LA VEILLE JURIDIQUE

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

RUBRIQUE

DROIT DE L'ESPACE NUMÉRIQUE

ANNÉE 2020

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

PAR LE CAPITAINE THIBAUT HECKMANN

PAR LE CAPITAINE MATTHIEU AUDIBERT

PAR LE LIEUTENANT OCÉANE GERRIET

CREOGN
CENTRE DE RECHERCHE

TABLE DES MATIÈRES

Janvier

Jurisprudence constitutionnelle

Décision n° 2019-796 DC du 27 décembre 2019 (à propos de l'expérimentation de la collecte et de l'exploitation, par les administrations fiscale et douanière, des données rendues publiques sur les réseaux sociaux et les sites des opérateurs de plateforme) 10

I. Un texte attentatoire aux libertés qui répond à un objectif constitutionnel

II. Les conditions de l'équilibre sont garanties par le texte

III. Une inconstitutionnalité partielle

Cour de justice de l'Union européenne

Conclusions de l'avocat général dans l'affaire C-311/18. Data Protection Commissioner/Facebook Ireland et Maximillian Schrem 17

Le mot de passe d'un smartphone peut-il être considéré comme une « convention secrète de déchiffrement » ?..... 23

Le non-respect du Réglement général sur la protection des données (RGPD) à nouveau sanctionné : une sanstion d'un demi-million d'euros prononcée par la CNIL à l'encontre d'une société française..... 26

Février

Jurisprudence judiciaire

Cour de cassation, Chambre criminelle (n° 1884.755), arrêt n° 2790

du 7 janvier 2020, Procureur général près la Cour d'appel de Poitiers et autres 32
Cour d'appel, Aix-en-Provence, 4e et 6e chambres réunies (n° 16/12997), arrêt du 24 janvier 2020 34
Tribunal judiciaire de Paris, ordonnance de référé du 8 janvier 2020, **C**artier International et autres / Bouygues Telecom et autres 36
Regard sur l'actualité : La « vengeance pornographique » 41

Mars

Discours d'ouverture du FIC 2020, prononcé par le Général d'armée (2S) Marc Watin-Augouard, directeur du CREOGN (2012-2020) 46
Un nouveau souffle numérique pour l'Union européenne 50
1. L'appui de la transformation numérique sur des valeurs communes
2. Une cybersécurité au service de la transformation numérique
3. Une souveraineté technologique européenne
4. Une transformation numérique respectueuse du Pacte vert

Avril

Jurisprudence judiciaire
Recel de fichiers faisant l'apologie du terrorisme 60
Les certitudes
Le doute de la Cour de cassation
Jurisprudence administrative
Le droit à l'oubli sur le web 64
Les principes posés par le Conseil d'État
L'application aux données dites sensibles
L'application du droit au déréférencement par le juge judicaire
Le tribunal administratif de Marseille a tranché : il n'y aura pas de reconnaissance faciale dans les lycées 74

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

Une technologie engendrant des questionnements...
… et une première réponse juridique !

Mai

Tracing but not Tracking (article publié par *La Tribune* le 12 mai 2020) 82
Jurisprudence constitutionnelle
Décision n° 2020800 DC du 11 mai 2020 relative à la loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions 86
Jurisprudence administrative
Conseil d'État, Ordonnance du 18 mai 2020, Quadrature du Net, Ligue des Droits de l'Homme 90
Le Conseil d'État déclare conformes des recommandations relatives à l'usage des réseaux sociaux visant à assurer le respect de l'obligation de réserve 97
Sur la légalité et la portée de la Charte
Sur la légalité de la recommandation relative à l'usage des réseaux sociaux

Juin

Jurisprudence constitutionnelle
Décision n° 2020801 DC du 18 juin 2020 relative à la loi visant à lutter contre les contenus haineux sur Internet 106
La genèse
Les modifications prévues par la loi Avia
La sage décision des Sages
Que reste-t-il de la loi Avia ?
Décision n° 2020845 QPC du 19 juin 2020 relative au recel d'apologie du terrorisme 114
La genèse
La décision du Conseil constitutionnel

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

Actualité numérique
L'opérateur des systèmes d'information interministériels classifiés (OSIIC)..... 120
StopCovid..... 121
5e rapport d'activité de l'autorité qualifiée de la CNIL, 2 février 31 -décembre 2019..... 126

Septembre

CJUE (grande chambre), 16 juillet 2020 (affaire C-311/18), Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems..... 130
Du *Safe Harbor* au *Privacy Shield*
L'invalidation du *Privacy Shield*
L'action des services de renseignement américains mise en cause par la *High Court*
La décision CJUE
Jurisprudence administrative
Conseil d'État (10ème et 9ème chambres réunies), arrêt n° 430810 du 19 juin 2020, Google LLC/ CNIL..... 139
La saisine du Conseil d'État
Les motifs évoqués par Google
La décision du Conseil d'État
Actualité numérique
L'Union européenne inflige ses premières sanctions à la suite de cyberattaques..... 143
Les textes mis en application
Les décisions du 30 juillet 2020
Encrochat, une enquête exemplaire..... 151
Les décisions de justice accessibles librement en ligne..... 154
Le « dossier pénal numérique »..... 155
Bref rappel sur le contrôle des accès au lieu de travail..... 157

Octobre

Jurisprudence européenne 164
I) L'applicabilité de la « directive communications électroniques »
II) Fin de la conservation généralisée des données
III) Un tempérament pour la sécurité nationale
IV) Un tempérament pour la lutte contre la criminalité grave
V) Effet immédiat et rétroactif
Jurisprudence judiciaire
Code de déverrouillage d'un téléphone portable 172
Géolocalisation – Information du magistrat 184
Compte Facebook, atteinte à la vie privée du salarié/Information confidentielle de l'entreprise 185
Jurisprudence administrative
Plateforme des données de santé 187

Novembre

La CJUE : un premier pas vers la consécration du principe de neutralité du Net 194
Cour de justice de l'Union européenne – Grande chambre – Affaires C551/18 et C552/18 – Arrêt du 6 octobre 2020 – Quadrature du Net, French Data Network et autres / Premier ministre, garde des Sceaux, ministre de la Justice et autres 202
La conservation des données de connexion. Le droit français et la Cour de justice de l'Union européenne. Quelles conséquences pour les enquêtes judiciaires ? 203
La conservation des données de communication aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique
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
La conservation rapide des données de connexion et de localisation

aux fins de lutte contre la « criminalité grave »
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
Le juge national et l'arrêt de la CJUE
Après avoir présenté les grandes lignes de cet arrêt, quelles en sont les conséquences pour les enquêtes judiciaires ?

Jurisprudence judiciaire

Tribunal judiciaire de Meaux – 1ère chambre – Ordonnance sur incident du 2 novembre 2020 – M.X /Google LLC..... 218

Jurisprudence administrative

Conseil d'État – 10ème et 9ème chambres réunies – Arrêt du 4 novembre 2020 – La Quadrature du Net/ État..... 219
« Alicem », la protection du consentement « by design »
Le rejet de la requête par le Conseil d'État

Actualité numérique

Téléphones sécurisés, « darkphones » : quand le chiffrement devient la norme..... 224

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..... 229

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

JANVIER 2020

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

Par le G^al^ d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE CONSTITUTIONNELLE

Décision n° 2019-796 DC du 27 décembre 2019

Sont conformes à la Constitution, à l'exception des dispositions qui s'appliquent à une infraction déjà établie, la collecte et l'exploitation au moyen de traitements informatisés, par les services fiscaux et douaniers, des contenus « librement accessibles », autorisées par l'article 154 de la loi de finances pour 2020.

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

significatif dans le cadre des prérogatives confiées à ces administrations dans le cadre de leurs missions », comme le souligne la Commission nationale de l'informatique et des libertés (CNIL), saisie pour avis[1], qui considère que ce type de traitement est d'un « genre nouveau » par rapport aux cas qu'elle a eu à traiter auparavant.

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

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

sur un réseau social.
Le Conseil constitutionnel a partiellement censuré cet article mais en a validé l'essentiel en vérifiant les conditions garantissant un équilibre entre l'atteinte aux libertés et l'objectif constitutionnel de lutte contre les fraudes fiscales et douanières les plus graves.

I. Un texte attentatoire aux libertés qui répond à un objectif constitutionnel

L'examen des dispositions du texte met en évidence leur caractère attentatoire à la vie privée, dès lors qu'il s'agit de « collecter de façon indifférenciée d'importants volumes de données, relatives à un grand nombre de personnes, publiées sur des services de communication au public en ligne et, d'autre part, d'exploiter ces données, en les agrégeant et en opérant des recoupements et des corrélations entre elles ».
L'atteinte à la vie privée est effective, même s'il s'agit de données rendues publiques par les personnes qu'elles concernent. L'atteinte à l'exercice de la liberté d'expression et de communication est également constituée, les mesures envisagées étant « susceptibles de dissuader d'utiliser de tels services ou de conduire à en limiter l'utilisation ». Eu égard au développement généralisé des services de communication au public en ligne, la liberté d'accès est une des manifestations de la libre communication des pensées et des opinions garantie par l'article 11 de la Déclaration de 1789.
Les Sages rappellent que la lutte contre la fraude et l'évasion fiscales est un objectif de valeur constitutionnelle[2] qui doit toutefois

2. Décision n° 99-424 DC du 29 décembre 1999, cons. 52 ; décision n° 2001-457 DC du 27 décembre 2001, cons. 6.

être concilié avec le droit au respect de la vie privée.

II. Les conditions de l'équilibre sont garanties par le texte

L'objectif de lutte contre la fraude et l'évasion fiscales doit être mis en balance avec la liberté d'expression et de communication qui permet de parler, d'écrire et d'imprimer, conditionne la démocratie et est l'une des garanties du respect des autres droits et libertés. Conformément à sa jurisprudence, les atteintes portées à cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi.

Des données librement accessibles et manifestement rendues publiques

Pour que cet équilibre soit respecté, le Conseil constitutionnel relève que les recueils de données doivent répondre à deux conditions cumulatives. Les contenus doivent être librement accessibles et manifestement rendus publics par les utilisateurs des sites. La collecte ne peut concerner des sites dont l'accès est restreint par la saisie d'un mot de passe ou l'inscription sur le site en cause. Elle ne peut porter que sur les données mises en ligne par la personne concernée et exclut les données dites « sensibles »[3] énoncées à l'article 9 du RGPD (art. 6 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

3. La prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne, les données génétiques et biométriques et celles concernant la santé et la vie ou l'orientation sexuelles.

Un traitement par des agents spécialement habilités

Les traitements doivent être mis en œuvre par des agents des administrations fiscale et douanière ayant au moins le grade de contrôleur, spécialement habilités et tenus au secret professionnel[4]. Seule la conception des outils de traitement des données, à l'exclusion de leur collecte, de leur traitement et de leur conservation, peut être confiée à un sous-traitant de l'administration. Les agents spécialement habilités auront la responsabilité d'effectuer le tri des données et transmettront aux services compétents à des fins d'exploitation opérationnelle les données laissant suspecter la commission d'une des infractions limitativement prévues par l'article 154. À cet égard, il résulte des termes mêmes du sixième alinéa de l'article 154 de la loi de finances pour 2020, qui évoque la corroboration et l'enrichissement des données, que celles-ci ne pourront à elles seules justifier l'engagement d'une procédure pénale, fiscale ou douanière. Elles devront être confrontées à d'autres éléments d'information dont disposent ces services, issus d'enquêtes ou de contrôles effectués par d'autres moyens. Les données collectées dans le cadre de cet article 154 constituent ainsi des moyens de preuve supplémentaires justifiant l'engagement d'une procédure de contrôle.

Une conservation des données encadrée

La conservation des données est strictement encadrée. Celles manifestement sans lien avec les manquements et infractions recherchés ou qui constituent des données sensibles sont détruites

4. Articles 226-13 et 226-14 du Code pénal, article L. 103 du Livre des procédures fiscales et article 59 bis du Code des douanes.

au plus tard dans les cinq jours suivant leur collecte, sans aucune autre exploitation possible de ces données pendant ce délai. Les autres données doivent être détruites dans les trente jours si elles ne sont pas de nature à concourir à la constatation des manquements ou infractions. Seules peuvent être conservées les données strictement nécessaires à une telle constatation, dans la limite d'une année ou, le cas échéant, jusqu'au terme de la procédure pénale, fiscale ou douanière dans le cadre de laquelle elles sont utilisées, quand bien même ce terme surviendrait postérieurement à l'expiration de la durée d'expérimentation de trois ans.

L'exclusion de la reconnaissance faciale

La loi exclut la mise en œuvre de tout procédé de reconnaissance faciale à partir de photographies diffusées en ligne. Cette interdiction ne fait pas obstacle à l'exploitation de photographies révélant la commission d'une des infractions en cause par une personne nommément désignée ou identifiable par d'autres voies. Dans le cadre de l'expérimentation, l'administration fiscale envisage de n'exploiter les photographies qu'en tant qu'elles comportent du texte, en cas notamment de numérisation d'un document. L'administration des douanes exploitera, quant à elle, les images et les vidéos, à l'exclusion de tout traitement de reconnaissance faciale, notamment pour ce qui concerne les contrefaçons.

L'humain derrière le traitement algorithmique

Application de l'interdiction de prendre une décision sur le seul résultat d'un traitement algorithmique, aucune procédure pénale, fiscale ou douanière ne peut être engagée sans qu'ait été portée

une appréciation individuelle de la situation de la personne par l'administration, qui ne peut alors se fonder exclusivement sur les résultats du traitement automatisé. Pour le Conseil constitutionnel, il appartiendra au pouvoir réglementaire, sous le contrôle du juge, de veiller à ce que les algorithmes utilisés par ces traitements ne permettent de collecter, d'exploiter et de conserver que les données strictement nécessaires à ces finalités.

Partant de ces observations, les Sages considèrent que « le législateur a, compte tenu de l'ensemble de ces conditions, assorti le dispositif de garanties propres à assurer, entre le droit au respect de la vie privée et l'objectif de valeur constitutionnelle de lutte contre la fraude et l'évasion fiscales, une conciliation qui n'est pas déséquilibrée. Il en résulte également que l'atteinte à l'exercice de la liberté d'expression et de communication est nécessaire, adaptée et proportionnée aux objectifs poursuivis ». Le Conseil constitutionnel invite le législateur à apprécier, au terme du délai de trois ans, fixé par la loi, son efficacité dans la lutte contre la fraude et l'évasion fiscales, au regard des atteintes portées aux droits et libertés et du respect des conditions édictées. À la lumière de cette évaluation, la conformité à la Constitution de ce dispositif pourra de nouveau être examinée.

