrait en déduire qu'un crime est nécessairement grave mais qu'un délit ne l'est pas. Or, si l'on prend

25. Points 216-220.
26. Points 221-226.

l'exemple d'un délit souvent constaté sur Internet, le cyberharcèlement, celui-ci est puni de deux ans d'emprisonnement et de 30 000€ d'amende[27]. Est-ce une infraction grave ? Pour la victime certainement mais pour l'ordre public ? L'actualité récente nous indique que des faits de cyberharcèlement peuvent déboucher sur des atteintes réelles à l'intégrité physique.
Autre exemple, les atteintes aux mineurs sur Internet (propositions sexuelles, diffusion de l'image d'un mineur présentant un caractère pornographique, etc.) sont des délits et non des crimes[28]. Or, sont-elles des infractions graves ?

Comme le souligne le colonel Éric Freyssinet sur son blog[29], il n'existe à ce jour aucune définition dans le droit de l'Union européenne ou dans le droit français de ce qui relèverait de la « criminalité grave » telle que l'entend la CJUE dans son arrêt. Dans notre droit national, seule l'échelle des peines peut constituer un éventuel indicateur mais comme cela a été expliqué précédemment : peut-on considérer qu'un délit commis sur Internet n'est pas une infraction grave ? Le seul texte explicitant la notion d'infraction grave est la Convention de Palerme relative à la lutte contre le crime transnational organisé adoptée en 2004. Son article 2 b) dispose qu'une infraction grave *« désigne un acte constituant une infraction passible d'une peine privative de liberté dont le*

27. Article 222-33-2-2 du Code pénal.
28. Articles 227-22-1 et 227-23 du Code pénal.
29. FREYSSINET Éric, Décision de la CJUE du 06/10/2020 sur les données de connexion, *Investigation & transformation numériques* (*blog*), 9 octobre 2020. Disponible sur : https://eric.freyssi.net/2020/10/09/decision-de-la-cjue-du-06-10-2020-sur-les-donnees-de-connexion/

maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde ».

On constate ici que c'est l'échelle des peines qui détermine la gravité de l'infraction et non l'atteinte qu'elle est censée réprimer. Dès lors, il serait aisé de modifier l'échelle des peines mais cela ne saurait être une solution satisfaisante, le problème ne consistant pas réellement dans cette notion de « criminalité grave » mais plutôt dans l'absence de conservation de données antérieures à la commission.

En réalité, la liste des délits aggravés par *« l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique »* est extrêmement longue et les investigations sur ces infractions vont être rendues difficiles, presque impossibles avec cet arrêt de la CJUE.

De nombreuses infractions sont commises exclusivement sur Internet ou, en tout cas, par l'utilisation d'un moyen de communication électronique. Pour reprendre les infractions citées *supra*, si la CJUE admet la conservation de l'adresse IP et des identités civiles associées[30], comment faire le lien entre l'équipement terminal et l'adresse IP au moment de la commission des faits ? En pratique ce sera impossible.

Illustration : un individu publie des contenus illicites sur le réseau social Twitter. Un enquêteur constate immédiatement l'infraction

30. Points 152 à 160.

et ouvre une enquête de flagrance[31]. Il constate que le message a été diffusé via une application pour smartphone. Il émet ensuite une réquisition à Twitter[32] pour solliciter la communication des données de connexion concernant le compte ayant diffusé ces contenus. La société Twitter répond en communiquant l'adresse email ou le numéro de téléphone utilisé au moment de la création du compte ainsi que l'adresse IP.
L'enquêteur peut alors identifier le titulaire du compte et son fournisseur d'accès à Internet. Toutefois, comment faire le lien avec le suspect ? En effet, en l'absence de conservation des données de connexion par le fournisseur d'accès (i.e. l'opérateur téléphonique), il serait impossible d'affirmer de manière certaine que c'est de ce téléphone que le suspect s'est connecté tel jour à telle heure sur le réseau social et a publié ce message.

Autrement dit, l'imputation du message sera quasi impossible à prouver puisque les données de connexion seront absentes.

Au-delà des faits commis sur Internet, la conservation des données de connexion est aussi nécessaire pour élucider des enquêtes complexes.

Prenons un autre exemple, s'agissant d'un dossier criminel qui sera bientôt jugé. Dans la nuit du 11 au 12 avril 2017, un individu disparaît à Chambéry. La nuit de sa disparition, son téléphone a été localisé dans le centre-ville puis à 6 km de là. Le 7 septembre 2017,

31. Article 53 du Code de procédure pénale.
32. Article 60-1 du Code de procédure pénale.

un promeneur découvre les restes d'un crâne humain. Plusieurs mois après ces faits, dans une autre enquête criminelle dont les faits ont été commis à plusieurs kilomètres, les enquêteurs ont identifié un suspect. Travaillant sur la téléphonie et l'historique des données de connexion et de localisation (via les relais téléphoniques), ils constatent que le téléphone du suspect a déclenché les mêmes antennes relais que le téléphone de l'individu qui a disparu en avril 2017. Le suspect sera mis en examen dans le cadre de ce dossier.

Que retenir de ce second exemple ?
Sans les données de connexion et de localisation nécessairement antérieures à la commission des faits que les opérateurs conservent en vertu des dispositions législatives et réglementaires en vigueur, il aurait été impossible de faire le lien entre ces deux dossiers, quand bien même une conservation ciblée aurait pu être demandée, la clé des investigations résidant dans les données de connexion antérieures à la découverte des faits.

Que faut-il en conclure ?

Cet arrêt de la CJUE ne peut que soulever une vive inquiétude[33]. Comme le souligne le procureur François Molins[34], *« à l'exception*

33. BERLIN Dominique, La Cour de justice revient sur l'interdiction absolue des mesures générales de conservation et de traitement des données à caractère personnel, pour finalement en dresser le régime dérogatoire, *Juris-Classeur périodique, édition générale (JCP G)*, n° 48, 23 novembre 2020.

34. MOLINS François, La protection des citoyens européens dans un monde ultra-connecté, Fondation Robert Schuman, *Questions d'Europe*, n° 510, 8 avril 2019. Disponible sur : https://www.robert-schuman.eu/fr/questions-d-europe/0510-la-protection-des-citoyens-europeens-dans-un-monde-ultra-connecte

des enquêtes pour association de malfaiteurs visant des objectifs nominatifs, il n'y a pas de crime dont on connaîtrait préalablement les auteurs et dont la conservation des données pourrait être ordonnée. Ce n'est bien évidemment qu'a posteriori, une fois les premiers éléments d'enquête recueillis, que la consultation des données conservées va être effectuée. S'il n'y a pas de données conservées préalablement, il n'y a pas de consultation ».

Il poursuit en indiquant que *« sans conservation préalable des données, il n'est pas possible, après un fait criminel grave tel un acte terroriste, de croiser les connexions entre les personnes impliquées et dès lors d'établir leur participation aux faits ou d'identifier leurs complices et de démanteler les réseaux ».*

Dans un monde de plus en plus connecté et dans lequel le numérique prend de plus en plus de place, il semble impossible de se passer des données de connexion pour lutter contre la délinquance. En 1996, le Conseil constitutionnel déclarait que *« la recherche des auteurs d'infractions est nécessaire à la sauvegarde de principes et droits de valeur constitutionnelle »*[35].
Toutefois, il ne faut pas opposer la protection de la vie privée à la recherche des auteurs d'infractions. Il faut concilier ces deux impératifs. Le choix à privilégier aurait pu être celui de la conservation des données dont l'accès est garanti par le contrôle juridictionnel d'un magistrat indépendant.

35. Conseil constitutionnel, DC n° 96-377 du 16 juillet 1996, §16.

Droit de l'espace numérique

Général d'armée (2S) Marc WATIN-AUGOUARD

JURISPRUDENCE JUDICIAIRE

Tribunal judiciaire de Meaux – 1ère chambre – Ordonnance sur incident du 2 novembre 2020 – M.X / Google LLC

Internet étant accessible en tout point d'un territoire, le demandeur d'un déréférencement peut s'adresser au juge de son choix.

Dans le cadre d'une procédure de « droit à l'oubli », M. X. demande que soit ordonné à la société GOOGLE LLC de déréférencer 14 URL des versions européennes de son moteur de recherche. Google soulève une exception d'incompétence du tribunal, en référence aux dispositions de l'article 42 du Code de procédure civile (la juridiction compétente est celle où réside le défendeur) et à la domiciliation de son siège social aux États-Unis. Google considère que le tribunal saisi n'est ni celui dans le ressort duquel le dommage a été subi, ni celui du lieu du fait dommageable, l'atteinte à son image du fait de référencement des liens concernés portant sur l'exercice par le plaignant de son activité professionnelle au siège de la Bred Banque Populaire à Paris.
Celui-ci réplique qu'il est libre d'assigner la défenderesse devant le tribunal judiciaire de son choix, soit Meaux, dès lors que les faits en cause se sont déroulés sur Internet.
Le tribunal judiciaire de Meaux écarte l'application de l'article 42 (qui aboutirait à la compétence d'un juge californien en raison de

l'implantation du siège social de Google LLC) pour s'appuyer sur l'article 46 du même Code qui offre au demandeur le choix de la juridiction, notamment celle dans le ressort de laquelle le dommage a été subi. Le tribunal judiciaire de Meaux justifie ainsi sa compétence : *« Il est constant que les écrits objet du litige (dont il est sollicité le déréférencement) ont été publiés sur internet et sont en conséquence diffusés sur l'ensemble du territoire national et ainsi mis à la disposition des utilisateurs éventuels du site de sorte que M. X. pouvait légitimement choisir la présente juridiction ».*

JURISPRUDENCE ADMINISTRATIVE

Conseil d'État – 10ème et 9ème chambres réunies – Arrêt du 4 novembre 2020 – La Quadrature du Net/ État

L'application « Alicem » répond aux exigences du Règlement général sur la protection des données (RGPD) relatives au traitement de données biométriques, au consentement, au caractère pertinent, adéquat et non excessif de leur collecte.