III. Une inconstitutionnalité partielle

Le Conseil constitutionnel, en revanche, déclare contraires à la Constitution les dispositions permettant la collecte et l'exploitation automatisées de données pour la recherche du manquement prévu au b du 1 de l'article 1728 du Code général des impôts, qui sanctionne d'une majoration de 40 % le défaut ou le retard de production d'une déclaration fiscale dans les trente jours suivant la

réception d'une mise en demeure. En effet, l'administration, qui a mis en demeure le contribuable de produire sa déclaration, a déjà connaissance d'une infraction à la loi fiscale, sans avoir besoin de recourir au dispositif automatisé de collecte de données personnelles. La mise en œuvre d'une telle mesure pour la simple recherche de ce manquement porte au droit au respect de la vie privée et à la liberté d'expression et de communication une atteinte qui n'est pas proportionnée au but poursuivi.

COUR DE JUSTICE DE L'UNION EUROPÉENNE

Conclusions de l'avocat général dans l'affaire C-311/18 Data Protection Commissioner / Facebook Ireland et Maximillian Schrem

Le 19 décembre 2019, la Cour de Justice de l'Union européenne a publié les conclusions de l'avocat général Saugmandsgaard Øe. Selon lui, la décision 2010/87/UE de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers est valide. Plusieurs médias ont alors titré « le transfert des données personnelles vers les États-Unis validé par la CJUE » ou « la CJUE donne raison aux GAFAM ». Si les conclusions de l'avocat général sont souvent suivies, il convient de les présenter comme une étape de la réflexion juridique et non comme une jurisprudence.

Au cœur du problème se trouve la question du transfert de données à caractère personnel vers des sous-traitants établis en dehors de l'Union. On admettra aisément que ces données doivent alors

bénéficier d'un traitement au moins égal à celui qui est imposé aux échanges entre États membres, au risque d'opérer à l'extérieur de l'Union des traitements illégaux en son sein. Dès 1995, la directive 95/46/CE[5] a imposé la reconnaissance par la Commission d'un niveau de protection adéquate des données à caractère personnel respecté par le pays d'importation. Le Règlement général sur la protection des données (RGPD)[6] a maintenu cette exigence (art. 44[7]), ainsi que les dérogations offertes en l'absence de décision d'adéquation. En l'absence d'une telle reconnaissance, le responsable du traitement peut procéder au transfert, par contrat entre l'exportateur et l'importateur, des données intégrant des clauses types de protection prévues par la décision 2010/87/UE[8]. Cette décision a institué des clauses contractuelles types (Art. 46 RGPD) pour le transfert de données à caractère personnel vers des sous-traitants

5. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

6. Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

7. « Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. »

8. Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil modifiée par la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016.

établis dans des pays tiers. Son article 1er dispose que les clauses contractuelles types figurant en annexe sont considérées comme offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.

Maximillian Schrems, étudiant autrichien, est déjà connu pour être à l'origine de la fin de la « Sphère de sécurité »[9]. Le 25 juin 2013, il saisit l'autorité irlandaise de protection des données (*Data Protection Commissioner* - DPC) d'une plainte concernant Facebook, réseau social auquel il est abonné. Il lui demande d'interdire à Facebook Ireland de transférer les données à caractère personnel le concernant vers les États-Unis. Il fait référence aux révélations faites par M. Edward Snowden, concernant « l'affaire PRISM » qui met en lumière les activités des services de renseignement des États-Unis. Le droit américain impose, selon lui, à Facebook Inc. de mettre les données à caractère personnel des utilisateurs à la disposition d'autorités américaines, telles que *la National Security Agency* (NSA) et le *Federal Bureau of Investigation* (FBI), dans le cadre de programmes de surveillance et entrave ainsi l'exercice des droits garantis aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union. Il en est ainsi de l'article 702[10] du *Foreign Intelligence*

9. La décision n° 2000/520/CE du 26 juillet 2000 de la Commission, constatant que les États-Unis respectent la « Sphère de sécurité – *Safe Harbor* », est annulée par l'arrêt CJUE C-362/14 *Maximillian Schrems/ Data Protection Commissionner* du 6 octobre 2015. Elle est désormais remplacée par la décision « Bouclier de protection - *Privacy Shield* ».

10. L'article 702 du FISA permet à l'*Attorney General* (procureur général, États-Unis) et au *Director of National Intelligence* (DNI) (directeur du renseignement national, États-Unis) d'autoriser conjointement, pour une durée d'un an, aux fins de se procurer des informations en matière de renseignement extérieur, la surveillance de personnes qui ne sont pas des citoyens américains et qui ne résident pas de manière permanente aux États-Unis (dites « personnes non américaines »).

Surveillance Act (FISA) (loi sur la surveillance en matière de renseignement extérieur) et de l'*Executive Order* 12333 (décret présidentiel n° 12333). Il considère que le droit et les pratiques en vigueur dans ce pays tiers ne garantissent pas une protection suffisante des données à caractère personnel conservées sur son territoire contre les intrusions découlant des activités de surveillance pratiquées par les autorités publiques. Les données des utilisateurs de Facebook résidant au sein de l'UE étant transférées depuis Facebook Ireland, filiale irlandaise de Facebook Inc., vers des serveurs situés sur le territoire des États-Unis, où elles font l'objet de traitements, le plaignant estime qu'elles ne font pas l'objet d'une protection suffisante.

Cette plainte est rejetée au motif que l'accord « Sphère de sécurité » offre des garanties suffisantes. Mais cet accord ayant été annulé, la *High Court* (Haute Cour, Irlande) annule la décision par laquelle l'autorité de contrôle a rejeté la plainte de M. Schrems et la renvoie devant cette autorité pour examen. Celle-ci relance la procédure en tenant compte de l'invalidation de la décision « Sphère de sécurité ». Maximillian Schrems demande à Facebook Ireland d'identifier les fondements juridiques sur lesquels reposent les transferts des données à caractère personnel des utilisateurs de Facebook depuis l'Union vers les États-Unis. Dans sa réponse, Facebook Ireland fait référence à un accord de transfert et de traitement de données (*data transfer processing agreement*) conclu entre elle-même et Facebook Inc., applicable depuis le 20 novembre 2015, et invoque la décision 2010/87. M. Schrems conteste cet accord : d'une part, les clauses contenues dans cet accord ne sont pas conformes aux clauses contractuelles types prévues par la décision 2010/87 et, d'autre part, ces clauses contractuelles types ne pourraient pas, en tout état de cause, fonder le transfert des données à caractère personnel le concernant vers les États-Unis. M. Schrems ajoute

qu'aucune voie de recours ne permet aux personnes concernées de faire valoir aux États-Unis leurs droits au respect de la vie privée et à la protection des données à caractère personnel.

L'autorité de contrôle estime alors que le traitement de la plainte dépend de la validité de la décision 2010/87. Elle engage une nouvelle procédure devant la *High Court* pour que celle-ci, par renvoi préjudiciel, saisisse la CJUE.

Dans ses conclusions, l'avocat général propose à la CJUE de répondre que l'analyse de la décision 2010/87 n'a pas révélé d'éléments de nature à entacher sa validité. L'ensemble de son analyse est guidé, dit-il, par la recherche d'un équilibre entre, d'une part, la nécessité de faire preuve d'un « degré de pragmatisme raisonnable afin de permettre une interaction avec le reste du monde » et, d'autre part, celle d'affirmer les valeurs fondamentales reconnues dans les ordres juridiques de l'Union et de ses États membres, en particulier par la Charte. Pour lui, le droit de l'Union s'applique aux transferts de données à caractère personnel vers un pays tiers lorsque ces transferts obéissent à des finalités commerciales, même si les données transférées sont susceptibles de subir de la part des autorités publiques de ce pays tiers des traitements à des fins de sécurité nationale. La conformité de la décision 2010/87 à la Charte dépend du point de savoir s'il existe des mécanismes suffisamment solides permettant d'assurer que les transferts fondés sur les clauses contractuelles types soient suspendus ou interdits en cas de violation de ces clauses ou de l'impossibilité de les honorer. Selon l'avocat, tel est le cas dans la mesure où il existe une obligation – pesant sur les responsables du traitement et, en cas d'inaction de ces derniers, sur les autorités de contrôle – de suspendre ou d'interdire un transfert lorsque, en raison d'un conflit entre les obligations découlant des clauses types et celles imposées par le droit du pays tiers de destination, ces

clauses ne peuvent pas être respectées.
Ainsi, l'avocat général place Facebook Irland et le DPC devant leurs responsabilités. La question de la validité de la décision « bouclier de protection des données » n'ayant pas été expressément déférée, il déconseille à la Cour de statuer sur ces questions dans le seul but d'aider le DPC à traiter cette plainte. « Il n'y a pas lieu d'y répondre pour permettre à la juridiction de renvoi de résoudre le litige au principal. La procédure prévue à l'article 267 TFUE instituant un dialogue entre juges, la Cour n'est pas appelée à apporter un éclairage à l'unique fin d'assister une autorité administrative dans le cadre d'une procédure sous-jacente à ce litige ». M. Saugmandsgaard Øe expose toutefois, à titre subsidiaire, les raisons qui l'amènent à s'interroger sur la validité de la décision « bouclier de protection des données » au regard des droits au respect de la vie privée et à la protection des données à caractère personnel. Le dossier Schrems n'est pas clos…

Par le lieutenant Océane GERRIET

Le mot de passe d'un smartphone peut-il être considéré comme une « convention secrète de déchiffrement » ?

Commentaire de l'arrêt rendu par la Chambre criminelle de la Cour de cassation le 10 décembre 2019, n° 18-86.878

Dans un arrêt rendu le 10 décembre 2019, les hauts magistrats répondent implicitement à cette question en confirmant l'arrêt rendu par la Cour d'appel de Paris le 8 novembre 2018 ayant condamné le mis en cause pour refus de communication de la convention secrète de déchiffrement d'un moyen de cryptologie. La Cour de cassation précise également que cette disposition, issue de l'article 434-15-2 du Code pénal, n'est pas contraire aux articles 6 et 7 de la Convention européenne des droits de l'Homme (ConvEDH).

En l'espèce, un individu est contrôlé à bord de son véhicule. Les fonctionnaires de police constatent la présence de résine de cannabis, d'une somme importante en numéraire et d'un téléphone portable. Lors d'une perquisition effectuée à son domicile, ils trouvent de nouveau des milliers d'euros et trois téléphones portables. Le mis en cause refuse de communiquer les codes de déverrouillage de ses téléphones. Il est ainsi poursuivi de plusieurs chefs, dont le refus de communiquer la convention secrète de déchiffrement de son téléphone.
Ses avocats soulèvent (notamment) l'inconventionnalité de l'article 434-15-2 du Code pénal en ce qu'il porte atteinte au droit de se taire taire et de ne pas s'auto-incriminer, droits garantis par les articles 6

et 7 de la ConvEDH. Ce moyen fut déjà soulevé dans un autre cas d'espèce similaire à celui-ci et précédemment évoqué dans la veille juridique de juin 2019 (n° 79, p. 29-36). Il avait donné lieu à une saisine du Conseil constitutionnel qui, par décision n° 2018-696 QPC rendue par le Conseil constitutionnel le 30 mars 2018, avait conclu à la conformité des dispositions du Code pénal. Pour mémoire, il estimait que cette disposition n'avait ni pour objet d'obtenir des aveux de la part du mis en cause, ni de reconnaître ou poser une présomption de culpabilité, mais simplement de permettre le déchiffrement de données cryptées **par** la personne (ou l'organisme) **ayant connaissance** de cette convention. Le Conseil constitutionnel précisait également que l'enquête ou l'instruction devait démontrer que ces données avaient été utilisées pour « préparer, faciliter ou commettre un crime ou un délit ». Enfin, il rappelait également que ces données existaient« indépendamment de la volonté de la personne suspectée ».

Dans le présent arrêt commenté, la Cour de cassation suit ce raisonnement. Elle précise que « l'atteinte au droit de se taire et au droit de ne pas s'auto-incriminer est constituée dès lors que les données ne peuvent exister indépendamment de la volonté du suspect, ce qui n'est pas le cas des données contenues dans les téléphones, qui peuvent être obtenues par des moyens techniques ». Cette approche est constante pour la Cour de cassation[1]. En l'espèce, les données contenues dans un smartphone peuvent être obtenues par des « pouvoirs coercitifs » existant « indépendamment de la volonté de l'intéressé », de sorte qu'en refusant de transmettre son mot de passe (par ailleurs, duquel s'agit-il : du code PIN ou du code de déverrouillage ?), le mis en cause

1. Exemple : Crim., 6 janvier 2015, n° 13-87.652.

n'a fait que retarder l'échéance. Enfin, la seconde condition constitutive est bien évidemment remplie, dès lors qu'au moment de son interpellation, le requérant était en possession de sommes d'argent importantes et de cannabis laissant « présumer un usage du téléphone portable en lien avec des infractions à la légalisation sur les stupéfiants ».

Cette solution est-elle évidente ? Rien n'est moins sûr. Dans un arrêt rendu le 16 avril 2019[2], la Cour d'appel de Paris prenait clairement le contrepied de la décision du Conseil constitutionnel. À ses yeux, si le code de déverrouillage d'un téléphone portable « **permet d'accéder** aux données de ce téléphone portable et donc aux éventuels messages qui y sont contenus », il « **ne permet pas de déchiffrer des données ou messages cryptés et, en ce sens, ne constitue pas une convention secrète d'un moyen de cryptologie** ». En effet, comme nous l'avions brièvement expliqué dans la veille juridique de juin 2019, c'est un système interne au smartphone qui permet de chiffrer et déchiffrer, tout en générant ses propres clés. Ainsi, l'infraction ne pouvait être constituée, le mot de passe d'un smartphone ne répondant pas à la définition de moyen de cryptologie telle que fixée dans l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique[3].