Le décret n° 2019-452 du 13 mai 2019 autorise la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile » (« Alicem »). La Quadrature du Net demande au Conseil d'État de l'annuler pour excès de pouvoir. Elle demande également, à titre subsidiaire, de poser à la Cour de justice de l'Union européenne (CJUE) des questions préjudicielles. La première est relative à l'appréciation de la validité du consentement et demande s'il doit être recueilli au niveau de

chaque service faisant l'objet d'un traitement de données personnelles, indépendamment de l'existence d'un autre service « équivalent » ou au niveau de l'ensemble des « services équivalents ». La seconde porte sur le caractère adéquat, pertinent et non excessif, de la collecte et du traitement des données biométriques, au regard des finalités pour lesquelles elles sont collectées et traitées, par une application mobile recourant à une technologie de reconnaissance faciale à des fins d'authentification auprès de certains services publics et de leurs partenaires.

« Alicem », la protection du consentement « by design »

« Alicem » a pour finalité de proposer, aux ressortissants français titulaires d'un passeport biométrique et aux ressortissants étrangers titulaires d'un titre de séjour biométrique, la délivrance d'un moyen d'identification électronique leur permettant de s'identifier électroniquement et de s'authentifier auprès d'organismes publics ou privés. Cette procédure s'opère au moyen d'un équipement terminal de communications électroniques doté d'un dispositif permettant la lecture sans contact du composant électronique de ces titres, en respectant les dispositions prévues par le règlement du Parlement européen et du Conseil du 23 juillet 2014[36], notamment les exigences relatives au niveau de garantie requis par le téléservice concerné. Le traitement utilise un système de reconnaissance faciale statique et de reconnaissance faciale

36. Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

dynamique. Les données collectées par ce système de reconnaissance faciale le sont à cette seule fin et sont effacées sitôt ces reconnaissances terminées. L'Agence nationale des titres sécurisés procède, au moment de la demande d'ouverture du compte, à l'information de l'usager concernant l'utilisation d'un dispositif de reconnaissance faciale et au recueil de son consentement au traitement de ses données biométriques. L'usager enregistre alors une courte vidéo à partir de laquelle un algorithme de reconnaissance faciale vérifie qu'il est le titulaire légitime du titre biométrique sur lequel l'identité numérique est fondée, tandis qu'un algorithme de reconnaissance du vivant analyse les actions effectuées sur la vidéo pour détecter toute tentative d'attaque informatique ou de tromperie. Les identifiants électroniques, associés à son compte, permettent au titulaire d'un passeport ou d'une carte de séjour biométrique de s'identifier en ligne auprès d'organismes publics ou privés partenaires, d'accéder à leurs téléservices et de bénéficier d'une protection renforcée contre l'utilisation abusive ou l'usurpation de son identité dans le cadre de ses démarches en ligne.

Le rejet de la requête par le Conseil d'État

Le Conseil d'État écarte d'emblée les griefs relatifs à la légalité externe du décret – qui a respecté les règles imposées quant à l'identité du texte par rapport au projet de règlement qui lui a été soumis pour avis par le gouvernement – et au contreseing des ministres concernés.

Sur la légalité interne, la première question porte sur la légalité du

traitement de données biométriques. Le Conseil d'État rappelle l'interdiction de principe posée par l'article 8 de la loi du 6 janvier 1978, relative au traitement des données biométriques aux fins d'identifier une personne physique de manière unique. Mais cette interdiction n'est pas absolue, car le RGPD (art. 9) permet de déroger au principe si la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, notamment lorsque *« le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre, proportionné à l'objectif poursuivi et respecte l'essence du droit à la protection des données et prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »*.

Sur la finalité du traitement, le Conseil d'État constate qu'il ne ressort pas des pièces du dossier que, pour la création d'identifiants électroniques, il existait à la date du décret attaqué d'autres moyens d'authentifier l'identité de l'usager de manière entièrement dématérialisée en présentant le même niveau de garantie que le système de reconnaissance faciale. Il s'ensuit que le recours au traitement de données biométriques autorisé par le décret attaqué doit être regardé comme exigé par la finalité de ce traitement. S'agissant du caractère adéquat et proportionné de la collecte de données, le Conseil d'État observe que celle-ci est opérée pour l'identification de l'usager, celle du titre biométrique, de l'équipement terminal de communications électroniques qu'il utilise et, enfin, pour établir l'historique des transactions associées à son compte (informations ne pouvant être communiquées aux

fournisseurs de téléservices) et répond donc aux exigences.
La question de la liberté du consentement est également examinée. Le citoyen n'est pas contraint, selon le juge administratif, car les téléservices accessibles via l'application « Alicem » l'étaient également, à la date du décret attaqué, à travers le dispositif FranceConnect, dont l'utilisation ne présuppose pas le consentement à un traitement de reconnaissance faciale. L'usager qui ne recourt pas à « Alicem » n'est pas privé d'accès aux télétraitements offerts par les services et ne saurait, dès lors, être regardé comme subissant un préjudice au sens du RGPD.
Pour toutes ces raisons, le Conseil d'État rejette la requête de la Quadrature du Net et ne transmet pas à la CJUE les questions préjudicielles. Cette décision enrichit la jurisprudence relative à l'application du RGPD.

ACTUALITÉ NUMÉRIQUE

Capitaine Thibaut HECKMANN

Téléphones sécurisés, « darkphones » : quand le chiffrement devient la norme

La sécurité native des téléphones portables a évolué très rapidement cette dernière décennie avec le renforcement par les constructeurs de la sécurité logicielle (*software*) mais également matérielle (*hardware*). Initialement, ce besoin de sécurité des données s'est fait ressentir par les entreprises qui souhaitaient échanger des données de façon sécurisée. Les ingénieurs avaient

alors dû penser à une nouvelle forme de sécurité en développant des téléphones qui ne permettent pas l'accès aux données d'entreprise en cas de perte ou de vol du téléphone, protégeant ainsi l'accès à des informations sensibles par des tiers.
Très vite, ce besoin des entreprises s'est étendu aux particuliers afin de préserver les données personnelles : sécurisation des échanges privés, des photos et vidéos personnelles, secret des correspondances. En quelques années, le téléphone est passé d'un dispositif permettant de recevoir et passer des appels téléphoniques à un accessoire indispensable pour le travail, favorisant le lien social et la gestion du quotidien professionnel et personnel.

Ainsi, les téléphones classiques non sécurisés et utilisant les réseaux des opérateurs de téléphonie mobile, qui étaient jusque-là facilement exploitables par les enquêteurs lors des saisies judiciaires et par le biais des écoutes judiciaires, ont, dans un premier temps, laissé progressivement la place à des smartphones avec un mot de passe de déverrouillage. Au début, le déverrouillage du téléphone n'était pas une technologie de chiffrement de données, il permettait juste de limiter l'accès aux données du téléphone sans utiliser de technologie de chiffrement au niveau de la mémoire physique du téléphone. Nous verrons dans la suite que, pour la loi française, la nuance entre déverrouillage et déchiffrement est d'une importance capitale.

Les déclarations d'Edward Snowden aux États-Unis, en 2013, révélant un espionnage d'État de la *National Security Agency* (NSA)

a fait la belle affaire des sociétés qui font de la sécurité un argument de vente. Les constructeurs de téléphones portables se sont alors organisés pour augmenter considérablement la sécurité de leurs téléphones mobiles. C'est ainsi que d'un simple téléphone utilisant le déverrouillage pour restreindre l'accès aux données qu'il contient, les industriels ont généralisé la mise en place de puissants algorithmes chiffrant intégralement les données du téléphone. Le mot de passe de chiffrement s'est alors décliné sous plusieurs technologies : la technologie digitale (*les personnes saisissent un mot de passe de plusieurs caractères ou un chemin de déverrouillage*), la technologie biométrique (empreinte digitale ou reconnaissance faciale). Ces technologies ont très rapidement complexifié le travail des enquêteurs pour lire les données du téléphone sans avoir connaissance du mot de passe de déverrouillage (*devenu un mot de passe de chiffrement*), les obligeant à se tourner vers des unités de police ou de gendarmerie expertes. Quelle plus belle publicité pour un constructeur (Apple, Samsung, BlackBerry…) que de pouvoir affirmer que ses téléphones sont inviolables et que même les moyens d'État ne permettent pas d'accéder aux données de son téléphone personnel grand public. Ainsi, la tuerie de San Bernardino en est un exemple concret. Le 2 décembre 2015, une attaque terroriste est perpétrée sur le sol américain, faisant 14 victimes. Le terroriste est abattu par le *Federal Bureau of Investigation* (FBI) et laisse derrière lui un téléphone portable de marque Apple modèle 5C. Nous pouvons alors comprendre la nécessité pour le FBI d'avoir accès aux données du terroriste afin de pouvoir identifier des complices, connaître les interlocuteurs du terroriste et évaluer la probabilité d'autres

attentats. Cependant, ces téléphones sont chiffrés par un mot de passe à 4 caractères représentant 10 000 possibilités. Le téléphone est protégé par un mécanisme de retard (*après chaque essai d'un mot de passe un délai plus ou moins long est activé entre deux tentatives*) qui rendrait la possibilité de tester tous les mots de passe trop longue (*plusieurs années*). Le téléphone embarquait également une technologie permettant la mise en place d'un nouveau mécanisme de sécurité qui rend possible l'effacement totale de la mémoire (*wipe*) après 10 tentatives d'un mauvais mot de passe. Le FBI avait alors intenté une procédure judiciaire très médiatisée pour contraindre Apple à créer une *« backdoor »* dans son système, ce qu'Apple refusa de faire. Le FBI, alors incapable techniquement d'extraire les données, avait fait appel à des tierces personnes qui ont réussi, après quelques semaines, à trouver une faille de sécurité matérielle publiée par le Dr Sergei Skorobogatov de l'université de Cambridge. Cette découverte mettra fin à la procédure judiciaire.