Force est de constater que l'appréhension de cette notion n'est pas aisée et qu'elle suscite le débat au sein des juridictions. Cela crée également des brèches favorables à la défense. Il reste donc à savoir si les juridictions vont s'aligner sur la position de la Cour de cassation ou forcer le législateur à amender ces dispositions…

2. Cour d'appel de Paris, 16 avril 2019, n° 18-09267.

3. « Tout matériel ou logiciel conçu ou modifié pour transformer des données (…) à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. »

Le non-respect du Règlement général sur la protection des données (RGPD) à nouveau sanctionné : une sanction d'un demi-million d'euros prononcée par la CNIL à l'encontre d'une société française

Délibération de la formation restreinte de la CNIL n° SAN-2019-010 du 21 novembre 2019 concernant la société Futura Internationale

Après avoir sévèrement sanctionné Google, la Commission nationale de l'informatique et des libertés (CNIL) démontre qu'elle assume pleinement son rôle de vigie des données personnelles. Une société française a été sanctionnée pour ne pas avoir respecté de nombreuses dispositions du RGPD dans le cadre de ses actions de démarchage téléphonique.

La société Futura Internationale est spécialiste de la rénovation énergétique pour les particuliers. À cette fin, elle sous-traite à des centres d'appels, situés en dehors de l'Union européenne, ses campagnes de prospection téléphonique. C'est une nouvelle fois le démarchage abusif qui est pointé du doigt et ce, en dépit du renforcement de la législation. Une plainte a donc été déposée auprès de la CNIL contre cette société par un plaignant dénonçant des appels réguliers et abusifs, malgré l'exercice de son droit d'opposition.

Conformément aux prérogatives qui sont les siennes, la Commission s'est rendue dans les locaux de l'entreprise pour effectuer un contrôle. Elle a découvert, à cette occasion, que d'autres plaignants

avaient exprimé leur mécontentement auprès de la société en raison d'un défaut de prise en compte de leur droit d'opposition. Elle a, par ailleurs, remarqué que le logiciel de gestion de clientèle permettait d'enregistrer des commentaires sur les clients et que ceux-ci pouvaient s'avérer « injurieux » ou « relatifs à l'état de santé » des personnes appelées. En outre, les clients étaient mal informés, voire pas informés du tout, sur le traitement de leurs données personnelles ou sur la possibilité que l'appel soit enregistré. Enfin, à l'issue du contrôle, elle a demandé à la société de fournir de nombreux documents, tels que les contrats passés avec les sous-traitants. Malgré de nombreux délais accordés, la société n'a répondu que partiellement aux exigences de la CNIL.

De fait, dans une décision en date du 27 septembre 2018, elle a mis en demeure la société de se mettre en conformité avec les exigences du RGPD et a prescrit des mesures correctrices :

- veiller au caractère pertinent et non excessif des données collectées (art. 5-1-c) en supprimant les commentaires injurieux et en empêchant leur enregistrement, notamment par la mise en place d'une exclusion automatique de termes et par la sensibilisation des salariés ;
- transmettre les documents initialement demandés sur les sociétés sous-traitantes (leur nom et leurs enregistrements les plus récents) ;
- fournir une information complète sur le régime de traitement des données (responsable du traitement, finalité, règles de transfert, etc.) aux personnes auprès desquelles les données sont directement (articles 12 et 13 du RGPD) ou indirectement (article 14 du RGPD) collectées (en l'espèce, les personnes prospectées par téléphone n'étaient pas averties du régime de traitement de leurs données) ;

- rendre effectif le droit d'opposition (article 21-1 du RGPD) ;
- respecter les garanties relatives au transfert de données à caractère personnel vers un État n'assurant pas un niveau suffisant de protection (articles 46 à 49 du RGPD) ;
- justifier auprès de la CNIL de l'effectivité de ces mesures.

Une nouvelle fois, Futura Internationale demande des reports de délais pour finalement informer la CNIL qu'elle ne pourra répondre à la totalité des mesures. Dès lors, le 11 juin 2019, la CNIL a notifié à la société un rapport détaillant les manquements constatés. Peu de temps après, cette dernière a fourni des observations, dont l'information selon laquelle les commentaires inappropriés présents dans le logiciel étaient effacés. Néanmoins, la société n'ayant pas respecté l'ensemble des préconisations, la CNIL a maintenu les propositions formulées par le rapporteur. Elle conclut aux manquements suivants :

- **absence de prise en compte du droit d'opposition des personnes** (absence de mécanisme efficace permettant d'identifier les personnes ayant émis leur droit d'opposition et de répercuter leur demande sur l'ensemble des sous-traitants, de sorte que malgré une demande d'opposition, certaines personnes figuraient encore dans le traitement) ;
- **présence de données non pertinentes** (commentaires excessifs ou inadéquats) ;
- **information insuffisante relative au traitement des données personnelles** (la société a mis en place un mécanisme d'information *a posteriori* par l'envoi d'un courriel postérieur à l'échange téléphonique, or ce process n'est pas conforme aux prescriptions de l'article 13 du RGPD qui exige une information, même sommaire, au moment où les données sont collectées) ;
- **absence d'encadrement suffisant relatif au transfert de**

données personnelles en dehors de l'UE ;
- **défaut de coopération avec la CNIL**. Cette dernière souligne deux points : d'une part, il incombe à la société de choisir des professionnels compétents pour répondre aux exigences du RGPD, d'autre part, la société a « clairement exprimé » son « désintérêt flagrant pour ces sujets ».

Au-delà de la gravité des manquements, la CNIL met en lumière l'absence de diligence de la société. Ainsi, outre l'amende de 500 000 € et l'astreinte de 500 € par jour de retard concernant la mise en conformité, la CNIL entérine la publicité de la décision qui vise à rappeler qu'elle « porte attention particulière au respect des droits des personnes, notamment dans le contexte des pratiques de démarchage téléphonique qui sont une préoccupation du quotidien pour les personnes **et que le fait de coopérer avec la CNIL est une obligation qui, si elle n'est pas respectée, est sanctionnable** ».

Cette décision se veut donc véritablement pédagogique mais résonne également comme un avertissement à l'encontre des entreprises responsables de traitement. Elle rappelle que la protection des données personnelles relève de la vigilance de tous mais qu'elles ont un rôle prééminent à jouer et une responsabilité à endosser. Enfin, cette décision souligne également l'« ampleur » du phénomène du démarchage et ses « conséquences pratiques pour les personnes démarchées ». À ce jour, la proposition de loi visant à renforcer les droits des consommateurs en matière de démarchage téléphonique, qui prévoit notamment des amendes administratives plus conséquentes et une obligation d'actualiser leur base de fichiers avec la base Bloctel, est renvoyée à la commission des lois. *To be continued…*

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

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

FÉVRIER 2020

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

Par le G^al^ d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE JUDICIAIRE

Cour de cassation, Chambre criminelle (n° 18-84.755), arrêt n° 2790 du 7 janvier 2020, Procureur général près la Cour d'appel de Poitiers et autres

Les atteintes aux systèmes de traitement automatisé de données prévues aux articles 323-1 à 323-3 du Code pénal ne sauraient être reprochées à la personne qui, bénéficiant des droits d'accès et de modification des données, procède à des suppressions de données, sans les dissimuler à d'éventuels autres utilisateurs du système.

Une société a conçu et développé un logiciel de gestion à destination des pharmacies, commercialisé par une autre entreprise. Lors d'un contrôle dans des officines, l'administration fiscale découvre une fonctionnalité qui permet, après saisie d'un mot de passe personnel, d'effacer, avant l'arrêté comptable, les lignes d'écritures relatives à des ventes payées en espèces qui ne correspondent pas à des actions traçables par ailleurs (prescription médicale par ex.). En outre, une manipulation externe au logiciel, effectuée directement en ligne de commande, détruit les traces de ces effacements par suppression du fichier qui les contient. La fraude fiscale est évidente, mais ce n'est pas elle qui est l'objet du pourvoi devant la Cour de cassation.

L'affaire est examinée au regard des dispositions de la « loi Godfrain » qui réprime les infractions portant atteinte aux systèmes

de traitement automatisé de données (STAD), prévues et réprimées par les articles 323-1 et suivants du Code pénal. Ces infractions sont constituées lorsqu'il y a eu « violation de la volonté du maître du système », notamment lorsqu'on pénètre ou se maintient frauduleusement dans un STAD ou lorsqu'on modifie frauduleusement les données qu'il contient (art. 323-3 CP).

L'article 323-3-1, quant à lui, réprime « le fait, sans motif légitime de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 à 323-3 […] ».

C'est en s'appuyant sur cet article qu'est diligentée une enquête préliminaire suivie d'une information. La chambre de l'instruction de la Cour d'appel de Poitiers ayant tranché par une ordonnance de non-lieu, le procureur général et l'administration fiscale se pourvoient en cassation.

L'administration fiscale considère que la suppression frauduleuse de données (art.323-3 CP) est établie, « même si elle est réalisée dans un système auquel une personne a un accès légitime ». L'administration fiscale conteste aussi qu'ait été écarté le caractère « frauduleux » de l'action au prétexte qu'elle est aisément décelable. Enfin, elle conteste que l'infraction prévue et réprimée par l'article 323-3-1 ne soit pas relevée.
S'agissant de la suppression frauduleuse, les juges du fond lui opposent la double condition que le système n'appartienne pas à l'agent et que la modification soit effectuée à l'insu du propriétaire.

C'est une parfaite application de la « volonté du maître du système ». Dans le cas d'espèce, le propriétaire est nécessairement informé de l'existence du logiciel et de ses conséquences, puisqu'il en est le bénéficiaire. Puisque l'infraction prévue à l'article 323-3 n'est pas constituée, on ne peut poursuivre l'entreprise ayant fourni le logiciel sur la base de l'article 323-3-1.

La Cour de cassation donne raison à la chambre de l'instruction. Cet arrêt complète une jurisprudence déjà riche sur la notion de « volonté du maître du système ».

Cour d'appel, Aix-en-Provence, 4e et 6e chambres réunies (n° 16/12997), arrêt du 24 janvier 2020

La consultation pendant les heures de service de sites libertins à partir d'un ordinateur professionnel est constitutif d'une faute grave justifiant un licenciement.

Saisie par voie d'appel d'un jugement de conseil des prud'hommes de Fréjus, la Cour d'appel d'Aix-en-Provence confirme le licenciement pour faute grave d'un employé.
Celui-ci, depuis un ordinateur mis à sa disposition par son employeur pour les besoins de sa mission, consultait pendant ses heures de service des sites de rencontre à caractère sexuel et stockait des documents sans rapport avec son activité professionnelle.
Pour sa défense, l'employé avait avancé que l'ordinateur était à la disposition de tout le personnel et sans protection par mot de passe et que l'employeur n'établissait pas que les fichiers stockés étaient les siens. Il avait également opposé le fait que l'employeur y avait accédé sans information préalable du salarié et sans déclaration à la

Commission nationale de l'informatique et des libertés (CNIL)…
La Cour constate que l'ordinateur est bien un ordinateur dévolu à un seul usage professionnel avec un mot de passe. Elle relève que l'huissier a examiné, lors de son constat, l'historique du navigateur Internet, le contenu du fichier « documents » sans jamais ouvrir la messagerie et les dossiers manifestement personnels[1]. Pour la Cour, l'historique de connexion de l'employé ne saurait être qualifié de fichier personnel clairement identifié. Il met en évidence de nombreuses connexions de longue durée, aussi bien pendant les heures de travail qu'en dehors de celles-ci, sur des sites de rencontres ou à caractère sexuel, comme le site « becoquin.fr », prouvant les manquements de celui-ci à son obligation de loyauté. Il est ainsi établi un comportement créant un trouble dans le bon fonctionnement de l'entreprise au regard des fonctions du salarié dont la faute grave est établie.
Le contrôle de l'usage des moyens informatiques, mis par l'employeur à la disposition des personnels d'une entreprise ou d'une administration, fait l'objet d'une abondante jurisprudence. L'usage abusif par l'employé de l'outil informatique à des fins privées est un manquement à ses obligations contractuelles[2]. Il en est de même pour un usage abusif à des fins immorales susceptibles de nuire aux intérêts de l'entreprise[3].
Dans un récent arrêt du 3 octobre 2018, la chambre sociale de la Cour de cassation[4] a examiné un litige relatif au licenciement pour faute grave du salarié pour utilisation abusive de son ordinateur et

1. Cour européenne des droits de l'Homme, 5e section, arrêt du 22 février 2018. Un employeur peut accéder aux données stockées sur l'ordinateur professionnel d'un employé, dès lors qu'elles ne sont pas identifiées comme étant privées.
2. Cass. Soc. n° 05-46.455, arrêt du 16 mai 2007.
3. Cass. Soc. n° 03-45.269, arrêt du 2 juin 2004.
4. Cass.Soc. n° 17-13.087, arrêt du 3 octobre 2018.

d'Internet durant ses heures de travail, consistant dans la consultation de sites pornographiques. Dans le cas d'espèce, elle a donné tort à l'employeur en se fondant sur trois éléments :
1/ Les codes d'accès de chacun des ordinateurs de la société consistaient dans les simples initiales de leurs utilisateurs habituels respectifs et les doubles des clés de l'ensemble des bureaux étaient également accessibles, de sorte qu'il était possible à n'importe lequel des salariés d'avoir accès au poste informatique du salarié ;
2/ Le procédé de géolocalisation, au moyen duquel l'employeur entendait démontrer la présence du salarié dans l'entreprise lors des connexions litigieuses, n'avait pas fait l'objet d'une déclaration préalable à la CNIL, n'avait pas été soumis à une consultation des représentants du personnel et n'avait pas fait l'objet d'une information individuelle préalable auprès des salariés ;
3/ L'employeur ne produisait aucun élément permettant de s'assurer que le salarié était réellement l'auteur des connexions litigieuses.

Tribunal judiciaire de Paris, ordonnance de référé du 8 janvier 2020, Cartier International et autres / Bouygues Telecom et autres

Les dispositions de l'article L. 716-6 du Code de la propriété intellectuelle, relatives au référé interdiction en matière de contrefaçon, ne font pas obstacle à l'application de l'article 6-I-8 de la Loi sur la confiance en l'économie numérique (LCEN). Lorsque les démarches auprès des hébergeurs restent vaines, le juge des référés peut enjoindre aux fournisseurs d'accès à Internet de bloquer l'accès aux sites illégaux.