Les criminels ont également profité de dispositifs grand public en orientant leurs communications via des messageries instantanées chiffrées de bout en bout, comme Telegram, Signal et WhatsApp. Les récents attentats en France ont, une fois de plus, montré la nécessité pour les forces de l'ordre de développer des techniques pour accéder à ces données cruciales. Les écoutes en direct par les forces de l'ordre sont alors devenues difficilement opérantes, les amenant à développer des techniques logicielles et matérielles pour récupérer physiquement les données dans les mémoires des téléphones. Des sociétés privées se sont alors lancées dans la

préparation de téléphones « inviolables » ; c'est la naissance des « darkphones », instruments de communication privilégiés du grand banditisme. Les revendeurs appliquent des politiques de sécurité qui désactivent physiquement la caméra (*dessoudage de la caméra sur la carte mère*), rendent inopérants l'utilisation de la voix (*retrait du micro*), des applications de localisation et l'échange de données via la connectivité USB (utilisée uniquement pour recharger le téléphone). Les téléphones sont modifiés pour ne permettre que l'échange des mails chiffrés et ne sont pas modifiables par les membres du réseau. Ils sont vendus sur le darknet et payés en cryptomonnaies ou en espèces. Comme dans le cas d'EncroChat, les téléphones sont livrés avec deux systèmes d'exploitation distincts. Lorsque le téléphone est démarré, un Android normal s'affiche sans, généralement, aucune donnée utilisateur. Une combinaison de touches spécifiques permet à l'utilisateur de passer en mode sécurisé et de démarrer le système d'exploitation EncroChat développé par la société préparant le téléphone. Par conséquent, les enquêteurs primo-intervenants peuvent manquer des informations cruciales en pensant que le téléphone est neuf ou non utilisé. Les données s'échangent uniquement via un serveur central, localisé en France dans le cadre d'EncroChat, mais hors du territoire national la plupart du temps (*limitant les capacités d'investigation physique sur le serveur*). Le téléphone crée donc un canal chiffré pour envoyer ou recevoir des e-mails chiffrés via ce serveur dédié. De plus, un effacement à distance de l'appareil est nativement intégré, permettant à la tête du réseau d'effacer toutes les données en cas d'arrestation d'un des membres.

D'un point de vue du Code de procédure pénale, la nuance entre déverrouillage et chiffrement est importante et rappelée par un arrêt rendu le 13 octobre 2020 par la Chambre criminelle de la Cour de cassation. Ainsi, l'article 434-15-2 du Code pénal va dans le sens des enquêteurs qui peuvent maintenant s'appuyer sur une base légale consolidée pour leurs investigations.

Les réseaux criminels n'utilisent donc pas les systèmes d'exploitation normaux, car ils sont potentiellement reconfigurables par les utilisateurs, à la différence des « darkphones » qui sont distribués par la tête du réseau et dont les paramètres ne sont pas modifiables. Pour contrer ces mesures de dissimulation criminelle, les forces de l'ordre ont dû développer des techniques de pointe pour faire face et s'unir. En 2015, grâce à une forte coopération policière internationale, la gendarmerie royale canadienne a démantelé le réseau de « darkphones » BlackBerry PGP, suivie par la police néerlandaise qui a fait tomber successivement Ennetcom en 2016 et PGP safe en 2018. Le FBI a, quant à lui, démantelé le réseau Phantom Secure en 2018. Notons enfin que le réseau EncroChat a été neutralisé en 2020 par la gendarmerie française, en collaboration avec la police néerlandaise et sous l'égide d'Eurojust, mettant un coup d'arrêt à plusieurs milliers de criminels dans le monde.

Ainsi, le renforcement de la coopération internationale du point de vue technique permet à la gendarmerie française et à ses partenaires internationaux de développer et de rechercher des failles de sécurité logicielles et matérielles, d'acquérir du matériel

de pointe pour lire les données à très bas niveaux et de contourner les mécanismes de sécurité utilisés à des fins criminelles. Malheureusement, même si les réseaux EncroChat, Phantom secure, PGP safe, Ennetcom ont été démantelés, d'autres émergent déjà, en utilisant des technologies différentes (Omerta, SkyECC). Le jeu du chat et de la souris perdure encore et toujours ; les réseaux criminels s'efforcent d'utiliser des technologies permettant l'échange sécurisé dans leur réseau, les forces de l'ordre tentant d'anticiper les difficultés techniques d'accès aux données en développant leurs propres outils afin de mettre fin aux agissements criminels.

Général d'armée (2S) Marc WATIN-AUGOUARD

Le versement d'une rançon, lors d'un ransomware, sanctionné aux Etats-Unis. Avertissement de l'OFAC sur les risques potentiels de sanctions relatives au paiement des rançons associées à un rançongiciel

Le 1er octobre 2020, l'*Office of Foreign Assets Control* (OFAC), relevant du Département américain du Trésor, a publié un avertissement mettant en garde les entreprises qui paieraient une rançon pour libérer leurs données frauduleusement chiffrées par un ransomware. L'Office souligne combien les cyberattaques de cette nature ont augmenté au cours de la pandémie Covid-19, visant notamment les sites les plus utiles à l'activité économique. Les paiements de rançon, selon l'OFAC, menacent les intérêts de sécurité nationale et les objectifs de politique étrangère des États-

Unis. Selon le FBI, le nombre d'attaques par rançongiciel a augmenté de 37 % entre 2018 et 2019, tandis que les pertes financières ont connu une progression de 147 %.
Ne sont pas visées par l'avertissement les entreprises victimes, mais celles qui facilitent le paiement pour le compte des victimes, en particulier les institutions financières, les assurances garantissant le risque cyber, les prestataires de cybersécurité. Il peut leur être reproché d'encourager les auteurs et de violer les réglementations de l'OFAC, sans avoir la garantie de retrouver les données.
L'*International Emergency Economic Powers Act* (IEEPA), du 28 octobre 1977, qui autorise le Président à réglementer le commerce en cas de menace, et le *Trading with the Ennemy Act* , du 6 octobre 1917, offrent les bases légales de ces mesures. Le paiement d'une rançon à des personnes physiques ou morales relevant de pays désignés (Cuba, la région de Crimée Ukraine, Iran, Corée du Nord et Syrie) constitue le comportement fautif, de même que les transactions des personnes non américaines qui conduiraient un Américain à transgresser l'IEEPA.

Quant aux Américains, ils ne doivent pas faciliter une transaction au profit d'un non-Américain. Une personne soumise à la juridiction américaine peut être sanctionnée, même si elle ne savait pas qu'elle se livrait à une transaction interdite.
L'avertissement décrit les risques de sanctions et fournit des informations pour contacter les agences gouvernementales américaines compétentes, y compris l'OFAC.
L'OFAC encourage les institutions financières et autres entreprises à mettre en place un programme de conformité fondé sur les

risques pour atténuer l'exposition aux sanctions. Il annonce atténuer ses sanctions en fonction de l'attitude à l'égard des forces de l'ordre, dès lors que la victime a dénoncé les faits et coopéré avec elles. Les victimes doivent également contacter l'*Office of Cybersecurity and Critical Infrastructure Protection* (OCCIP) du Département américain du Trésor si une attaque implique un financier américain ou peut obérer considérablement la capacité d'une entreprise.

Cette mesure prise de manière unilatérale par les États-Unis pourrait avoir des conséquences pour les acteurs européens, en raison de ses conséquences transfrontalières. Mais il faut souligner que la question est également posée sur le Vieux Continent, car il est établi que le paiement d'une rançon accentue le sentiment d'impunité du rançonneur et l'incite à *« augmenter ses tarifs »*, de ransomware en ransomware. Il faut bien, à un moment donné, casser la spirale infernale. C'est plus la méthode qui est une fois de plus à déplorer. La même attitude a conduit Donald Trump à promulguer le *Cloud Act*, texte aux conséquences transfrontalières par nature, sans la moindre concertation. Depuis le 25 septembre 2019, une négociation transatlantique est en cours, alors que l'Europe travaille sur un règlement e-evidence. L'arrivée de l'administration Biden sonnera-t-elle l'heure du dialogue ?

Actualité pénale

Claudia GHICA-LEMARCHAND

REFUS DE SE SOUMETTRE À UN PRÉLÈVEMENT BIOLOGIQUE ET AU RELEVÉ D'EMPREINTES DIGITALES

Crim. 28 octobre 2020, n° 19-85812, publ. Bull. à venir

Une femme est interpellée lors d'une manifestation dite « des Gilets jaunes ». Une cinquantaine de personnes ont jeté des projectiles sur les policiers et procédé à diverses dégradations sur un poste de police (*« caméras de surveillance arrachées, graffitis sur les murs, projectiles lancés sur les vitres, banderoles embrasées avec un début d'incendie, destruction de la guérite d'entrée, visiophone endommagé, utilisation d'un fumigène »*). Placée en garde à vue, elle refuse de se soumettre au prélèvement biologique destiné à recueillir son empreinte génétique, ainsi qu'au relevé de ses empreintes digitales. Le tribunal correctionnel la déclare coupable des faits visés à la prévention et la condamne à quatre mois d'emprisonnement pour les faits de dégradations aggravées et de refus de se soumettre aux relevés signalétiques, ainsi qu'à deux mois d'emprisonnement pour le refus de se soumettre au prélèvement biologique. La Cour d'appel confirme la décision et la prévenue forme un pourvoi en cassation. Elle soutient plusieurs arguments critiquant la régularité de la garde à vue, qui sont écartés par la Cour de cassation, en vertu de sa jurisprudence déjà bien établie sur cette question, mais elle soulève aussi certains arguments relatifs au refus de prélèvement biologique et d'empreintes. Même s'ils ne reçoivent pas un écho favorable de la

part de la Cour de cassation, il est intéressant de les reprendre. Seul le régime juridique des prélèvements biologiques sera développé, les règles applicables aux relevés d'empreintes digitales étant similaires, mais plus classiques et ne soulevant pas les mêmes problématiques du point de vue du respect de la dignité et de l'inviolabilité du corps. Le régime juridique des prélèvements biologiques est défini par le Code de procédure pénale, autant dans sa partie législative (articles 706-54 s.) que réglementaire (article R 53-9).