Le Groupe Richemont regroupe dix-sept entreprises de luxe (joaillerie, horlogerie et instruments d'écriture), parmi lesquelles Cartier International AG, Montblanc-Simplo GmbH, Officine Panerai AG et Richemont International SA. Par huissier, ces entreprises font constater que les sites « nowmontres », « contrefaconmontres », « repliquemontres » et « repliquefrance » commercialisent des répliques de montres sur lesquelles figurent leurs marques. Ces sites sont rédigés en français, indiquent des prix en euros et sont manifestement destinés à un public français. Les intentions des auteurs sont explicites : ils vendent, selon leurs propres termes, des « répliques de montres de luxe pas chères », des « fausses montres ».

Trois des quatre sites Internet litigieux affichent clairement qu'ils procèdent à la vente de copies de montres de luxe, l'un d'eux revendique par son nom de domaine le caractère contrefaisant des répliques vendues. Le site Internet accessible à l'adresse www.repliquefrance.com procède à une redirection automatique de ce site vers le site Internet accessible à l'adresse www.faussemontre.fr, site rédigé en langue française et dont les prix sont affichés en euros, proposant à la vente au public français des « fausses montres ». S'il fallait encore écarter le doute, le comparatif des prix de vente proposés par ces sites avec le prix de vente pratiqué pour les véritables montres confirme que les produits vendus ne sont pas authentiques. L'absence des mentions exigées par la LCEN pour les sites objets du litige et l'anonymisation intégrale de ces sites par le biais de ses différents prestataires (enregistrement anonymisé du nom de domaine, absence de point de contact), démontrent la connaissance du caractère illicite des biens proposés à la vente sur les sites en litige par les auteurs et éditeurs de ces sites.

Les entreprises victimes se tournent d'abord vers les hébergeurs, sociétés américaines, pour obtenir la fermeture des sites. À l'exception de l'un d'entre eux, les démarches sont infructueuses.
Dans ces conditions, les entreprises victimes assignent en référé Orange, Bouygues Telecom, Free et SFR afin qu'il leur soit ordonné de mettre en œuvre ou faire mettre en œuvre toutes mesures appropriées de blocage afin d'empêcher l'accès aux services de communication au public en ligne accessibles à la date du présent acte introductif d'instance aux URL vwwv.contrefaconmontre.com, www.repliquefrance.com et www.repliquemontre.cn, à partir du territoire français (y compris dans les départements ou régions d'Outre-mer et collectivités uniques, ainsi que dans les îles Wallis et Futuna, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises) et/ou par leurs abonnés ayant conclu un contrat sur ce territoire.
Pour soutenir leur demande, les entreprises s'appuient sur l'article 809 du Code de procédure civile, selon lequel le président peut toujours, même en présence d'une contestation sérieuse, prescrire en référé les mesures conservatoires ou de remise en état qui s'imposent, soit pour prévenir un dommage imminent, soit pour faire cesser un trouble manifestement illicite. Elles visent aussi l'article 6-I-8 de la LCEN et, à défaut, l'article L. 716-6 du Code de la propriété intellectuelle.
L'article 6-I-8 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est issu de la transposition de l'article 18 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 sur le commerce électronique. Il dispose que « l'autorité judiciaire peut prescrire, en référé ou sur requête, [aux hébergeurs] ou, à défaut, [aux fournisseurs d'accès à Internet], toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication

au public en ligne ».

L'article L. 716-6 du Code de la propriété intellectuelle est issu de la loi n° 2007-1544 du 29 octobre 2007 de lutte contre la contrefaçon. Il crée une procédure de référé-interdiction en matière de contrefaçon. Il dispose que « toute personne ayant qualité pour agir en contrefaçon peut saisir en référé la juridiction civile compétente afin de voir ordonner, au besoin sous astreinte, à l'encontre du prétendu contrefacteur ou des intermédiaires dont il utilise les services, toute mesure destinée à prévenir une atteinte imminente aux droits conférés par le titre ou à empêcher la poursuite d'actes argués de contrefaçon. La juridiction civile compétente peut également ordonner toutes mesures urgentes sur requête lorsque les circonstances exigent que ces mesures ne soient pas prises contradictoirement, notamment lorsque tout retard serait de nature à causer un préjudice irréparable au demandeur. Saisie en référé ou sur requête, la juridiction ne peut ordonner les mesures demandées que si les éléments de preuve, raisonnablement accessibles au demandeur, rendent vraisemblable qu'il est porté atteinte à ses droits ou qu'une telle atteinte est imminente (…) ».

Les fournisseurs d'accès ne sont pas hermétiques à la demande des sociétés victimes. Ils demandent au juge des référés de trancher un certain nombre de points de droit. Orange, en particulier, estime qu'en application de l'adage « *Specialia generalibus derogant* », la LCEN ne s'applique pas, l'article L. 716-6 du Code de la propriété intellectuelle, spécifique au droit des marques, prévoyant la possibilité d'agir en référé à l'encontre d'un prestataire de service utilisé par des contrefacteurs de marques, afin de prendre des mesures nécessaires pour empêcher la poursuite des actes de contrefaçon, parmi lesquelles figurent les mesures de blocage. Selon la juridiction, tant le législateur européen que le législateur national n'ont pas entendu écarter les dispositions de la directive

2000/31/CE et les dispositions de l'article 6-I-8 de la LCEN, en énonçant une règle spéciale en matière de marques, à l'article 9 de la directive 2004/48/CE et à l'article L. 716-6 du Code de la propriété intellectuelle. Les demandes de blocage de l'accès à certains noms de domaine faites par les sociétés demanderesses peuvent de ce fait reposer sur le fondement des articles 809 du Code de procédure civile et 6- I-8 de la LCEN. C'est la première fois que cet article est appliqué à un site de produits contrefaits.

S'agissant des interrogations portant sur le caractère proportionné et strictement nécessaire à la protection des droits en cause, au regard notamment de la difficulté d'agir à l'encontre de l'auteur et/ou éditeur et/ou hébergeur, des risques d'atteinte au principe de la liberté d'expression et de communication (risques d'atteintes à des contenus licites et au bon fonctionnement des réseaux), de l'importance du dommage allégué, des risques d'atteinte à la liberté d'entreprendre des FAI, et de l'efficacité des mesures, d'ordonner aux FAI, la mise en œuvre des mesures de blocage sollicitées, le juge oppose le principe de subsidiarité. Celui-ci, « fondé sur des motifs d'efficacité et de proportionnalité, suppose que celui qui se prétend victime d'une atteinte à ses droits et qui sollicite une mesure auprès des fournisseurs d'accès à internet établisse l'impossibilité d'agir efficacement et rapidement contre l'hébergeur, de même que contre l'éditeur ou l'auteur du contenu litigieux ».

Orange, Bouygues Telecom, Free et SFR doivent donc mettre en œuvre et/ou faire mettre en œuvre, dans le délai de 15 jours à compter de la signification de la présente décision et ce, pendant une durée de 12 mois, toutes mesures propres à empêcher l'accès aux sites incriminés.

Regard sur l'actualité : La « vengeance pornographique »

De récents événements ont souligné combien les messages, images, vidéos publiés sur le web, notamment sur les réseaux sociaux, pouvaient gravement compromettre l'e-réputation et la réputation tout court d'une personne. La diffusion d'images intimes d'un(e) « ex » sur les réseaux sociaux est une « cyberviolence » devenue un mode de vengeance d'autant plus attentatoire à l'image que la diffusion en cascade est très difficile à maîtriser en raison notamment de la viralité des réseaux sociaux ou du caractère très relatif du « droit à l'oubli ».

L'incrimination de la vengeance pornographique (*revenge porn*) est récente. Elle fait suite à un arrêt de la Cour de cassation du 16 mars 2016[5] qui, s'appuyant sur le droit du moment, a cassé un arrêt de la Cour d'appel de Montpellier. En l'espèce, cette juridiction avait confirmé une condamnation en première instance d'une personne qui avait diffusé, sur Internet, une photographie de son ex-compagne, prise par lui, à l'époque de leur vie commune, la représentant nue alors qu'elle était enceinte. Pour la Cour de cassation, n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement[6]. Les commentateurs ont accusé les magistrats de la

5. Cass.crim, 16 mars 2016, n°15-82.676.

6. « Attendu que, pour confirmer cette décision, l'arrêt énonce que le fait, pour la partie civile, d'avoir accepté d'être photographiée ne signifie pas, compte tenu du caractère intime de la photographie, qu'elle avait donné son accord pour que celle-ci soit diffusée ; Mais attendu qu'en se déterminant ainsi, alors que n'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement, la cour d'appel a méconnu les textes susvisés et le principe ci-dessus énoncé. »

juridiction suprême de ne pas être « de leur temps », oubliant sans doute que la Cour de cassation a pour mission de dire le droit et non de combler ses lacunes. C'est le rôle du Parlement ! La modification du Code résulte de la loi du 7 octobre 2016 pour une République numérique qui modifie l'article 226-2-1 du Code pénal. Elle comble un vide, car le législateur n'est pas toujours en phase avec les usages et surtout les mésusages liés au développement des nouvelles technologies. Indifférente au consentement lors de la prise de photographie, la nouvelle incrimination rend possible une condamnation, dès lors que c'est la diffusion sans consentement exprès qui est visée.

Est puni de deux ans d'emprisonnement et de 60 000 euros d'amende le fait de transmettre ou de diffuser sans le consentement exprès de la personne l'image ou la voix de celle-ci, prise dans un lieu public ou privé, dès lors qu'elle présente un caractère sexuel. Cette modification du Code pénal était nécessaire. Comme cela a été rappelé lors des débats parlementaires, 90 % des victimes sont des femmes qui évoquent souvent un viol virtuel.

Le *revenge porn* peut aussi faire l'objet d'une action au civil. Ainsi, dans un jugement du 20 novembre 2018, le tribunal de grande instance de Bobigny[7] a jugé que la diffusion sans autorisation de correspondances privées et d'images portant sur la vie sexuelle et sentimentale du plaignant est constitutive d'une atteinte à la vie privée.

En l'espèce, le plaignant demandait à la juridiction saisie de condamner une ancienne maîtresse sur la base de l'article 9 du Code civil qui protège le droit à la vie privée. Il reprochait à madame Y. d'avoir envoyé, sans son autorisation, sur le téléphone portable de

7. TGI de Bobigny, chambre 5/section 3, jugement du 20 novembre 2018, M.X/Mme Y.

sa femme et de sa sœur des documents intimes, notamment la photographie de son sexe. Le tribunal lui a donné raison en minimisant toutefois l'évaluation du préjudice, eu égard au caractère connu de sa liaison.

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

MARS
2020

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

DISCOURS D'OUVERTURE DU FIC 2020

Prononcé par le Général d'armée (2S) Marc Watin-Augouard, directeur du CREOGN (2012-2020)

Avec l'équipe d'organisation du FIC, Guillaume Tissier et moi-même, accompagnés par Elly Van den Heuvel, présidente de l'Advisory Board du FIC, nous sommes heureux de vous accueillir pour cette douzième édition qui, pour la première fois, se déroule sur trois jours et voit le nombre des participants dépasser sans doute le seuil de 12 000. Ce dynamisme témoigne d'une prise de conscience partagée des enjeux de la transformation numérique et, en particulier, de la cybersécurité qui la conditionne.

Soyez les bienvenus !
Le FIC n'est pas un événement comme un autre ! il a son ADN.
Les fidèles, depuis les origines, le connaissent ; les nouveaux participants le découvrent. On vient au FIC par curiosité, on y revient par conviction !

Mesdames, messieurs, vous l'avez compris, vous participez à un Forum. Dans la Rome Antique, le Forum était en même temps un marché et un espace de débat public, l'un et l'autre inséparables. Déjà les Romains avaient compris l'importance du partenariat public-privé.

Sans les entreprises partenaires, toujours plus nombreuses, que nous saluons et remercions, le FIC n'existerait pas ou ne serait pas ce qu'il est. Merci aux 450 exposants.

Sans les participants, venant de 112 pays – parfois de continents

lointains – les idées, les projets resteraient sans partage. Que nos amis étrangers se sentent ici membres d'une même communauté, d'un même « réseau social » qui transcende les différences de langue, de culture. Les « gens du cyber » sont comme les « gens de mer ». Ils se comprennent parce que l'espace numérique les unit dans un même destin.

Sans les 120 médias accrédités qui couvrent l'événement, le discours serait confiné dans ces murs, la prise de conscience collective serait imparfaite, alors que l'acculturation de tous est une priorité absolue.

Au sein de la région des Hauts-de-France, si proche du Royaume-Uni et du Benelux, à Lille, métropole européenne par sa géographie et son engagement, le FIC a l'ambition de rassembler les hommes et les femmes qui veulent entrer pleinement dans le siècle du numérique sans jamais renoncer aux fondamentaux de l'humanité.

« Replacer l'humain au cœur de la cybersécurité », de « sa » cybersécurité, tel est le thème de cette année. Ce n'est pas un effet de mode ou un hasard mais un choix délibéré. « La cybersécurité pour l'humain, par l'humain », une devise qui pourrait être nôtre, tant nous sommes convaincus que l'humain est la finalité de toute technologie, de toute organisation, de tout protocole, de toute procédure. « Science sans conscience n'est que ruine de l'âme » écrivait François Rabelais au XVIe siècle. Propos prémonitoires, tant nous sommes responsables du substrat numérique que nous allons laisser aux jeunes générations, de plus en plus présentes parmi nous au FIC. « En notre temps, la seule querelle qui vaille est celle de l'homme. C'est l'homme qu'il s'agit de sauver, de faire vivre et de développer ». Prononcées il y a plus de soixante ans par Charles de Gaulle, ces paroles résument « l'esprit FIC ».

Dans ce contexte, les États doivent se « reformater », car ils doivent assurer la défense et la sécurité des personnes physiques et morales et des biens matériels et immatériels face aux nouveaux prédateurs. C'est ce qui les légitime et fonde leur souveraineté. S'agissant de l'Europe, nombreux sont les commentateurs qui affirment qu'elle a perdu la bataille du *hardware* et celle du *software*, qu'elle est devenue championne de la norme, laissant ainsi imaginer qu'il n'y a plus d'option possible pour des Européens condamnés au suivisme, condamnés à faire partie d'une « colonie du numérique », comme l'a souligné un rapport parlementaire.

Il n'en est rien ! La transformation numérique a ceci d'extraordinaire : sa capacité de changer rapidement de cap sous l'effet d'une technologie disruptive qui rebat les cartes. À nous de la chercher, de ne pas la tuer dans l'œuf, en soutenant nos centres de recherche, nos start-up, en favorisant l'essor d'une industrie européenne à la hauteur de la première puissance économique mondiale.

L'Europe ne peut subir ! Mieux, elle doit proposer une autre voie, une autre voix.
Une voie qui libère de l'étau qui se resserre sur nous avec pour mâchoires une société de liberté surveillée, dont nous avons vérifié l'existence en 2013, et une société de contrôle permanent où chaque geste, chaque parole, chaque comportement est capté, mesuré, évalué, sanctionné.
Une voix dont l'Europe doit être porteuse par un discours universel qui ne s'impose pas mais se propose au reste du monde ! Le discours d'une liberté sécurisée qui place d'abord la cybersécurité au service de la société, de l'humain. D'une liberté sécurisée qui redonne à l'humain une pleine souveraineté numérique individuelle et

collective qui préserve sa vie privée, sa sphère d'intimité, son identité au sens de son unicité.

Un nouveau souffle, une nouvelle ambition, une nouvelle ardeur ! C'est aujourd'hui le moment ! La transformation numérique est une chance pour notre société ! Ne la laissons pas passer ! Ne la laissons pas nous dépasser !

Par le Gal d'armée (2S) Marc Watin-Augouard

Un nouveau souffle numérique pour l'Union européenne

Au moins depuis la promulgation, en avril 2016, du Règlement général sur la protection des données (RGPD)[1], puis de la directive NIS (ou SRI)[2], relative à la cybersécurité des opérateurs de services essentiels (OSE) et des fournisseurs de services numériques (FSN), l'Union européenne prend la pleine conscience des enjeux de la transformation numérique[3]. Le sommet de Tallinn, en septembre 2017, a été l'occasion de lancer le « Paquet cyber » ayant débouché sur le *Cybersecurity Act* qui a pérennisé l'ENISA et fixé un cadre pour une certification européenne de cybersécurité.

Avec le renouvellement de la Commission et l'arrivée de sa présidente Ursula von der Leyen et, surtout, la nomination de Thierry Breton, commissaire en charge du numérique, on pouvait s'attendre à une accélération du programme européen. En l'espace de quelques jours, la Commission vient de publier plusieurs communications au Parlement européen, au Conseil et au Comité économique des régions qui rendent publique la stratégie qu'elle entend conduire dans les cinq prochaines années. La première, « Façonner l'avenir numérique de l'Europe[4] », en date du 19 février

1. RGPD Règlement (UE) 2016/679 .
2. Directive SRI Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016.
3. On peut ajouter le règlement relatif à la libre circulation des données à caractère non personnel dans l'Union européenne (Règlement (UE) 2018/1807), le règlement sur la cybersécurité (Règlement (UE) 2019/881) et la directive sur les données ouvertes (Directive (UE) 2019/1024).
4. Communication COM (2020) 67 final du 19 février 2020.

2020, est en quelque sorte la déclaration d'intention, précisée, le même jour, par une communication sur la « Stratégie européenne pour les données » et une autre sur l'intelligence artificielle[5]. Ce corpus a été complété, le 10 mars, par une communication sur une « Nouvelle stratégie industrielle pour une Europe verte et numérique, compétitive à l'échelle mondiale[6] ». En exposant ses orientations politiques, Ursula von der Leyen avait déclaré que l'Union européenne devait conduire la transition vers « une planète saine et un nouveau monde numérique ». Le lien entre la « transformation verte » et la « transformation numérique » n'est pas un hasard, car les deux sont étroitement liées. Si l'on n'y prend garde, la seconde peut contrarier la première, car son bilan carbone n'est pas toujours aussi vertueux que ce que l'on croit. Inversement, la transformation numérique peut avoir des effets régulateurs très positifs, notamment en ce qui concerne l'énergie, le développement durable.

De la lecture de ces documents ressortent quelques « idées force » qui rejoignent l'esprit du FIC 2020 consacré à la place de l'humain au cœur de la cybersécurité (voir discours d'ouverture *supra*).

1. L'appui de la transformation numérique sur des valeurs communes

La référence aux valeurs communes est ici essentielle. Trop souvent la transformation numérique est abordée sous une approche technologique qui masque l'essentiel : sa finalité. « La vision de la Commission découle des valeurs et des droits fondamentaux et de la

5. Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance, COM (2020) 65 final.

6. Une nouvelle stratégie industrielle pour l'Europe, Communication COM (2020) 102 final du 10 mars 2020.

conviction que l'être humain est et doit rester au centre […]. Les citoyens doivent avoir la possibilité de se développer personnellement, de poser des choix en toute liberté et en toute sécurité, de s'engager dans la société, indépendamment de leur âge, de leur sexe ou de leur parcours professionnel. Les entreprises ont besoin d'un cadre qui leur permette de démarrer, de se développer, de mettre en commun et d'utiliser des données, d'innover et d'entrer en concurrence ou de coopérer dans des conditions équitables. Et l'Europe doit avoir le choix de poursuivre la transformation numérique selon ses propres modalités ». Les valeurs et les règles éthiques de l'UE, ainsi que ses normes sociales et environnementales, doivent s'appliquer aussi dans l'espace numérique.

Souvent ringardisées par ceux qui placent en avant le business, souvent dévoyées ou détournées par ceux qui les accaparent au service d'une idéologie, les valeurs vont revenir au premier plan à la faveur de la crise que nous traversons. C'est une évidence !
C'est l'occasion pour l'Europe de prendre l'initiative et d'offrir au reste du monde « une autre voix, une autre voie » qui reflètent les meilleurs aspects de notre continent : l'ouverture, l'équité, la diversité, la démocratie et la confiance. Ainsi peut-on lire « L'Europe peut se saisir de cette transformation numérique et fixer les normes mondiales en matière de développement technologique. Plus important encore, elle peut le faire tout en garantissant l'inclusion et le respect de chaque être humain. La transformation numérique ne peut réussir que si elle fonctionne pour tous et pas seulement pour quelques-uns. Il s'agira d'un projet véritablement européen – une société numérique fondée sur les valeurs et les règles européennes – qui peut véritablement inspirer le reste du monde ». L'Europe devra ainsi se positionner en tant que pionnier dans le

débat mondial.
Au cours des cinq prochaines années, la Commission visera trois objectifs clés permettant à l'Europe de suivre sa propre voie par une transformation numérique qui profite aux citoyens tout en respectant les valeurs : une technologie au service des personnes[7], une économie juste et compétitive[8], une société ouverte, démocratique et durable[9].

Tenant compte des expériences passées, la Commission souhaite que, dans un monde où une grande partie du débat public et de la publicité politique se fait désormais en ligne, l'Union soit prête à agir pour défendre vigoureusement nos démocraties. « Les citoyens attendent des réponses pertinentes aux tentatives de manipulation de l'espace d'information, qui prennent souvent la forme de campagnes de désinformation ciblées et coordonnées. L'Europe a besoin de plus de transparence sur les modes de partage et de gestion de l'information sur l'internet. La démocratie, de même que la diversité culturelle, a absolument besoin de médias de qualité et

7. Développement, déploiement et adoption de technologies qui améliorent sensiblement la vie quotidienne des citoyens. Une économie forte et compétitive qui maîtrise et façonne la technologie dans le respect des valeurs européennes.
8. Un marché unique sans heurts, où les entreprises, quelle que soit leur taille ou leur secteur d'activité, peuvent se concurrencer sur un pied d'égalité et peuvent développer, commercialiser et utiliser des technologies, des produits et des services numériques à une échelle qui dope leur productivité et leur compétitivité à l'échelle mondiale, et où les consommateurs peuvent avoir la certitude que leurs droits sont respectés.
9. Un environnement fiable dans lequel les citoyens ont la maîtrise de la façon dont ils agissent et interagissent et des données qu'ils fournissent à la fois en ligne et hors ligne. Une approche européenne de la transformation numérique qui renforce nos valeurs démocratiques, respecte nos droits fondamentaux et contribue à une économie durable, neutre pour le climat et efficace dans l'utilisation des ressources.

fiables. C'est dans ce contexte que la Commission présentera un plan d'action pour la démocratie européenne et un plan d'action spécifique pour le secteur des médias et de l'audiovisuel. Un plan d'action pour la démocratie européenne destiné à améliorer la résilience de nos systèmes démocratiques, à soutenir le pluralisme des médias et à faire face aux menaces d'intervention extérieure dans les élections en Europe[10]».

2. Une cybersécurité au service de la transformation numérique

Le FIC le proclame depuis ses origines, il n'y a pas de transformation numérique au service de la liberté sans cybersécurité. Comme le souligne la Commission, « une authentique transformation numérique doit commencer par des entreprises et des citoyens européens convaincus que leurs applications et leurs produits sont sûrs. Plus nous sommes interconnectés, plus nous sommes vulnérables à la cyberactivité malveillante. Pour faire face à cette menace croissante, nous devons travailler ensemble à chaque étape : fixer des règles cohérentes pour les entreprises et renforcer les mécanismes proactifs d'échange d'informations ; assurer la coopération opérationnelle entre États membres et entre l'UE et les États membres ; établir des synergies entre la cyber-résilience civile et la répression et la défense dans le domaine de la cybersécurité ».
Cette cybersécurité doit s'appuyer sur une stratégie européenne, comprenant la mise en place d'une unité conjointe de cybersécurité[11], une révision de la directive sur la sécurité des

10. Action prévue au 4e trimestre de 2020.
11. Le cadre de l'UE pour la certification de cybersécurité et l'Agence de l'UE pour la cybersécurité (ENISA) (Règlement (UE) 2019/881 sur la cybersécurité) devraient jouer un rôle important à cet égard.

réseaux et des systèmes d'information[12] et une impulsion au marché unique de la cybersécurité. Il convient de soutenir les services répressifs et les autorités judiciaires afin qu'ils puissent travailler efficacement en développant de nouveaux outils de lutte contre la cybercriminalité, mais aussi de sensibiliser les citoyens de l'UE à la cybersécurité. Ce qui est illicite hors ligne doit aussi l'être en ligne.
La communication évoque la cybersécurité liée aux nouvelles pratiques en matière de données, selon lesquelles les volumes stockés en centres de données diminuent tandis que davantage de données sont réparties de manière systématique plus à proximité de l'utilisateur, « à la périphérie ». C'est le « *edge computing* » que Thierry Breton, alors patron d'Atos, présentait lors du dernier salon VIVATECH. A terme, 80 % de nos données seront stockées, traitées à proximité et non plus dans le « *cloud* », ne serait-ce que pour assurer leur traitement en temps réel. « Il sera essentiel de préserver la sécurité des données lors de l'échange de données. Assurer la continuité des contrôles d'accès (c'est-à-dire la gestion et le respect des attributs de sécurité des données) tout au long de la chaîne de valeurs des données sera un préalable ardu mais indispensable pour favoriser l'échange de données et garantir la confiance entre les différents acteurs des écosystèmes de données européens. »

3. Une souveraineté technologique européenne

Cette souveraineté est particulièrement sensible à l'heure du déploiement de la 5G. L'Europe doit développer et mettre en œuvre ses propres capacités critiques pour réduire sa dépendance vis-à-vis du reste du monde. La Commission souhaite, en faisant appel à un

12. Directive SRI Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016.

large éventail de fonds publics et privés, investir davantage dans les capacités stratégiques qui permettent de développer et d'utiliser des solutions numériques à grande échelle et de viser l'interopérabilité dans des infrastructures numériques essentielles, telles que les réseaux 5G (puis 6G) étendus. Cette ambition couvre aussi les innovations disruptives, les *« deep tech »* (IA, calcul à haute performance, technologies quantiques, chaîne de blocs et capacités en nuage sécurisées pour l'ensemble de l'Europe). Elle dévoilera au 2e trimestre de 2020 ses stratégies en matière de technologies quantiques et de chaînes de blocs, tandis que le règlement EuroHPC[13] sur le calcul à haute performance sera révisé.

4. Une transformation numérique respectueuse du Pacte vert

Le Pacte vert a été récemment présenté par la Commission[14]. « En tant que puissants vecteurs de la transition vers la durabilité, les solutions numériques peuvent faire progresser l'économie circulaire, soutenir la décarbonation de tous les secteurs et réduire l'empreinte environnementale et sociale des produits commercialisés dans l'UE. Ainsi, les solutions numériques peuvent apporter d'immenses avantages à des secteurs clés tels que l'agriculture de précision, les transports et l'énergie, en vue d'atteindre les ambitieux objectifs de durabilité du Pacte vert pour l'Europe ».

La Commission rappelle que le secteur des TIC doit connaître sa propre transformation écologique. Son empreinte écologique est

13. Règlement (UE) 2018/1488 du Conseil du 28 septembre 2018.

14. COM(2019) 640 final du 11 décembre 2019 : https://ec.europa.eu/info/sites/info/files/european-green-deal-communication_fr.pdf

importante. Selon le Forum mondial de l'énergie, on estime sa part de la consommation d'électricité mondiale dans une fourchette de 5 à 9 %, et à plus de 2 % de toutes les émissions[15].

Des initiatives doivent conduire à un objectif de neutralité climatique des centres de données (*data centers*) au plus tard en 2030, ainsi qu'à des mesures de transparence sur l'empreinte environnementale des opérateurs de télécommunications.

Les solutions numériques, et notamment l'utilisation des données, doivent permettre une approche totalement intégrée du cycle de vie, de la conception jusqu'aux produits finaux et à la fin de vie de ceux-ci, en passant par l'approvisionnement en énergie, en matières premières et en autres intrants. Par exemple, en cernant avec précision les lieux et les moments où le courant électrique est le plus nécessaire, il est possible d'accroître l'efficacité énergétique et de réduire la consommation de combustibles fossiles. Les modes de conception, d'achat, de consommation et de recyclage du matériel informatique sont également importants. Au-delà des exigences d'efficacité énergétique de l'écoconception, il faut, pour la Commission, que la gestion des équipements TIC devienne totalement circulaire : les produits doivent être conçus pour durer plus longtemps, être correctement entretenus et faciles à désassembler et à recycler. On rappelle que la Directive 2002/96/CE prévoit la valorisation obligatoire des déchets d'équipements électriques et électroniques (DEEE) mais qu'« en Europe, six déchets électroniques sur dix ne sont pas répertoriés dans les registres de recyclage et disparaissent donc du circuit légal. Autrement dit, ces

15. Between 10 and 20% of electricity consumption from the ICT sector in 2030 ?, *enerdata.net*, 9 août 2018. Disponible sur : https://www.enerdata.net/publications/executive-briefing/expected-world-energyconsumption-increase-from-digitalization.html

déchets prennent un chemin détourné qui peut inclure un enfouissement sauvage dans le pays d'origine, ou bien une exportation à l'étranger. Les personnes qui travaillent dans ce secteur ont une espérance de vie très faible ; on trouve rarement des personnes de plus de 35/40 ans qui travaillent dans ce domaine[16]». Selon un rapport du Programme des Nations Unies pour l'environnement (PNUE), publié le 12 mai 2015, de 60 à 90 % des déchets électroniques échappent aux filières de traitement et sont vendus ou enfouis en toute illégalité. Il faut donc rendre indissociables la transformation numérique et les exigences environnementales. Le progrès des uns ne doit pas faire le malheur des autres.