L'article 706-54 du Code de procédure pénale met en place le fichier national automatisé des empreintes génétiques (FNAEG) qui est destiné à centraliser les empreintes génétiques relatives à certaines infractions mentionnées à l'article 706-55. La liste établie par cet article est longue et comprend aussi bien des infractions contre les personnes (les crimes contre l'humanité et les crimes et délits d'atteintes volontaires à la vie de la personne, de torture et actes de barbarie, de violences volontaires, de menaces d'atteintes aux personnes, de trafic de stupéfiants, d'atteintes aux libertés de la personne, de traite des êtres humains, de proxénétisme, d'exploitation de la mendicité et de mise en péril des mineurs) que les infractions contre les biens (les crimes et délits de vols, d'extorsions, d'escroqueries, de destructions, de dégradations, de détériorations et de menaces d'atteintes aux biens) ou les infractions contre la Nation, l'État ou la paix publique (les atteintes aux intérêts fondamentaux de la Nation, les actes de terrorisme, la fausse monnaie, l'association de malfaiteurs et les crimes et délits de guerre), ainsi que les infractions relatives aux armes (le trafic, la fabrication et le commerce, les importations, exportations,

transferts, etc.). Mais la liste ne serait pas complète sans parler de son début et de sa fin.

Au tout début de la liste figurent les infractions qui ont justifié la création du FNAEG, à savoir les infractions sexuelles qui cristallisent la volonté du législateur qui a imaginé ce moyen spécial pour les combattre et qui l'a ensuite étendu à d'autres infractions. Si la rédaction de l'article 706-55 renvoie expressément à l'article 706-47, il est possible de remarquer que sont concernées toutes les agressions sexuelles, y compris le viol, les atteintes sexuelles, ainsi que les propositions sexuelles faites à des mineurs par voie électronique ou les messages pornographiques à destination des mineurs.

La fin de l'article 706-55 est tout aussi intéressante, car elle permet de comprendre la méthode du législateur, puisque l'alinéa 6° permet de centraliser les empreintes génétiques des personnes ayant commis des infractions de recel ou de blanchiment du produit de l'une des infractions mentionnées. Cela signifie que le droit pénal combat avec la même ardeur les auteurs des infractions principales que les auteurs des infractions de conséquence qui entretiennent et inspirent les premières.

Si la liste des infractions visées par le FNAEG est très large, le prélèvement concerne, bien évidemment, une personne et l'article retient une définition tout aussi large et englobante.

Les prélèvements biologiques visent les personnes impliquées dans une infraction visée sur la liste légale, qu'elles soient identifiées ou non. Si leur implication peut être diverse, elle détermine un régime juridique différent. D'une part, le FNAEG est automatiquement nourri par les empreintes génétiques identifiées de personnes

déclarées coupables ou pénalement irresponsables en raison d'un trouble mental total pour l'une des infractions précédemment mentionnées. Dans cette dernière hypothèse, leur implication matérielle dans la commission de l'infraction est prouvée, mais leur responsabilité pénale ne peut être retenue en raison d'une absence d'imputabilité causée par une abolition de leur discernement ou de leur volonté. Dans cette même logique, l'article 706-56-1 permet d'inscrire au FNAEG les empreintes génétiques des personnes de nationalité française, ou de nationalité étrangère résidant de façon habituelle sur le territoire national, et qui ont été condamnées par une juridiction pénale étrangère pour une infraction de même nature lorsque ces condamnations, en application d'une convention ou d'un accord international, ont fait l'objet d'un avis aux autorités françaises ou ont été exécutées en France à la suite du transfèrement des personnes condamnées. Cette inscription ne se fait pas automatiquement mais sur demande du procureur de la République.

En revanche, lorsqu'il n'y a pas de décision judiciaire, même si la personne est identifiée, la procédure s'entoure de conditions supplémentaires. Le FNAEG peut être alimenté par les empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une de ces infractions, mais uniquement sur décision d'un officier de police judiciaire agissant, soit d'office, soit à la demande du procureur de la République ou du juge d'instruction. Il peut être intéressant de mentionner que cette même procédure permet de procéder au rapprochement de l'empreinte avec les données incluses au fichier, sans toutefois que cette empreinte puisse y être conservée. D'autre part, une procédure distincte d'enregistrement

permet d'ajouter les empreintes génétiques recueillies à l'occasion des procédures de recherche des causes de la mort ou des causes d'une disparition ou des recherches aux fins d'identification de personnes décédées dont l'identité n'a pu être établie, selon l'article 16-11 du Code civil, à l'exception des militaires décédés à l'occasion d'une opération conduite par les forces armées ou les formations rattachées.

Le FNAEG a été considéré comme un outil criminalistique probatoire important concentrant les efforts du législateur afin de le rendre indispensable. Mais les prélèvements biologiques peuvent constituer une atteinte à l'intégrité du corps humain, garantie par l'article 16 du Code civil, selon lequel *« la loi assure la primauté de la personne, interdit toute atteinte à la dignité de celle-ci et garantit le respect de l'être humain dès le commencement de sa vie »*, raison pour laquelle ils ne peuvent être imposés de force. Afin d'en garantir, cependant, l'effectivité, le législateur a accompagné la création du FNAEG d'un délit de refus de prélèvement génétique.

L'article 706-56 prévoit que l'officier de police judiciaire (OPJ) peut procéder ou faire précéder sous son contrôle à des prélèvements biologiques permettant l'analyse de l'empreinte génétique à l'égard des personnes identifiées qui sont condamnées ou contre lesquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées dans le cadre de ces articles. Cependant, l'OPJ est soumis au principe de respect de l'intégrité du corps humain et ne peut imposer un prélèvement biologique, tout au plus peut-il réaliser l'identification d'une empreinte génétique à partir de

matériel biologique *« qui se serait naturellement détaché du corps de l'intéressé »*. Afin de renforcer l'impérativité de cette analyse, le refus de prélèvement constitue un délit puni d'un an d'emprisonnement et de 15 000 euros d'amende. Lorsque la personne a été condamnée pour crime, se fondant sur une certitude de culpabilité dans le cadre des infractions les plus graves, la peine est doublée et portée à deux ans d'emprisonnement et 30 000 euros d'amende. La loi punit le refus, ainsi que la fraude, dans le cadre de l'identification génétique. Ainsi, le fait, pour une personne faisant l'objet d'un prélèvement, de commettre ou de tenter de commettre des manoeuvres destinées à substituer à son propre matériel biologique le matériel biologique d'une tierce personne, avec ou sans son accord, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

Le législateur crée donc trois délits différents avec un *crescendo* de répression afin de pousser la personne à accepter le prélèvement biologique. Le régime juridique de l'application de la peine s'inscrit aussi dans le même sens répressif. En premier lieu, les peines prononcées pour les délits prévus au présent article se cumulent, sans possibilité de confusion, avec celles que la personne subissait ou celles prononcées pour l'infraction ayant fait l'objet de la procédure à l'occasion de laquelle les prélèvements devaient être effectués. Ensuite, lorsque les infractions prévues par le présent article sont commises par une personne condamnée, elles entraînent de plein droit le retrait de toutes les réductions de peine dont cette personne a pu bénéficier et interdisent l'octroi de nouvelles réductions de peine.

Cependant, la loi du 5 mars 2007 relative à la prévention de la délinquance a modifié la philosophie de la loi en autorisant des

prélèvements sans l'autorisation de l'intéressé, sur réquisitions écrites du procureur de la République, uniquement lorsqu'il s'agit d'une personne condamnée ou déclarée irresponsable pour cause de trouble mental total pour un crime ou un délit puni de dix ans d'emprisonnement. Il est possible de constater que l'autorité judiciaire contrôle le prélèvement en la personne du représentant du ministère public (sans entrer ici dans le débat récurrent de savoir si le Parquet fait partie de l'autorité judiciaire au sens de l'article 5 de la Convention européenne des droits de l'Homme) et que la mesure contraignante vise exclusivement les infractions les plus graves constituées par les qualifications criminelles ou délictuelles lorsqu'elles font encourir la peine maximale sur l'échelle des peines correctionnelles.

Si les règles de centralisation des empreintes génétiques sont relativement stables depuis 2011, en revanche, le droit pénal français a dû modifier substantiellement les règles d'effacement et de contrôle de l'enregistrement des données.
La durée de conservation des données est déterminée à la partie réglementaire du Code de procédure pénale à laquelle renvoie la partie législative. L'article R 53-14 fixe spécialement la durée maximale de conservation. Cette dernière ne saurait dépasser quarante ans lorsqu'il s'agit d'empreintes génétiques de personnes condamnées ou déclarées pénalement irresponsables pour cause de trouble mental ou de traces biologiques prélevées dans le cadre de recherches en vue de l'identification d'une personne. En revanche, les échantillons biologiques prélevés dans le cadre d'une enquête préliminaire, d'une enquête pour crime ou délit flagrant, ou d'une instruction préparatoire sur les personnes à l'encontre

desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions visées, ne peuvent être gardés pour une durée supérieure à vingt-cinq ans. Ce dispositif appelle deux remarques.

D'une part, le Conseil constitutionnel a validé le procédé du renvoi législatif au texte réglementaire pour fixer le délai de conservation des données génétiques, car *« dès lors, il appartient au pouvoir réglementaire de proportionner la durée de conservation de ces données personnelles, compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées »* (décision du Conseil constitutionnel 2010-25, QPC 16 septembre 2010).

D'autre part, la Cour européenne des droits de l'Homme, dans son arrêt du 22 juin 2017, *Aycaguer c/ France*, s'est prononcée sur le FNAEG. La Cour affirme qu'elle a pleinement conscience que pour remplir *« leur devoir de protection des populations »*, les autorités nationales créent des fichiers qui contribuent efficacement à la répression et à la prévention de certains infractions, notamment les infractions sexuelles pour lesquelles le FNAEG a été créé. L'enregistrement de profil ADN, donnée relative à la vie privée d'un individu, constitue une ingérence au sens de l'article 8. M. Aycaguer a été arrêté pour participation à une manifestation et dégradation volontaire, mais a refusé de se soumettre aux prélèvements biologiques. Si l'ingérence est considérée comme prévue par la loi et *« poursuivant un but légitime »*, la Cour remarque que l'article R 53-14 prévoit une durée maximale de conservation pour ces infractions qui présenteraient toutes *« un certain degré de gravité »*. Or, cette période maximale aurait dû être aménagée par décret. Le décret n'ayant pas été adopté, le délai de quarante ans s'applique, alors qu'il s'agit plutôt d'une norme que d'un maximum.

La Cour européenne renvoie spécifiquement à la décision du Conseil constitutionnel de 2016 exigeant que le décret proportionne la durée de conservation des données personnelles à la nature ou à la gravité des infractions concernées. Elle remarque que l'état du droit français est lacunaire de ce point de vue, ne permettant pas de distinguer certaines infractions, comme celles commises par M. Aycaguer (des coups de parapluie en direction de gendarmes qui n'ont pas été identifiés, donc sans résultat tangible ou incapacité totale de travail), d'infractions particulièrement graves à l'instar des infractions sexuelles, du terrorisme, etc. La Cour européenne constate aussi que la procédure d'effacement n'existe que pour les personnes soupçonnées d'infraction, mais pas pour celles qui ont été condamnées, qui devraient aussi pouvoir en bénéficier. Compte tenu des règles insuffisantes de conservation et d'effacement des empreintes génétiques au FNAEG, les juges européens considèrent que la condamnation d'une personne pour refus de se soumettre à un prélèvement biologique constitue *« une atteinte disproportionnée au droit à la vie privée et ne peut passer pour nécessaire dans une société démocratique »*.

Afin de parer aux dernières critiques européennes, la loi du 23 mars 2019 (loi n° 2019-222 de programmation et de réforme de la justice) a créé un nouvel article – l'article 706-54-1 qui prévoit les règles d'effacement des données. Pour les personnes condamnées, la décision d'effacement est prise sur instruction du procureur de la République agissant sur demande de l'intéressé. Pour les personnes à l'encontre desquelles il existe des indices graves ou concordants, l'effacement des données est effectué sur instruction du procureur agissant, cette fois-ci, soit d'office, soit sur demande de l'intéressé.

Dans un cas comme dans l'autre, l'effacement des données est décidé lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier.

Dans l'arrêt du 28 octobre 2020, la cour d'appel avait condamné la manifestante pour refus de se soumettre à un prélèvement biologique. Le pourvoi conteste la condamnation en utilisant trois arguments. D'une part, l'obligation de se soumettre à un prélèvement biologique en vue de permettre l'inscription au FNAEG constitue une atteinte disproportionnée au droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (CSDHLF), en permettant la conservation des données pendant une durée fixe de 25 ou 40 ans, *« sans distinguer selon la gravité des faits ou des infractions en cause »* (il est aisé de reconnaître l'inspiration tirée de l'arrêt *Aycaguer*). D'autre part, le prélèvement biologique ne peut être demandé que lorsqu'il y a des indices graves ou concordants rendant vraisemblable que la personne ait commis l'une des infractions limitativement énumérées au Code de procédure pénale. La personne avait été relaxée dans le cadre de la prévention de destruction de bien public en réunion, cependant, les indices graves et concordants de commission de cette infraction avaient permis de la condamner pour refus de prélèvement. Enfin, en tant que suite logique de l'argument précédent, s'il n'y a pas de preuve de l'infraction cadre de l'enregistrement au FNAEG, il ne saurait y avoir de délit de refus de prélèvement.

La Cour de cassation rejette les différentes critiques formulées. Le

raisonnement de la Cour de cassation apparaît clairement dès le rappel des règles applicables. L'article 706-54 autorise l'inscription au FNAEG des empreintes génétiques d'une personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable qu'elle ait commis l'une des infractions limitativement énumérées. Le refus de se soumettre au prélèvement constitue une infraction en elle-même. Si la personne n'est pas condamnée pour l'infraction pour laquelle elle est poursuivie, cela n'a pas d'importance, car la loi autorise l'enregistrement de données relatives à la personne soupçonnée et pas uniquement à la personne condamnée pour la commission de l'infraction. Le refus de prélèvement est une infraction autonome et pas une infraction de conséquence qui repose sur l'existence d'une infraction précédente. Elle sanctionne un comportement distinct qui lui assure une autonomie de qualification pénale et de régime juridique. C'est la raison pour laquelle la personne bénéficie de garanties indépendantes dans la mesure où elle peut demander l'effacement de ses données et, en cas de refus, dispose d'un recours juridictionnel effectif.

L'enseignement que tire la Cour de cassation de cette situation juridique est intéressant, car les indices graves et concordants de commission d'une infraction déclenchent une double conséquence procédurale. En premier lieu, la personne peut être placée en garde à vue. En second lieu, pendant la garde à vue, elle est tenue de se soumettre au prélèvement biologique. Le refus constitue le délit prévu par l'article 706-56 du Code de procédure pénale. Le délit est consommé au moment du refus et ne peut être modifié par le cours ultérieur de la procédure. La décision de relaxe, tout comme celle de condamnation, n'a pas d'effet sur l'obligation de se soumettre

au prélèvement. Si la personne est condamnée, cela ne fait pas naître de nouvelles obligations à son égard. Parallèlement, si elle est relaxée, cela n'efface pas le délit de refus de se soumettre au prélèvement précédemment commis. Ce dernier a été entièrement consommé et la modification postérieure de la situation juridique n'efface ni la qualification pénale, ni la responsabilité pénale qui en découle. Le Code de procédure pénale autorise le prélèvement à l'égard des personnes soupçonnées, pas seulement à l'égard des personnes condamnées. Or, la relaxe ultérieure ne fait pas disparaître les *« indices graves et concordants »* qui ont justifié le prélèvement dans un cadre procédural distinct. La décision du Conseil constitutionnel du 16 septembre 2016 contenait déjà cette appréciation lorsque les juges affirmaient *« l'obligation pénalement sanctionnée de se soumettre au prélèvement, qui n'implique pas davantage de reconnaissance de culpabilité, n'est pas contraire à la règle selon laquelle nul n'est tenu de s'accuser ; que, dès lors, ces dispositions ne portent pas atteinte à la présomption d'innocence »*, montrant que l'on se plaçait nécessairement avant la décision de condamnation. En tirant toutes les conséquences utiles de ce raisonnement, la Chambre criminelle considère ainsi que, ni le prélèvement, ni le délit de refus de prélèvement ne constituent des ingérences excessives dans le droit à la vie privée et familiale, reconnu à l'article 8 CSDHLF.

Afin d'appuyer et conforter la décision de la Cour de cassation, il peut être utile de rappeler que le Conseil constitutionnel aboutit à cette même conclusion dans sa décision du 16 septembre 2010 en affirmant que le dispositif mis en œuvre dans le Code de procédure pénale permet d'assurer *« entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas*

manifestement déséquilibrée ».

Il convient d'apporter deux précisions supplémentaires sur le FNAEG, même si elles ne ressortent pas de l'arrêt évoqué.
D'une part, le prélèvement biologique en vue de l'enregistrement des données génétiques dans un fichier a été critiqué comme un traitement inhumain ou dégradant portant atteinte à l'intégrité du corps humain ou à la dignité. La décision du Conseil constitutionnel a écarté ces critiques, considérant que manquent *« les griefs tirés de l'atteinte à l'inviolabilité du corps humain, au principe du respect de la dignité de la personne humaine et à la liberté individuelle »*.
D'autre part, ces mesures techniquement nouvelles sont censées s'appliquer à des cadres divers. Une difficulté d'application de ces mesures dans le temps surgit pour les personnes condamnées. L'enregistrement des données peut-il concerner les personnes ayant commis des infractions avant la création du FNAEG ? La Cour de cassation a admis l'application rétroactive de l'enregistrement des données génétiques pour les auteurs d'infractions commises avant son entrée en vigueur et est allée encore plus loin en l'admettant aussi pour les personnes ayant subi des condamnations antérieures. Cette solution s'appuie sur la nature intrinsèque de l'enregistrement des données génétiques dans un fichier qui constitue une mesure de sûreté, puisqu'elle se fonde sur l'état de dangerosité de la personne qui y est soumise. Si l'application semble rétroactive du point de vue de l'infraction commise ou de la condamnation prononcée, elle est en réalité immédiate car elle se fonde sur l'état dangereux concomitant au jugement et à la décision d'inscription dans le FNAEG. Les mesures de sûreté connaissent un régime dérogatoire d'application dans le temps qui

s'exprime avec force dans le cadre des prélèvements biologiques et des inscriptions dans le cadre de fichiers automatisés de données.
L'effet d'impérativité de la loi pénale est ici maximal, car cela aboutit à une application immédiate du délit de refus de prélèvement biologique. Même lorsque les faits commis ou condamnés ont été antérieurs à la création du FNAEG et donc du délit de refus de prélèvement, ce dernier s'y applique. L'article 706-56 du Code de procédure pénale punit le refus de prélèvement et nullement les faits commis antérieurement, qui ne font que déterminer le champ d'application de l'obligation violée. Dans ce cas, le délit saisit immédiatement le refus sans égard pour les faits qui ont servi de fondement à la condamnation pour l'infraction commise. L'autonomie de l'infraction est pleinement affirmée par cette analyse et va dans le même sens que la règle rappelée par l'arrêt du 28 octobre 2020.

VIOL

Crim. 14 octobre 2020, n° 20-83273, inédit

Une jeune femme de dix-neuf ans a dénoncé l'ex-compagnon de sa mère qui, depuis ses treize ans, a pris l'habitude de lui imposer de se déshabiller, lui caressant le vagin et les fesses, se frottant contre elle et lui léchant le sexe, sous prétexte de prétendues punitions destinées à la corriger. Le juge d'instruction a notamment requalifié les faits de viol commis par une personne ayant autorité sur la victime en faits d'agression sexuelle incestueuse par personne ayant autorité sur la victime et renvoyé le mis en examen devant le tribunal correctionnel. La chambre de l'instruction a confirmé

l'ordonnance. Les juges estiment que la pénétration doit avoir été *« d'une profondeur significative »* pour constituer un viol, ce qui ne semble pas être le cas en l'espèce puisque la victime indique que l'auteur l'a *« pénétrée avec sa langue à force d'insister »*, mais que cette déclaration n'était *« assortie d'aucune précision en termes d'intensité, de profondeur, de durée ou encore de mouvement »*, de sorte qu'elle *« ne caractérisait pas suffisamment une introduction volontaire au-delà de l'orée du vagin, suffisamment profonde pour caractériser un acte délibéré »*.