16. C. Salvoch et A. Pirot, *Magazine de la Diplomatie*, 2019.

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

AVRIL
2020

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

Par le Gal d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE JUDICIAIRE

Recel de fichiers faisant l'apologie du terrorisme

La combinaison des articles 321-1 et 421-5 du Code pénal soulève des difficultés quant à la motivation de l'auteur. Après avoir eu des certitudes, illustrées notamment par l'arrêt du 7 janvier 2020 commenté ci-dessous, la Cour de cassation a aujourd'hui des doutes dont témoigne la question prioritaire de constitutionnalité, objet de son arrêt du 24 mars 2020.

Les certitudes

Cour de cassation, Ch. criminelle n° 2789 (19-80.136), M.X, 7 janvier 2020

Le téléchargement volontaire de fichiers faisant l'apologie du terrorisme est condamnable si est caractérisée, en la personne du receleur, son adhésion à l'idéologie exprimée dans de tels fichiers.
Autorisée par le juge des libertés et de la détention, la visite d'un véhicule et au domicile où réside M.X., permet de découvrir, dans son ordinateur portable et dans ses deux téléphones mobiles, de nombreux documents et enregistrements faisant l'apologie d'actes de terrorisme.
En première instance, en vertu des dispositions des articles 321-1 et 421-2-5 du Code pénal, le tribunal correctionnel le condamne à 5 ans d'emprisonnement, dont un an avec sursis et mise à l'épreuve, ainsi qu'à une interdiction de séjour en Moselle de cinq ans et à la confiscation des scellés.

Article 321-1

« Le recel est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit.
Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit.
Le recel est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende. »

Article 421-2-5

« Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne.
Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

Le condamné fait appel sans succès. Il se pourvoit en cassation en arguant que le délit d'apologie d'actes de terrorisme réprime l'expression d'une opinion présentant l'acte terroriste sous un jour favorable et constitue un abus dans la liberté d'expression. Il ajoute dans son moyen que le seul fait de détenir un support dans lequel est exprimée cette opinion ne peut être qualifié de recel. Qu'en le

condamnant du chef de recel d'apologie d'actes de terrorisme pour avoir détenu des fichiers informatiques dans lesquels des tiers faisaient l'apologie d'actes de terrorisme, au seul motif qu'il avait connaissance de leur nature frauduleuse et illicite, la Cour d'appel a porté une atteinte non nécessaire et disproportionnée à son droit de recevoir des informations ou des idées, en violation notamment des articles 6, 7 et 10 de la Convention européenne des droits de l'Homme.

La Cour de cassation lui donne tort. Elle rappelle à titre liminaire que la condamnation prononcée n'est compatible avec l'article 10 de la Convention européenne des droits de l'Homme que si est caractérisée, en la personne du receleur, son adhésion à l'idéologie exprimée dans de tels fichiers. Elle constate que le comportement de M. X. démontre une certaine adhésion aux propos apologétiques. « La multiplicité, la diversité et le caractère volontaire de la sélection des documents téléchargés excluent qu'il ait pu agir de bonne foi par simple curiosité, quête spirituelle ou parce qu'il se retrouvait dans une situation de détresse psychologique, matérielle et familiale ainsi qu'il le prétend. »

Le doute de la Cour de cassation

Mais la Cour de cassation a des doutes. L'infraction de recel d'apologie du terrorisme, résultant de la combinaison des articles 321-1 et 421-2-5 du Code pénal, selon la portée que lui donne l'interprétation jurisprudentielle constante de la Cour de cassation (cf. Crim. 7 janvier 2020 ci-dessus), n'a pas déjà été déclarée conforme à la Constitution dans les motifs et le dispositif d'une décision du Conseil constitutionnel.

Par un arrêt du 24 mars 2020 (n°782 (19-86.706), la Chambre criminelle de la Cour de cassation a saisi le Conseil constitutionnel

par une question prioritaire de constitutionnalité (QPC) ainsi rédigée :
« Les dispositions combinées des articles 321-1 et 421-2-5 du code pénal, telles qu'interprétées par la jurisprudence de la Cour de cassation, en ce qu'elles incriminent, sous la qualification de recel d'apologie du terrorisme, la consultation de sites internet faisant l'apologie du terrorisme, ou la possession d'un support informatique ou numérique sur lequel serait téléchargé le produit d'une telle consultation, sont-elles contraires aux droits et libertés que la Constitution garantit et, plus précisément, au principe de la liberté d'opinion et de communication garanti par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, et méconnaissent-elles l'autorité de la chose jugée des décisions du Conseil constitutionnel ? »

La Cour de cassation estime (cf. *supra* arrêt du 7 janvier) que le recel de fichiers ou de documents apologétiques notamment issus de la consultation de sites à caractère terroriste peut être incriminé si est au moins caractérisée, en la personne du receleur, une adhésion à l'idéologie exprimée dans de tels fichiers. Elle demande donc au Conseil constitutionnel d'apprécier si son interprétation est susceptible de porter une atteinte disproportionnée à la liberté d'expression et de communication.
Le Conseil a eu à se prononcer à deux reprises sur la consultation habituelle des sites provoquant au terrorisme ou en en faisant l'apologie. Par décision n° 2016-611 QPC du 10 février 2017, il a censuré les dispositions de l'article 421-2-5-2 du Code pénal, dans sa rédaction issue de la loi du 3 juin 2016, en considérant qu'elles portaient à l'exercice de la liberté de communication une atteinte qui n'est pas nécessaire, adaptée et proportionnée. En outre, comme il l'a rappelé dans sa décision n° 2017-682 QPC du 15

décembre 2017, censurant la deuxième version de l'article incriminé, l'intention terroriste de l'auteur de l'infraction doit être établie par une adhésion à l'idéologie véhiculée par les sites en question.
Dans son arrêt du 7 janvier, la Cour de cassation a bien relevé un comportement indiquant une adhésion aux propos apologétiques.
Le Conseil constitutionnel a fixé au 23 avril la date limite des demandes en intervention. La décision devrait être rendue avant le 25 juillet 2020.

JURISPRUDENCE ADMINISTRATIVE

Le droit à l'oubli sur le web

Conseil d'État, section du contentieux, 10ème et 9ème chambres réunies, 27 mars 2020, GOOGLE Inc./CNIL

Le « droit à l'oubli » est un droit relatif qui ne s'applique qu'aux extensions européennes des noms de domaine. Les moteurs de recherche n'ont pas l'obligation de déréférencer sur la totalité des noms de domaine.

Le droit au déréférencement – ou « droit à l'oubli » – est une des conséquences de l'arrêt CJUE du 13 mai 2014, Google Spain et Google (C131/12). S'il ne fait pas disparaître le document que le plaignant estime contraire à sa vie privée, il supprime les liens vers les pages web qu'offre le moteur de recherche. Conformément au règlement 2016/679 (art. 17 du RGPD), ce droit au déréférencement est dénommé « droit à l'effacement » ou « droit à l'oubli ».
Le Conseil d'État a été saisi d'une requête de la société Google Inc. tendant à l'annulation de la délibération n° 2016-054 du 10 mars 2016 par laquelle la formation restreinte de la Commission

nationale de l'informatique et des libertés (CNIL) a prononcé à son encontre une sanction, rendue publique, de 100 000 euros. Par une décision du 19 juillet 2017, statuant au contentieux, il a sursis à statuer jusqu'à ce que la Cour de justice de l'Union européenne se soit prononcée, notamment sur la question de savoir si le « droit au déréférencement », tel que consacré par la CJUE dans son arrêt précité, doit être interprété en ce sens que l'exploitant d'un moteur de recherche est seulement tenu, lorsqu'il fait droit à une demande de déréférencement, de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur sur le nom de domaine correspondant à l'État où la demande est réputée avoir été effectuée ou, plus généralement, sur les noms de domaine du moteur de recherche qui correspondent aux extensions nationales de ce moteur pour l'ensemble des États membres de l'Union européenne.

La Cour de justice de l'Union européenne (CJUE) a répondu au Conseil d'État par son arrêt C-507/17 du 24 septembre 2019 (voir veille juridique n° 81 d'octobre 2019, p. 17-23). Elle a considéré que « lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement, il est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur, mais sur les versions de celui-ci correspondant à l'ensemble des États membres, et ce, si nécessaire, en combinaison avec des mesures qui, tout en satisfaisant aux exigences légales, permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens qui font l'objet de cette demande ».

Il appartenait donc au Conseil d'État de reprendre l'examen du litige qui opposait Google et la CNIL. Le Conseil d'Etat a jugé « qu'il ne

résulte, en l'état du droit applicable, d'aucune disposition législative qu'un tel déréférencement pourrait excéder le champ couvert par le droit de l'Union européenne pour s'appliquer hors du territoire des États membres de l'Union européenne ». Il a donc donné raison à Google.
La territorialité du déréférencement consacre l'absence d'extraterritorialité du droit européen. Elle n'interdit pas la procédure du géoblocage qui empêche l'accès à un contenu depuis le territoire de l'Union en fonction de l'adresse IP d'un ressortissant d'un État membre.

Cette relativité *rationae loci* se double d'une relativité *rationae personae*. Par 13 décisions du 6 décembre 2019, le Conseil d'État a appliqué les principes, définis par l'autre arrêt CJUE (Grande chambre), du 24 septembre 2019[1], qui fixent le cadre dans lequel un exploitant de moteur de recherche doit, sous le contrôle de la CNIL, appliquer le droit au déréférencement.
Un litige opposait quatre personnes à la CNIL. En cause, quatre décisions de cette dernière refusant de mettre en demeure Google LLC de procéder à des déréférencements de divers liens inclus dans la liste de résultats, affichée à la suite d'une recherche effectuée à partir de leur nom, et menant vers des pages web publiées par des tiers. Google, saisi en premier, avait refusé le déréférencement, conforté dans sa décision par la position prise par la CNIL. Les motifs des quatre plaignants étaient différents : montage satirique avec allusions à une relation intime avec un maire, article du journal *Libération* évoquant des responsabilités au sein de « l'Église de scientologie », mention d'une mise en examen dans une procédure

1. C-136/17, GC, AF, BH, ED/ Commission nationale de l'informatique et des libertés (CNIL).

judiciaire s'étant achevée par un non-lieu, articles de *Nice-Matin* et du *Figaro* sur une condamnation pour agression sexuelle sur mineurs de quinze ans.

Les plaignants avaient saisi le Conseil d'État pour contester la décision négative de la CNIL. Dans tous les cas – ce qui explique leur jonction – la question des données dites « sensibles » était posée. Le Conseil d'État avait sursis à statuer et adressé une demande de décision préjudicielle à la CJUE portant sur l'interprétation de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (texte alors en vigueur et remplacé depuis par le RGPD).

La CJUE avait ainsi répondu : un moteur de recherche est responsable d'un traitement de données à caractère personnel. Il n'est pas responsable des données mises en ligne sur les pages web mais il doit, en raison de leur référencement, respecter les exigences de la directive 95/46 – aujourd'hui RGPD – notamment en ce qui concerne le droit à la vie privée. Il doit faire droit aux demandes relatives aux « données sensibles », sous réserve des exceptions prévues et en respectant un principe de proportionnalité entre les droits du demandeur et ceux de l'internaute. Les données relatives aux procédures judiciaires relèvent des catégories « infractions » et « condamnations pénales ». Si elles sont maintenues au titre de la liberté d'information des internautes, les résultats doivent être aménagés par le moteur de recherche de telle sorte que l'image globale qui résulte du référencement reflète la situation actuelle (par ex. l'acquittement doit apparaître avant les poursuites).

C'est dans ce contexte que le Conseil d'État a posé les principes à

l'occasion de 13 décisions du 6 décembre 2019.

Les principes posés par le Conseil d'État

Il convient tout d'abord de rappeler qu'un particulier doit saisir l'exploitant du moteur de recherche lorsqu'il désire obtenir le déréférencement de liens vers des pages web, publiées par des tiers, qui contiennent des données à caractère personnel le concernant, et qui figurent parmi les résultats affichés en réponse à une recherche portant sur son nom. En cas de refus, il peut saisir soit le juge judiciaire[2], soit la Commission nationale de l'informatique et des libertés (CNIL) pour qu'elle ordonne à cet exploitant de procéder au déréférencement des liens en cause. Si la CNIL rejette cette demande, le contentieux peut être porté directement devant le Conseil d'État, qui se prononce en tenant compte des circonstances et du droit applicable à la date à laquelle il statue.

Pour le Conseil d'État, s'appuyant sur la récente jurisprudence de la CJUE, le déréférencement d'un lien associant au nom d'un particulier une page web contenant des données personnelles le concernant est un droit. Ce droit à l'oubli n'est pas cependant absolu. Une balance doit être effectuée entre le droit à la vie privée du demandeur et le droit à l'information du public. L'arbitrage entre

2. Tribunal de grande instance de Paris, ordonnance de référé du 10 février 2017, M.X/Google France et Google Inc. Saisine de la justice sur la base de l'article 809 du Code de procédure civile à propos d'un article faisant état d'une condamnation pénale. L'autorité judiciaire peut prescrire en référé ou sur requête, aux hébergeurs ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne (8 du I de l'art. 6 de la loi pour la confiance dans l'économie numérique).

ces deux libertés fondamentales dépend de la nature des données personnelles.

Trois catégories de données personnelles sont concernées : les données sensibles, les données pénales, les données touchant la vie privée sans être sensibles. La protection relative aux deux premières catégories est la plus élevée : il ne peut, dans ce cas, être légalement refusé de faire droit à une demande de déréférencement que si l'accès aux données sensibles ou pénales à partir d'une recherche portant sur le nom du demandeur est « strictement nécessaire à l'information du public ».

Pour se déterminer, la CNIL doit mettre en balance les trois paramètres principaux énoncés par le Conseil d'État :
- les caractéristiques des données personnelles en cause : leur nature, leur contenu, leur caractère plus ou moins objectif, leur exactitude, leur source, les conditions et la date de leur mise en ligne ainsi que les répercussions de leur référencement pour l'intéressé ;
- le rôle social du demandeur : sa notoriété, son rôle dans la vie publique et sa fonction dans la société – ce qui permet de mieux cerner l'intérêt du public à accéder à l'information en réponse à une recherche portant sur le nom de l'intéressé ;
- les conditions d'accès de l'information en cause : s'il est possible d'y accéder facilement à partir d'une recherche portant sur des mots-clés ne comportant pas le nom de l'intéressé, le droit à la liberté d'information apparaîtra moins affecté par un éventuel déréférencement. Par ailleurs, si l'intéressé a, de lui-même, rendu ces informations publiques, l'atteinte à la vie privée qu'il allègue apparaîtra en principe moins caractérisée.

Mais les conditions sont plus restrictives pour les données sensibles et les données pénales.

L'application aux données dites sensibles

Ce sont les données les plus intrusives dans la vie d'une personne comme celles concernant sa santé, sa vie sexuelle, ses opinions politiques, ses convictions religieuses, etc. Ces données sensibles, définies par l'articles 9 du RGPD, sont reprises par l'article 6 de la loi n° 78-17 du 6 janvier 1978. Aux termes de cet article, « il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». Le référencement est une forme de traitement de données à caractère personnel et relève donc du RGPD.

Pour se déterminer, la CNIL doit s'appuyer sur les trois paramètres énoncés ci-dessus. Compte tenu de l'ingérence particulièrement grave dans la vie privée de la personne, le Conseil d'État resserre les conditions permettant à la CNIL de refuser de mettre en demeure l'exploitant de moteur de recherches de faire droit à une demande de déréférencement. Il exige, comme cela a été dit *supra*, que l'accès à l'information litigieuse à partir d'une recherche portant sur le nom du demandeur soit « strictement nécessaire à l'information du public ».

Il fait l'application de ce principe dans plusieurs arrêts du 6 décembre.

Ainsi les informations relatives à une relation extraconjugale entretenue avec un haut dirigeant d'un pays étranger, contenues sur des pages web et relatives à une personne qui y joue un rôle très important dans la vie économique et sociale, ne sont pas strictement nécessaires à l'information du public et doivent être déréférencées (arrêt du 6 décembre, n° 395335). Le déréférencement peut être demandé par l'auteur d'un roman autobiographique pour des liens menant vers des sites qui, en décrivant l'œuvre, révèlent son orientation sexuelle. L'information a certes été manifestement rendue publique par l'intéressé, mais celui-ci n'exerce plus d'activités littéraires. Pour le Conseil d'État, les répercussions de ce référencement sur l'intéressé excèdent l'intérêt prépondérant du public à accéder à cette information à partir de son nom, ce d'autant plus que cette dernière peut être facilement obtenue via d'autres mots-clés (arrêt du 6 décembre, n° 409212). Enfin, un particulier est fondé à demander le déréférencement de liens menant vers un article de presse faisant état de son ancienne appartenance à « l'Eglise de scientologie », alors même que ces données doivent être regardées comme ayant été manifestement rendues publiques par l'intéressé compte tenu des responsabilités importantes qu'il a exercées au sein de cette organisation. L'ancienneté des faits, leur caractère non actualisé, et les répercussions de ce référencement sur la vie de l'intéressé justifient que le droit au respect de la vie privée prévale sur l'intérêt prépondérant du public, qui peut du reste accéder par d'autres moyens à ces informations (arrêt du 6 décembre, n° 393769).

L'application du droit au déréférencement par le juge judicaire

Le juge judiciaire, par un arrêt de la chambre civile de la Cour de

cassation du 27 novembre 2019[3], a eu également l'occasion de se prononcer sur les déréférencements après l'arrêt CJUE (C-507/17) du 24 septembre 2019.

En l'espèce, un expert-comptable, commissaire aux comptes, avait demandé en référé d'obliger la société Google LLC, exploitante du moteur de recherche Google, de supprimer des liens le concernant. Par un jugement du tribunal correctionnel de Metz, du 17 novembre 2011, le plaignant avait été condamné à quatre mois d'emprisonnement avec sursis et 20 000 euros d'amende pour escroquerie et tentative d'escroquerie avec, en outre, une obligation de payer une certaine somme à l'administration fiscale. *Le Républicain lorrain* en avait rendu compte sur son site Internet, les 18 novembre 2011 et 15 novembre 2013. Ces articles, archivés sur le site du journal, étaient toujours accessibles à partir de ses nom et prénom sur le moteur de recherche Google. Google a refusé de déréférencer.
Pour motiver son pourvoi devant la Cour de cassation, le plaignant considère que son droit à l'oubli prévaut sur l'intérêt du public à accéder à l'information. Il conteste l'arrêt de la Cour d'appel de Paris qui, pour exclure l'existence du trouble manifestement illicite dont il se plaint, évoque la référence à une infraction pénale qui, bien que commise dans le cadre de sa sphère privée, demeure pertinente au regard de sa profession.
La Cour de cassation applique l'arrêt de la CJUE du 24 septembre 2019 (voir *supra*) qui a dit pour droit que, lorsque l'exploitant d'un moteur de recherche est saisi d'une demande de déréférencement portant sur un lien vers une page web sur laquelle des données à caractère personnel relevant des catégories particulières (cas des

3. Cass. 1ère Civ., 27 novembre 2019, Pourvoi n° 18-14675.

infractions pénales) sont publiées, celui-ci doit vérifier, au titre des motifs d'intérêt public, si l'inclusion de ce lien dans la liste de résultats s'avère strictement nécessaire pour protéger la liberté d'information des internautes potentiellement intéressés, consacrée à l'article 11 de cette Charte. Il doit prendre sa décision sur la base de tous les éléments pertinents du cas d'espèce en tenant compte de la gravité de l'ingérence dans les droits fondamentaux de la personne concernée au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

La Cour de cassation considère qu'une juridiction, saisie d'une demande de déréférencement portant sur des données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté, doit vérifier, de façon concrète, si l'inclusion du lien litigieux dans la liste des résultats répond à un motif d'intérêt public important, tel que le droit à l'information du public, et si elle est strictement nécessaire pour assurer la préservation de cet intérêt. La Cour d'appel de Paris n'ayant pas procédé à cette vérification, la Cour de cassation casse son arrêt du 6 décembre 2017.

Par le Lieutenant Océane GERRIET

Le tribunal administratif de Marseille a tranché : il n'y aura pas de reconnaissance faciale dans les lycées[1]

Dans un jugement en date du 28 février 2020, le TA de Marseille confirme la position de la CNIL et annule la délibération du conseil régional de PACA en date du 14 décembre 2018 par laquelle il avait autorisé la mise en place d'une expérimentation de la reconnaissance faciale dans deux lycées, l'un à Nice et l'autre à Marseille, car elle ne respecte pas les exigences du Règlement général sur la protection des données (RGPD)[2].

Une technologie engendrant des questionnements...

Jadis, l'utilisation de la technologie biométrique à des fins d'authentification appartenait à l'imaginaire de la science-fiction (bien que certains éléments préfèrent les « multi-pass »). Parmi les données biométriques les plus connues figurent les empreintes rétiniennes et digitales, ainsi que la reconnaissance faciale. Bien entendu, ces données biométriques sont utilisées depuis longtemps pour l'identification judiciaire et criminelle mais c'est leur utilisation à des fins de reconnaissance spatiale et d'authentification qui

1. Tribunal administratif de Marseille, 9ème ch., jugement du 27 février 2020, *legalis.net*, 27 février 2020. Disponible sur : https://www.legalis.net/jurisprudences/tribunal-administratif-de-marseille-9eme-ch-jugement-du-27-fevrier-2020/

2. Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

questionne au regard notamment de leurs finalités[3]. L'ensemble de nos smartphones proposent d'ores et déjà de s'authentifier à l'aide d'une empreinte digitale, d'un scan de la rétine ou de la reconnaissance faciale et pourtant, qui s'interroge sur la finalité et les méthodes de stockage de ces données ? Mais « un grand pouvoir implique de grandes responsabilités », de surcroît lorsque c'est l'État ou les collectivités territoriales qui en sont le détenteur. Ainsi, lorsque la région PACA décide d'expérimenter la reconnaissance faciale dans des lycées, de nombreuses associations s'insurgent et c'est ainsi que le tribunal administratif (TA) de Marseille clôt cette (première) bataille juridique.

Et pourtant ! Lors de son annonce en 2018, la région PACA s'imposait comme précurseur dans le domaine. L'objectif était simple : garantir et renforcer la sécurité au sein des lycées, tout en fluidifiant la phase de contrôle. Cette initiative s'inscrivait alors dans le prolongement du virage technologique voulu par la région et dont la ville de Nice était le symbole. Cette dernière compte un parc important de caméras de vidéosurveillance et a déjà expérimenté l'utilisation de la reconnaissance faciale pour son carnaval. À cette occasion, la CNIL avait demandé à faire preuve de vigilance en raison d'un cadre juridique national peu étoffé et de la sensibilité inhérente aux données biométriques. Pour mémoire, **l'article 9 du RGPD** consacre l'interdiction de principe du traitement des « données biométriques aux fins d'identifier une personne physique (…) ». En outre, la CNIL avait également rappelé que si l'objet d'un tel traitement consiste à prévenir et/ou détecter des infractions pénales, des enquêtes, des poursuites ou l'exécution de sanctions

3. LEPLÂTRE, Simon, En Chine, des citoyens sous surveillance, *lemonde.fr*, 18 juin 2018 [Consulté le 31 mars 2020]. Disponible sur : https://www.lemonde.fr/economie/article/2018/06/15/en-chine-des-citoyens-sous-surveillance_5315522_3234.html

pénales, ce n'est plus le RGPD qui s'applique mais la directive dite Police/Justice, laquelle impose, notamment, l'édiction d'une norme législative ou réglementaire pour régir un tel dispositif. En tout état de cause, s'agissant du cas d'espèce, l'objectif est de contrôler les accès aux établissements scolaires, ainsi c'est bien le RGPD qui s'applique. Par une délibération en date du 14 décembre 2018, la région PACA a approuvé une convention tripartite entre la région, les lycées et une société privée (américaine de surcroît) dont l'objet a trait « à la mise en place d'un dispositif de contrôle d'accès par comparaison faciale et de suivi de trajectoire ». Par ladite délibération, elle autorise son président à signer cette convention mais également à lancer l'expérimentation. Par une requête introduite le 14 février 2019, de nombreuses associations demandent l'annulation de cette décision en excipant son illégalité externe et interne. Elles évoquent notamment l'incompétence de la région puisque seuls les chefs d'établissement sont responsables de la sécurité à l'entrée des lycées, ainsi que l'incompatibilité de la mesure avec les dispositions des articles 5 et 9 du RGPD, dès lors que « les finalités avancées pour justifier le traitement en cause ne sont ni explicites, ni légitimes, (…) ni adéquates, ni pertinentes et qu'elles sont, en tout état de cause, manifestement excessives au regard des finalités (…) ».

… et une première réponse juridique !

D'emblée, le TA accueille le moyen d'incompétence au motif que, conformément à l'article L. 214-6 du Code de l'éducation, les « missions d'encadrement et de surveillance » ne relèvent pas de la compétence de la région, même en présence d'un accord des chefs d'établissement (§7).
Ensuite, le TA précise qu'il existe des exceptions à l'interdiction du

traitement des données biométriques. Celles-ci sont précisément définies à **l'article 9 du RGPD** et elles sont, il faut l'admettre, restrictives. La première des exceptions concerne le cas où la personne concernée par le traitement a donné son **« consentement explicite »** pour « une ou plusieurs finalités spécifiques » et que le droit de l'Union ou le droit d'un État membre n'y fait pas obstacle (**article 9.2.a du RGPD**). Pour mémoire, le RGPD définit le consentement[4] comme « toute manifestation de volonté, libre, spécifique, éclairé et univoque » (**article 4.11 du RGPD**). Dans ses lignes directrices sur le consentement, le comité européen de la protection des données estime qu'en cas de lien de subordination, ou « de déséquilibres de rapports de forces », le consentement ne peut pas être « libre », dès que « tout élément de contrainte, de pression ou d'incapacité d'exercer un véritable choix » est présent. Le **considérant 43 du RGPD** souligne également qu'il y a un déséquilibre manifeste lorsque le « responsable du traitement est une autorité publique ». Il faut donc éviter d'utiliser cette base juridique pour un tel traitement ou prévoir, *a minima*, des garanties suffisantes. En l'espèce, la juridiction ne pouvait donc que constater que **« la seule signature d'un formulaire, alors que le public visé se trouve dans une relation d'autorité »** n'apporte pas les garanties suffisantes à l'obtention d'un consentement « libre et éclairé », de sorte que le moyen soulevé sur ce point doit être accueilli.

En outre, **l'article 9.g) du RGPD** prévoit également l'autorisation de traiter des données biométriques si cela est nécessaire « pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif

4. CNIL, Lignes directrices du CEPD, *cnil.fr* [Consulté le 24 mars 2020]. Disponible sur : https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

poursuivi ». Or, le TA souligne que la région PACA ne démontre pas que le traitement de telles données sensibles se fonde sur un motif d'intérêt public légalement défini. Les magistrats administratifs soulignent également que la région ne justifie pas, par ailleurs, que ce traitement puisse entrer dans l'une des exceptions énumérées par **l'article 9 du RGPD**.