La victime forme un pourvoi en cassation critiquant les juges d'instruction d'avoir ajouté à la loi une condition qu'elle ne comportait pas, puisque l'article 222-23 ne comporte pas de condition quant à la profondeur ou l'intensité de la pénétration pour caractériser le viol. La Cour de cassation rejette le pourvoi en se retranchant derrière l'appréciation souveraine des juges du fond, mais elle rappelle les exigences tenant à l'élément matériel de pénétration.

Les agressions sexuelles sont définies par le Code pénal comme des atteintes sexuelles commises avec violence, contrainte, menace ou surprise (article 222-22). Si toutes les agressions sexuelles ont en commun l'absence de consentement de la victime qui est matérialisé par l'emploi d'un des moyens limitativement énuméré par la définition légale, le viol s'en détache, étant caractérisé par une « pénétration sexuelle ». La Cour de cassation a largement défini cet élément comme étant une pénétration dans le sexe ou par le sexe. Si la loi du 3 août 2018 a élargi le champ d'application du viol, pouvant s'appliquer aussi bien à la personne de la victime qu'à celle de l'auteur, l'exigence de pénétration sexuelle est restée stable.

Actualité pénale

Dans l'arrêt du 14 octobre 2020, la Chambre criminelle constate que la victime n'a fait l'objet d'aucun examen gynécologique, qu'elle a affirmé au cours de l'enquête qu'elle était vierge et a déclaré aux enquêteurs que son agresseur *« avait peur d'aller trop loin avec ses doigts »* et qu'il ne l'a pas pénétrée, sauf pour l'unique pénétration dénoncée, *« j'ai senti qu'il m'a pénétrée avec sa langue à force d'insister »*. La Cour vérifie que *« cette déclaration [qui] n'a été assortie d'aucune précision en termes d'intensité, de profondeur, de durée ou encore de mouvement, ne caractérise pas suffisamment une introduction volontaire au delà de l'orée du vagin, suffisamment profonde pour caractériser un acte de pénétration »*. La requalification des faits en agression sexuelle est confirmée en se fondant sur l'absence d'éléments matériel et moral du viol. La Chambre criminelle assure une interprétation stricte de l'élément matériel du viol qui consiste en une « pénétration sexuelle », en mettant l'accent sur la valeur de l'adjectif et ne considérant plus exclusivement le substantif auquel il s'attache.

Même si la décision n'a pas les honneurs d'une publication au Bulletin des arrêts de la Chambre criminelle, elle a été largement médiatisée et soumise au tribunal de l'opinion publique. Elle est intéressante à plusieurs égards.

En premier lieu, elle confirme l'interprétation objective de la définition du viol qui est privilégiée par le Cour de cassation depuis plus d'une décennie. L'élément matériel l'emporte sur l'élément moral et la seule volonté de pénétration sexuelle ne permet pas de qualifier le viol en l'absence de la consommation de la pénétration.

Ensuite, l'article 222-23 exige une pénétration sexuelle, définie par la jurisprudence comme une pénétration dans le sexe ou par le sexe. Ainsi, la pénétration avec des objets dans le sexe ou la

pénétration buccale ou annale avec l'organe sexuel peuvent recevoir la qualification de viol. Mais lorsqu'il y a doute ou absence de pénétration par le sexe ou dans le sexe, comme en l'espèce (la langue n'avait pas pénétré le vagin de la victime), l'élément matériel du viol fait défaut car il n'y a ni pénétration dans le sexe (dans le vagin), ni par un organe sexuel (la langue). Il peut être regretté que l'attendu de la Cour de cassation soit trop explicite et s'attarde sur les caractères de la pénétration exigés par les juges d'instruction, « en termes d'intensité, de profondeur, de durée ou encore de mouvement », laissant l'impression d'ajouter cette condition au texte d'incrimination. Il aurait mieux valu que la Cour de cassation ne descende pas dans le détail d'appréciation des faits et s'en tienne à l'interprétation générale de l'article 222-23 rappelant l'exigence de la « pénétration sexuelle ». Mais cela permet de comprendre la raison de cette analyse juridique.

Enfin, la requalification des faits en agression sexuelle assure un traitement juridique efficace à cette affaire. La charge de la preuve pèse sur l'accusation et le ministère public, au premier titre, ainsi que la partie civile, ensuite, auraient dû apporter la preuve de la pénétration. Les éléments factuels semblaient démontrer l'impossibilité de cette preuve, la victime étant vierge alors qu'il fallait prouver une pénétration vaginale. Plutôt que de prendre le risque d'un procès retentissant débouchant sur un acquittement, les juges préfèrent retenir une qualification moindre d'agression sexuelle, mais avec des preuves solides permettant d'obtenir une déclaration de culpabilité. Médiatiquement moins bruyant, mais juridiquement plus efficace !

Actualité pénale

PRESCRIPTION

Crim. 13 octobre 2020, n° 19-87787, publ. à venir Bull.

Une personne est poursuivie pour avoir commis en récidive plusieurs infractions relatives au travail dissimulé commises en 2012. Alors que le dernier acte d'enquête date du 14 novembre 2014, il est jugé par défaut et condamné par le tribunal correctionnel le 19 décembre 2015. Il forme opposition de cette décision et, à la suite de son admission, le tribunal correctionnel se prononce de nouveau sur sa culpabilité. La personne forme un pourvoi en cassation et sa critique se concentre sur la prescription de l'action publique, plus particulièrement sur l'articulation des différentes règles relatives à la prescription dans le temps.

La loi du 27 février 2017 relative à la prescription en matière pénale a profondément réformé les règles applicables en la matière qui souffraient d'un manque évident de cohérence et de légitimité. En matière correctionnelle, la loi a unifié les délais de prescription de l'action publique et de la peine en les portant à six ans, avec une limite à ne pas excéder fixée à douze ans. Elle a aussi consacré le report du point de départ de la prescription au moment de la découverte des faits dans des conditions permettant l'exercice de l'action publique pour les infractions occultes ou dissimulées. Afin de réguler l'application de ces nouvelles règles, la loi du 27 février 2017 a prévu dans son article 4 que *« la présente loi ne peut avoir pour effet de prescrire des infractions qui, au moment de son entrée en vigueur, avaient valablement donné lieu à la mise en mouvement*

ou à l'exercice de l'action publique à une date à laquelle, en vertu des dispositions législatives alors applicables et conformément à leur interprétation jurisprudentielle, la prescription n'était pas acquise ».
Les travaux parlementaires, ainsi que la rédaction retenue, manifestent la volonté du législateur de ne pas permettre à la nouvelle loi d'offrir un régime juridique plus favorable aux prescriptions d'infractions faisant l'objet d'une procédure en cours. Antérieurement, la loi prévoyait un ensemble de règles dérogatoires allongeant les délais de prescription. Dans le même sens répressif, la jurisprudence utilisait la théorie des infractions clandestines afin de reporter le point de départ à la découverte d'infractions, pourtant instantanées. La loi du 27 février 2017 a expressément formulé une règle transitoire spéciale dans son article 4 afin de maintenir l'action publique dans les cas dans lesquels elle avait été engagée.
En même temps, l'article 112-2 4° formule une règle générale d'application immédiate des lois de prescription dans le temps. L'article a été modifié par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité. Si avant, seules les lois plus favorables à la personne poursuivie étaient applicables immédiatement, les lois plus sévères étant soumises à la règle de non-rétroactivité, la loi de 2004 unifie le régime des lois de prescription de l'action publique et de la peine, sans tenir compte de leur caractère plus ou moins doux pour la personne poursuivie. Ainsi, les lois de prescription rejoignent pleinement le régime juridique des lois de forme, étant soumises, par principe, à l'application immédiate. Cependant, la loi maintient, bien évidemment, une limite, qui est celle des prescriptions acquises. En

effet, la nouvelle loi de prescription ne peut ressusciter une situation juridique éteinte. Si la prescription est acquise, la nouvelle loi ne peut plus produire d'effet.

La règle transitoire spéciale de la loi de 2017 et le régime général de l'article 112-2 4° doivent être mis en cohérence et il est important de déterminer la règle devant prévaloir. En l'espèce, l'application de la règle transitoire énoncée par la loi de 2017 conduisait le pourvoi à considérer que l'action publique était prescrite, dans la mesure où l'opposition au jugement correctionnel de 2015 avait été acceptée et que la juridiction s'était prononcée une nouvelle fois. Ainsi, la règle applicable à l'époque conduisait à appliquer une durée de prescription de trois ans, de sorte que les faits se trouvaient prescrits lors de la nouvelle décision. La prescription acquise ne permettait plus d'engager les poursuites.

La Cour de cassation rejette la critique formulée par le pourvoi et en profite pour rappeler certains principes généraux du droit pénal.

En cas de conflit entre une règle spéciale et une règle générale, le juge devrait faire prévaloir la règle spéciale sur la règle générale, en vertu de la maxime *specialia generalibus derogant*. Néanmoins, cette maxime ne vaut que si les règles ont le même champ d'application et répondent aux mêmes impératifs de qualification. Or, la Cour de cassation ne considère pas que le régime transitoire édicté par la loi de 2017 se substitue aux règles d'application des lois de prescription dans le temps formulées à l'article 112-2 4°. La règle spéciale de la loi de 2017 énonce une exception au régime

général du Code pénal. *« Il résulte des travaux parlementaires que l'article 4 de la loi du 27 février 2017 a eu pour seule finalité, selon l'intention du législateur, de prévenir la prescription de certaines infractions occultes ou dissimulées par l'effet de la loi nouvelle, laquelle prévoit notamment que le délai de prescription de ces infractions, quand il s'agit de délits, ne peut excéder douze années révolues à compter du jour où l'infraction a été commise, alors que selon la jurisprudence constante de la Cour de cassation, ces infractions ne se prescrivaient qu'à partir du moment où le délit est apparu et a pu être constaté dans des conditions permettant l'exercice de l'action publique. »*

La Cour de cassation applique la méthode d'interprétation téléologique qui lui permet de rechercher l'intention du législateur, la *ratio legis*, afin d'éclaircir le domaine ou les conditions d'application des règles édictées par la loi. Il ne lui reste plus qu'à compléter l'édifice juridique, ce qu'elle fait par la mobilisation d'un autre principe général du droit – *odiosa sunt restrigenda* – conduisant à une application restrictive des exceptions. *« Dès lors, ce texte doit être interprété restrictivement et ne saurait avoir pour effet de déroger de façon générale aux dispositions de l'article 112-2, 4°, du code pénal, selon lesquelles les lois relatives à la prescription de l'action publique sont applicables immédiatement à la répression des infractions commises avant leur entrée en vigueur, lorsque les prescriptions ne sont pas acquises »*. La Cour de cassation rejette le pourvoi, car la nouvelle loi de 2017 s'applique immédiatement, dès lors que ses conditions ne sont pas remplies, donc lorsque la prescription n'est pas acquise. Le délai de prescription de six ans doit s'appliquer à l'espèce en l'absence d'acquisition de la

prescription au moment du jugement.

Si la solution de la Cour de cassation peut paraître classique, la rigueur du raisonnement et l'enchaînement impeccable des principes généraux du droit dans une matière qui a longtemps été instable et polémique, comme celle de la prescription, donnent une valeur particulière à cet arrêt.

Police administrative

Élisabeth Rolin

Injonction du juge des référés « libertés » à l'administration pénitentiaire de mettre fin à des carences structurelles caractérisant un traitement inhumain et dégradant[1]

Conseil d'État, 10ème-9ème chambres réunies, 19 octobre 2020, n° 439372[2]

Cet arrêt s'inscrit à la suite de la jurisprudence Hardouin et Marie du 17 février 1995[3] **qui a consacré le recul de la notion de mesures d'ordre intérieur. Il est novateur en ce qu'il admet que le juge des référés « libertés » puisse enjoindre à l'administration pénitentiaire de remédier à des atteintes structurelles aux droits fondamentaux des prisonniers. Il reconnaît également la possibilité pour ce juge de prononcer d'office une astreinte pour l'exécution des mesures qu'il a ordonnées. Enfin, il précise les limitations de son office, c'est-à-dire son champ de compétence.**

La Section française de l'Observatoire international des prisons (SFOIT) a demandé au juge des référés « libertés » du tribunal

1. Au sens de l'article 3 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH).
2. Conditions de détention indignes, le Conseil d'État répond à la Cour européenne des droits de l'Homme, publié au recueil Lebon, *AJDA*, n° 35, 26 octobre 2020, p. 1991.
3. CE, Assemblée, 17 février 1995, Marie ; CE, Assemblée, 17 février 1995, Marie, *GAJA*, n° 88, p. 637- 646.

administratif (TA) de Nouméa, statuant sur le fondement de l'article L. 521-2 du Code de justice administrative (CJA), d'ordonner aux autorités pénitentiaires et judiciaires de prendre toutes les mesures utiles afin de faire cesser les atteintes graves et manifestement illégales portées aux libertés fondamentales des personnes détenues au centre pénitentiaire de Nouméa. S'écartant de la jurisprudence du Conseil d'État qui considérait que le juge des référés « libertés » ne peut prescrire *« des mesures d'ordre structurel reposant sur des choix de politique publique »*[4], le tribunal administratif de Nouméa a fait droit partiellement à la requête[5]. Il a ainsi enjoint à l'administration pénitentiaire, non seulement de faire cesser les différents manquements à l'hygiène dans les quartiers du centre de détention pour hommes, notamment dans les cellules « containers maritimes », mais aussi de prendre des mesures, même transitoires, d'aménagements pour préserver l'intimité dans les cellules ou remédier dans les meilleurs délais à l'insalubrité des points d'eau et sanitaires du quartier des mineurs. Enfin, le juge a enjoint à l'administration de prendre dans les plus brefs délais les mesures nécessaires au recrutement et à la rémunération d'un

4. CE, 28 juillet 2017, Section française de l'observatoire international des prisons, n° 410677, p. 285.

5. Par une ordonnance n° 2000048 du 19 février 2020, le TA de Nouméa a aussi enjoint à l'administration pénitentiaire de faire en sorte que les détenus qui n'ont accès ni à un lave-linge, ni à un service de buanderie, puissent laver leur linge en leur fournissant le matériel nécessaire à cet effet ou en s'assurant qu'ils en sont dotés ; de s'assurer de la mise aux normes des installations électriques et de procéder de manière diligente au remplacement des ventilateurs cassés ou défectueux, compte tenu des températures élevées supportées par les détenus, en apportant, le cas échéant, par des mesures transitoires dans l'attente de solutions pérennes, une solution aux remontées d'égout.

médecin addictologue au centre pénitentiaire de Nouméa.

C'est cette dernière mesure qui a conduit le garde des Sceaux, ministre de la Justice, à demander au Conseil d'État d'annuler cette ordonnance mais aussi de rejeter la requête de la SFOIT devant le juge des référés du TA de Nouméa dans l'ensemble de ses prétentions.

Le Conseil d'État a rejeté le recours du ministre et a enjoint à l'administration pénitentiaire de procéder, dans les plus brefs délais, à l'installation d'abris dans les cours de promenades du centre pénitentiaire qui en sont dépourvues, d'assurer la séparation des annexes sanitaires dans l'ensemble des cellules où est détenue plus d'une personne, de prendre toute mesure susceptible d'améliorer la luminosité des cellules et de procéder au remplacement des fenêtres défectueuses. Il a aussi invité l'administration à produire dans un délai de dix jours tous les éléments d'informations utiles aux questions posées sur les cours de promenade du quartier disciplinaire et d'isolement et sur les cours de promenade du quartier fermé du centre de détention et du quartier des mineurs. Il a rejeté le surplus des conclusions de la SFOIT, reformé en conséquence l'ordonnance du juge des référés du TA de Nouméa, tout en mettant à la charge de l'État la somme de 3 000 euros au titre des frais irrépétibles sur le fondement de l'article L. 761-1 du CJA au bénéfice de la SFOIT.

Cet arrêt conduit le Conseil d'État à préciser les pouvoirs que le juge des référés « libertés » tient de l'article L. 521-2 du CJA mais

aussi les limitations de son champ d'intervention.

Les pouvoirs du juge du juge des référés « libertés »

Le juge des référés, saisi sur le fondement de l'article L. 521-2 du CJA, doit constater une atteinte grave et manifestement illégale portée par une personne morale de droit public à une liberté fondamentale pour prendre les mesures qui sont de nature à faire disparaître les effets de cette atteinte. Ces mesures doivent en principe présenter un caractère provisoire, sauf lorsqu'aucune mesure de cette nature n'est susceptible de sauvegarder l'exercice effectif de la liberté fondamentale à laquelle il est porté atteinte.
Le juge des référés « libertés » peut ainsi ordonner à l'autorité compétente de prendre, à titre provisoire, une mesure d'organisation des services placés sous son autorité lorsqu'une telle mesure est nécessaire à la sauvegarde d'une liberté fondamentale. Toutefois, il ne peut, au titre de cette procédure particulière, qu'ordonner les mesures d'urgence qui lui apparaissent de nature à sauvegarder, dans un délai de quarante-huit heures, la liberté fondamentale à laquelle il est porté une atteinte grave et manifestement illégale. Eu égard à son office, il peut également, le cas échéant, décider de déterminer, dans une décision ultérieure prise à brève échéance, les mesures complémentaires qui s'imposent et qui peuvent également être très rapidement mises en œuvre. Dans tous les cas, son intervention est subordonnée au constat que la situation litigieuse permet de prendre utilement et à très bref délai les mesures de sauvegarde nécessaires. Compte tenu du cadre temporel dans

lequel il se prononce, les mesures qu'il peut ordonner doivent s'apprécier en tenant compte des moyens dont dispose l'autorité administrative compétente et des mesures qu'elle a déjà prises.

En conséquence, c'est après avoir constaté que les conditions générales de détention dans ce centre pénitentiaire, notamment l'absence de luminosité dans les cellules ou d'abris dans certaines cours de promenade permettant de se protéger du soleil et des intempéries, sont de nature à caractériser une violation de l'article 3 de la CEDH et que l'implantation de tels équipements est susceptible d'être mise en œuvre à très bref délai que le juge des référés « libertés » peut enjoindre à l'administration d'y remédier. En revanche, dès lors qu'il ne dispose pas de toutes les informations, le même juge invite l'administration dans un délai court, en l'espèce dix jours, à fournir tous les éléments utiles complémentaires. En conséquence, il décide de surseoir à statuer sur les conclusions relatives à la fermeture des cours de promenade situées dans des conteneurs et à l'installation de toilettes dans l'ensemble des cours de promenade jusqu'à ce qu'une nouvelle décision du juge des référés du Conseil d'État intervienne.

Enfin, cet arrêt précise, dans un considérant de principe, que s'il n'appartient pas au juge des référés de prononcer, de son propre mouvement, des mesures destinées à assurer l'exécution de celles qu'il a déjà ordonnées, il peut, d'office, en vertu de l'article L. 911-3 du CJA, assortir les injonctions qu'il prescrit d'une astreinte. Par suite, il incombe dans tous les cas aux différentes autorités administratives de prendre, dans les domaines de leurs

compétences respectives, les mesures qu'implique le respect des décisions juridictionnelles. L'exécution d'une ordonnance prise par le juge des référés peut être ainsi recherchée dans les conditions définies par le livre IX du même Code. La personne intéressée peut également demander au juge des référés d'assurer l'exécution des mesures ordonnées demeurées sans effet, par de nouvelles injonctions et une astreinte.

En résumé, en reconnaissant que le juge des référés « libertés » peut être saisi d'une demande d'exécution et prononcer d'office une astreinte, le Conseil d'État affirme le caractère effectif de cette procédure d'urgence. Mais il souligne également les limitations de son office.

Les limitations de l'office du juge des référés « libertés »

La SFOIT soutenait que le juge de Nouméa n'avait pas complètement rempli son office en ne tirant pas toutes les conséquences de l'arrêt de la Cour européenne des droits de l'Homme (CEDH) du 30 janvier 2020, *J.M.B. et autres contre France* (9671/15), qui avait relevé l'absence de voie de recours préventive pour mettre fin aux conditions indignes de détention résultant de carences structurelles.
Le Conseil d'État répond à ce moyen en considérant qu'il résulte des dispositions de l'article 46 de la CEDH que la complète exécution d'un arrêt de la Cour européenne des droits de l'Homme condamnant un État partie à la convention implique, en principe, que cet État prenne toutes les mesures qu'appellent, d'une part, la

réparation des conséquences que la violation de la convention a entraînées pour le requérant et, d'autre part, la disparition de la source de cette violation. Eu égard à la nature essentiellement déclaratoire des arrêts de la Cour, il appartient à l'État condamné de déterminer les moyens de s'acquitter de l'obligation qui lui incombe ainsi. Par suite, le Conseil d'État relève que c'est au législateur qu'il appartient d'en tirer les conséquences et non au juge des référés « libertés », tout en soulignant qu'en parallèle de la procédure prévue à l'article L. 521-2 du CJA qui permet d'ores et déjà de remédier aux atteintes les plus graves aux libertés fondamentales des personnes détenues, le juge de l'excès de pouvoir peut, lorsqu'il est saisi à cet effet, enjoindre à l'administration pénitentiaire de remédier à des atteintes structurelles aux droits fondamentaux des prisonniers en lui fixant, le cas échéant, des obligations de moyens ou de résultats.

Xavier Latour

Un nouvel outil au service du *continuum* entre l'État et les communes

Lors d'un déplacement à Toulouse, le 9 octobre 2020, le Premier ministre Jean Castex a annoncé la signature du premier contrat de sécurité intégrée.
L'objectif affiché est de consolider les relations entre les polices municipales et les forces nationales de sécurité intérieure pour mieux lutter contre la délinquance quotidienne. Si Toulouse est la première ville, d'autres suivront, tandis qu'une approche métropolitaine est également programmée. La loi sur la sécurité globale devrait donner à l'ensemble un fondement législatif.

Cette évolution s'inscrit dans une continuité quant à la méthode, tout en tentant d'innover.

La continuité

La volonté de l'État de se coordonner avec les polices municipales n'est pas nouvelle, au contraire. Elle s'inscrit dans la logique bien connue de la coproduction de sécurité.

L'État a expérimenté plusieurs formules tant institutionnelles (les conseils locaux de sécurité et de prévention de la délinquance) que pseudo-contractuelles.
Dans les années 1990, la mode était aux contrats locaux de sécurité

(CLS) élaborés par le préfet, le procureur et le maire, sans implication assez marquée des policiers ou des gendarmes qui le regrettaient. Ils ont d'abord reposé sur une circulaire du 28 octobre 1997, puis ont reçu une consécration législative (loi du 15 novembre 2001 relative à la sécurité quotidienne). L'idée est alors de faire travailler ensemble tous ceux qui concourent à la sécurité locale, y compris dans un cadre intercommunal.

Faux contrats, car dépourvus de portée contraignante, les CLS se sont progressivement épuisés durant la première décennie des années 2000, comme avant eux les plans locaux de sécurité. Les engagements étaient réciproques, mais leur force juridique restait surtout indirecte. Cela explique sans doute leur affaiblissement inexorable. Une autre explication tenait à la piètre qualité des diagnostics préalables à leur élaboration. L'expertise tant publique que privée faisait défaut. En outre, le périmètre des intervenants impliqués était vraisemblablement trop large.

En 2006, le ministère de l'Intérieur a tenté de les relancer. L'idée était alors de mieux les préparer et mieux en mesurer les effets. De la sorte, l'État confirmait sa volonté de développer des méthodes incitatives, tout en affirmant son autorité, sa prééminence, en particulier à travers les préfets. Ils sont les véritables animateurs de la relation entre l'État et les communes. Le procureur a, quant à lui, la charge des enjeux judiciaires.

Les résultats n'ayant pas toujours été aussi bons qu'espérés, les CLS ont alors laissé la place aux stratégies territoriales de sécurité.

L'évolution sémantique gomme la dimension paracontractuelle, sans changer cependant l'esprit.

Après des années d'atermoiements, l'État revient à la logique initiale, celle du contrat. Il affirme sa volonté de lier les moyens locaux et nationaux pour faire face à la délinquance. L'approche partenariale ne se limite pas aux polices municipales et aux forces étatiques, elle traduit une vision toujours plus large qui embrasse, par exemple, les associations, l'Éducation nationale, voire les citoyens, selon le Premier ministre. Cette transversalité reflète les deux versants de la lutte contre la délinquance, préventif et répressif.

Si les éléments de continuité existent, les nouveaux contrats paraissent s'inscrire davantage dans une logique d'engagements réciproques, plus marqués qu'auparavant.

L'innovation

Chaque partie apporte à l'autre des éléments très concrets. Le stade de la coordination est dépassé, au profit d'une complémentarité plus marquée.
L'État s'engage ainsi à renforcer les effectifs des forces étatiques de sécurité. L'augmentation des recrutements sur le quinquennat lui donne cette marge de manœuvre. Dans le prolongement de sa visite à Nice, l'été dernier, le gouvernement a, par ailleurs, renouvelé son intention de conférer de nouveaux pouvoirs aux policiers municipaux.

Mais il ne le fera pas sans contrepartie. Les communes doivent assumer leur part de responsabilité en renforçant leur police

municipale et les moyens de vidéoprotection. L'utilité de cette dernière s'en trouve confirmée malgré des incertitudes en la matière. La portée réelle de cet outil reste sujette à débats malgré l'engouement pour les nouvelles technologies. Elles font entrer les caméras dans une dimension inconnue à leurs débuts, dans les années 1990. La reconnaissance faciale et l'intelligence artificielle en accroissent les potentialités.
Néanmoins, les demandes du Premier ministre ne s'arrêtent pas là. Elles vont jusqu'à l'aide que les communes apporteraient aux services de l'État en *« matière de logement, d'action sociale ou d'accueil des familles »*.

L'innovation devrait aussi atteindre les conseils locaux de sécurité et de prévention de la délinquance en fonction des résultats des réflexions de l'Assemblée nationale qui en étudie le fonctionnement.

Il est, enfin, significatif que le Premier ministre ait clairement affiché sa volonté d'inscrire les contrats dans une dimension métropolitaine.
Ce n'est pas une surprise. Déjà, des parlementaires avaient plaidé pour la création de polices territoriales. Déjà encore, l'intercommunalité devait impacter le fonctionnement des polices municipales.
Mais, jusque-là, les maires rechignaient à abandonner ou à affaiblir leurs prérogatives. Dès lors, l'incitation ne suffisant pas, le gouvernement semble enclin à se faire plus pressant. Selon un constat bien connu, les territoires traditionnels ne permettraient

plus de traiter une délinquance mobile. Les bassins, voire les couloirs de délinquance, ont rendu un peu obsolètes les approches strictement communales.
Dans le même temps, le Premier ministre n'exclut pas de relancer les travaux sur une redéfinition des zones de police et de gendarmerie. Ce sujet très sensible initié à la fin des années 1990 reste, par voie de conséquence, d'actualité.

Toutes ces réflexions s'inscrivent dans le contexte plus général de l'évolution des polices municipales qui ont fait l'objet d'un rapport de la Cour des comptes.

La vision de la Cour des comptes sur les polices municipales

Le sujet est largement traité dans un rapport public thématique de 220 pages, publié en octobre 2020.

Il en ressort que la croissance de ces polices se poursuit, même si elle a ralenti. Sans compter les gardes champêtres et les agents de surveillance de la voie publique (ASVP), les polices municipales totalisent 23 944 agents. Pour autant, la répartition sur le territoire demeure très hétérogène. Les zones d'implantation historique restent les plus actives (sud de la France par exemple). D'autres territoires sont moins denses, mais les villes à l'écart du mouvement sont de moins en moins nombreuses (Issy-les-Moulineaux par exemple).
L'hétérogénéité existe aussi en matière de conditions d'emploi. Le

constat était déjà connu. Selon les choix des maires, les polices municipales sont plus ou moins interventionnistes, certaines au point de se rapprocher des forces nationales de sécurité intérieure.

Le rapport confirme, par ailleurs, la faible percée des polices intercommunales pour des raisons bien connues. Les maires demeurent réticents, tandis que les conditions de création restent peut-être trop contraignantes. La Cour plaide donc en faveur d'un assouplissement, en particulier en supprimant les seuils.

Du côté des moyens, 81 % des policiers sont armés, dont 57 % d'armes à feu. Ces chiffres ne cessent d'augmenter, ce qui prouve que le caractère facultatif de l'armement n'est pas forcément un obstacle.
De plus, la vidéoprotection poursuit son développement, en dépit d'un manque de données sur certains aspects de son efficacité. Les progrès de la technologie la favorisent. D'ailleurs, la Cour pointe l'inadéquation du cadre légal et réglementaire et appelle à une évolution indispensable afin de garantir les droits fondamentaux.
Dans un autre registre, l'accroissement des compétences, sans doute inachevé, incite à s'interroger sur l'accès direct des policiers municipaux à certains fichiers, en particulier à celui des objets et véhicules signalés.

Dans le domaine de la gouvernance, la Cour dresse un constat assez sévère.
D'une part, elle regrette les conditions de fonctionnement de la Commission consultative nationale. Non seulement elle se réunit

peu, mais passe une grande partie de son temps à traiter de questions statutaires. Sur l'insuffisance d'une réflexion stratégique, le rapport n'occulte pas la responsabilité de l'État qui n'a pas encore réellement tranché la question du « champ d'intervention » des polices municipales et celle de la doctrine d'emploi.

D'autre part, le rapport plaide en faveur d'une amélioration de la formation (initiale et continue), de l'élaboration de véritables dispositifs d'évaluation et d'un meilleur contrôle externe.

Directeur de publication :	**Colonel Dominique SCHOENHER**
Rédacteur en chef :	**G^{al} d'armée (2S) Marc WATIN-AUGOUARD**
Rédacteurs :	**G^{al} d'armée (2S) Marc WATIN-AUGOUARD** **Claudia GHICA-LEMARCHAND** **Xavier LATOUR** **Elisabeth ROLIN** **CNE Matthieu AUDIBERT** **CNE Thibaut HECKMANN** **LTN Océane GERRIET**
Équipe éditoriale :	**Odile NETZER**