Par ailleurs, il n'est pas démontré que le traitement de ces données biométriques soit l'ultime recours et que les finalités poursuivies ne peuvent pas être « atteintes de manière suffisamment efficace » par d'autres moyens tels que « des contrôles par badges ». Sur ce point, il convient de lire ce considérant à la lumière de **l'article 5 du RGPD** qui rappelle que « les données traitées doivent être (…) **c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées** ». Le RGPD pose le principe de « minimisation des données » qui impose de traiter les données strictement nécessaires à la finalité poursuivie. Ce qui n'est pas le cas de l'espèce, d'autres moyens pouvant être mis en œuvre pour veiller à la sécurité des accès de l'établissement. Par conséquent, le TA conclut, sans qu'il y ait besoin d'examiner les autres moyens, que les requérants sont fondés à demander l'annulation de la délibération, en tant qu'elle a lancé l'expérimentation du dispositif de reconnaissance faciale. En ce sens, les magistrats confirment l'avis de la CNIL rendu en octobre 2019[5]. Cet avis avait été sollicité par la région et il était déjà sans appel. Elle concluait à l'absence de légalité d'un tel dispositif qui est **« contraire aux principes de proportionnalité et de minimisation des données posés par le RGPD »**. D'une part, elle

5. CNIL, Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position, *cnil.fr*, 29 octobre 2019 [Consulté le 24 mars 2020]. Disponible sur : https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

rappelait que les données biométriques sont d'une sensibilité particulière, de surcroît lorsqu'il s'agit d'un public vulnérable tel que des mineurs. D'autre part, elle estimait que d'autres mesures, moins intrusives, permettent d'atteindre les objectifs de la région.

Ce jugement rendu par le TA de Marseille arrive peu de temps après que la CNIL a appelé de ses vœux[6] un débat sur l'ensemble des éléments juridiques, techniques et éthiques en matière de reconnaissance faciale. Certains députés ont même demandé d'ériger un moratoire[7]. En tout état de cause, les entreprises privées, et les GAFAM en tête, disposent déjà de technologies performantes qu'ils expérimentent dans leur offre de service, de sorte qu'il est important que la France se positionne sur ce sujet pour offrir un cadre juridique sécurisé et sécurisant pour tous.

6. CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, *cnil.fr*, 15 novembre 2019 [Consulté le 24 mars 2020]. Disponible sur : https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux

7. TRIBUNE, COLLECTIF, Reconnaissance faciale : l'urgence d'un moratoire, *liberation.fr*, 17 décembre 2019 [Consulté le 24 mars 2020]. Disponible sur : https://www.liberation.fr/debats/2019/12/17/reconnaissance-faciale-l-urgence-d-un-moratoire_1769794

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

MAI 2020

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

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

Par le G^al^ d'armée (2S) Marc Watin-Augouard

Tracing but not Tracking

(article publié par *La Tribune* le 12 mai 2020)

Du *tracking tracking* au *tracing*, seule une lettre fait apparemment la différence. En vérité le fossé est béant ! D'un côté, un suivi géolocalisé des personnes, une atteinte profonde à la vie privée, de l'autre un souci de concilier liberté et sécurité sanitaire, deux principes à valeur constitutionnelle.

Hier, nous critiquions, à juste titre, l'usage des technologies numériques « à la chinoise » afin de capter, mesurer, évaluer, sanctionner le comportement des citoyens, en soulignant le caractère orwellien d'un tel dispositif, comme s'il s'agissait d'un modèle impossible à transposer dans les vraies démocraties. Aujourd'hui, ce modèle frappe à notre porte.

Le débat sur l'application « StopCovid » divise. La communauté médicale, Académie de médecine et Conseil national de l'ordre des médecins en tête, se montre plutôt favorable à ce dispositif d'accompagnement d'un déconfinement progressif, dès lors qu'il vient compléter un dispositif d'ensemble. Les personnalités politiques ont des opinions partagées, y compris au sein de la majorité. Les spécialistes de la cybersécurité et de la protection des données se répartissent entre un « oui mais ! » (Conseil national de l'informatique et des libertés – CNIL – , Conseil national du numérique) et un « non assurément ! » (Quadrature du Net en particulier). Le sujet est suffisamment délicat pour que le débat à l'Assemblée nationale, prévu le 28 avril 2020, ait été reporté par le Premier ministre. Outre les questions relatives à son efficacité, « StopCovid » appelle des interrogations sur les modalités de traitement des données à caractère personnel les plus sensibles : les

données de santé. Leur traitement est particulièrement encadré par le Règlement général sur la protection des données (RGPD), sans pour autant interdire aux autorités d'agir pour des motifs d'intérêt public dans le domaine de la santé lorsqu'il s'agit d'assurer la protection contre les menaces transfrontalières graves pesant sur elle.

Il est acquis qu'une telle application, si elle était autorisée, devrait respecter un cahier des charges strict encadré par la CNIL dans son avis du 24 avril 2020. « StopCovid » doit être limité dans le temps et dans sa finalité. Il doit être un « suivi de contacts » et non un suivi des personnes exposées ou diagnostiquées positives au virus. La technologie « Bluetooth », permettant d'évaluer la proximité entre deux ordiphones (bien qu'elle n'ait pas été conçue pour évaluer des distances) évite de recourir à une technologie de géolocalisation. Utilisée sur la base du volontariat, sans contrepartie aucune positive ou négative, elle devrait minimiser toute identification directe ou indirecte des personnes qui y auraient recours. La technologie ne doit faire remonter au serveur central que les pseudonymes générés par les applications associées aux personnes avec lesquelles un individu infecté a été en contact, et non le pseudonyme de ce dernier.

« StopCovid » est le fruit d'un travail en urgence dans le cadre du *« Pan European Privacy Proximity tracing »* (PEPP-PT), projet européen de recherche rassemblant plus de 130 scientifiques de haut niveau en provenance de huit pays, dont la France, l'Allemagne et la Suisse, « dont le but principal est de permettre le développement de solutions de suivi de contacts respectueuses des normes européennes en matière de protection des données, de vie privée et de sécurité, dans le cadre d'une réponse plus globale à la pandémie ». Le protocole est appelé ROBERT (*ROBust and privacy-presERving proximity Tracing*) et se veut respectueux des valeurs

européennes. En France, le chef de file est l'Institut national de recherche en sciences et technologies du numérique (INRIA), conseillé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur le volet de la sécurité numérique. Un consortium s'organise, notamment autour de Capgemini, Dassault Systèmes, Inserm, Lunabee Studio, Orange, Santé Publique France et Withings.

Mais, le 26 avril 2020, l'Allemagne annonce qu'elle quitte le projet européen. Certes, chaque pays est souverain et peut donc choisir ce que bon lui semble, sachant que la santé n'entre pas dans les attributions de l'Union européenne. Il n'empêche que c'est encore un mauvais coup porté à l'unité européenne qui n'en a pas besoin en ce moment !

L'Allemagne se retourne désormais vers Apple et Google qui ont développé une technologie « décentralisée », par opposition à la centralisation-décentralisation qui caractérise ROBERT. Mais est-ce souverain d'abandonner sa souveraineté aux GAFA ? Il est vrai que nous sommes déjà dépendants d'Apple et de Google qui doivent – s'ils le veulent bien – modifier leur système d'exploitation pour permettre le fonctionnement de « StopCovid » sur les OS (*operating systems*) installés sur les ordiphones commercialisés en France et en Europe.

Cédric O, soulignant les difficultés liées à la protection de la vie privée et en termes d'interconnexion avec le système de santé, écarte les solutions proposées par les géants américains qui ne sauraient se substituer aux États dans la maîtrise du système de santé et la lutte contre le coronavirus.

Les Allemands ont fait un choix (est-il définitif ?) au nom du pragmatisme. Devions-nous les suivre, comme nous invitent à le faire certains éditorialistes, en particulier Jean-Francis Pécresse (*Les Echos*) ? La souveraineté numérique doit-elle attendre, une fois de

plus ? La crise n'est-elle pas justement l'occasion de la recouvrer ? N'est-elle pas le moment venu d'offrir « une autre voie, une autre voix » pour l'Europe ? Abandonner, c'est renoncer au développement de technologies européennes, c'est casser l'élan qui rassemble des grandes entreprises, des centres de recherche, des start-ups sur un projet qui, même s'il n'aboutit pas dans sa mise en œuvre, fera progresser une Europe numérique que la Commission appelle de ses vœux dans ses communications du 12 février et du 19 mars 2020.

Au-delà de cette question essentielle de souveraineté se trouve posée celle de la légitimité d'une technologie de *« tracing »*. Tout progrès technologique franchit plusieurs étapes dans la mise en œuvre du process : sait-on le faire (conceptuellement) ? peut-on le faire (techniquement) ? a-t-on le droit de le faire (juridiquement) ? est-il accepté (socialement) ? L'acceptabilité sociale est, en effet, une condition nécessaire. Mais il faut parfois ajouter une autre étape : celle de la politique, au sens le plus noble du terme. Dans le cas d'espèce, la technologie est au cœur d'un dilemme entre deux principes fondamentaux qui prennent racine dans notre bloc constitutionnel : la liberté et la santé. Peut-on sacrifier l'une au profit de l'autre ? Quel juste équilibre peut-on établir sous la pression d'une opinion publique qui a peur de la mort ? Peut-on choisir le temps court du « sauve comme on peut » au détriment du temps long, celui qui inscrit la liberté dans la durée ? La question est certes technique, juridique, sociologique, mais elle est d'abord politique. La politique, c'est l'art de faire des choix, parfois contre la pensée dominante. C'est à cela que l'on reconnaît les hommes d'État qui entrent dans l'Histoire ; c'est en l'oubliant que les hommes et les femmes politiques se transforment en comptables, en gestionnaires de l'instant présent, en expéditeurs des affaires courantes. L'heure est à la décision souveraine. Passée l'heure…

Le 12 mai 2020, auditionné par l'Office d'évaluation des choix scientifiques et techniques, Guillaume Poupard, directeur général de l'ANSSI, a annoncé que l'INRIA travaillait sur un nouveau protocole, DESIRE, qui concilierait les approches « centralisées » et « décentralisées ». Mais, pour l'heure, l'application demeure théorique.

Le recours aux technologies, même encadré par la loi, même contrôlé, opère qu'on le veuille ou non un glissement irréversible (bien que l'application soit supprimée après un délai) qui conduit la société vers un modèle « à la chinoise ». Avant de se lancer dans l'aventure, il convient de vérifier que toutes les autres mesures humaines sont mises en œuvre. Les technologies ne doivent pas être une réponse à nos carences.

JURISPRUDENCE CONSTITUTIONNELLE

Décision n° 2020-800 DC du 11 mai 2020 relative à la loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions

Les traitements de données à caractère personnel de nature médicale aux fins de « traçage » portent atteinte à la vie privée mais poursuivent l'objectif de valeur constitutionnelle de protection de la santé. L'article 11 de la loi renforçant les moyens de la lutte contre l'épidémie de Covid-19, par l'identification des chaînes de contamination, est globalement conforme à la Constitution mais fait l'objet de deux censures partielles et de trois réserves d'interprétation.

L'article 11 de la loi prévoit que des données à caractère personnel

concernant la santé, relatives aux personnes atteintes par le coronavirus et aux personnes ayant été en contact avec elles, peuvent être collectées, traitées et partagées, le cas échéant sans le consentement des personnes intéressées, dans le cadre d'un système d'information créé par décret en Conseil d'État et mis en œuvre par le ministre chargé de la santé. Le dispositif exclut expressément le développement ou le déploiement d'une application informatique à destination du public et disponible sur équipement mobile permettant d'informer les personnes du fait qu'elles ont été à proximité de personnes diagnostiquées positives au Covid-19 (voir *supra « Tracing or not tracing* »).

Le traitement de l'information doit reposer sur deux systèmes : le fichier du service intégré de dépistage et de prévention (SI-DEP) et le fichier « Contact Covid » de l'assurance maladie.

Le Conseil constitutionnel considère qu'une telle collecte porte atteinte à la vie privée mais qu'en adoptant les dispositions contestées, le législateur a entendu renforcer les moyens de la lutte contre l'épidémie de Covid-19, par l'identification des chaînes de contamination. Il a ainsi poursuivi l'objectif de valeur constitutionnelle de protection de la santé.

L'atteinte à la vie privée n'est pas disproportionnée, car le recours au traitement est encadré :

- Il est créé aux seules fins de lutter contre la propagation de l'épidémie de Covid-19 et pour la durée strictement nécessaire à cet objectif ou, au plus, pour une durée de six mois à compter de la fin de l'état d'urgence sanitaire. Contribuent à la finalité poursuivie l'identification des personnes infectées, l'identification des personnes présentant un risque d'infection, par la collecte des informations relatives aux contacts des personnes infectées, l'orientation des personnes infectées, et des personnes susceptibles de l'être, la surveillance

épidémiologique aux niveaux national et local, ainsi que la recherche sur le virus et les moyens de lutter contre sa propagation. Les deux dernières finalités subordonnent la collecte d'informations à la suppression des nom et prénoms des personnes, de leur numéro d'inscription au répertoire national d'identification des personnes physiques et de leur adresse, garantissant ainsi leur anonymisation ;

- Les données ne peuvent être conservées à l'issue d'une durée de trois mois après leur collecte ;
- Les données sont strictement limitées au statut virologique ou sérologique de la personne à l'égard du virus ainsi qu'à des éléments probants de diagnostic clinique et d'imagerie médicale ;
- Les agents des organismes chargés de la collecte n'ont accès qu'aux seules données nécessaires à leur intervention.

Les finalités et restrictions citées *supra* vérifient l'adéquation et la proportionnalité du dispositif.

Toutefois, le Conseil constitutionnel formule trois réserves d'interprétation :

- Sauf à méconnaître le droit au respect de la vie privée, l'anonymisation prévue pour la surveillance épidémiologique et la recherche doit également s'étendre aux coordonnées de contact téléphonique ou électronique des intéressés ;
- Le pouvoir réglementaire doit définir des modalités de collecte, de traitement et de partage des informations assurant leur stricte confidentialité et, notamment, l'habilitation spécifique des agents chargés, au sein de chaque organisme, de participer à la mise en œuvre du système d'information ainsi que la traçabilité des accès à ce système d'information ;
- Le recours à des sous-traitants, par les organismes

concourant au dispositif, implique la responsabilité et le contrôle de ces derniers, en conformité avec les exigences de nécessité et de confidentialité.

Le texte encourt cependant la censure sur un point de fond et un point de forme.
Sur le fond, est contesté le caractère trop extensif de la liste des organismes participant à la mise en place et à l'exploitation d'un traitement excluant le consentement des personnes concernées. Pour les Sages, l'implication de l'Agence nationale de santé publique, des agences régionales de santé, du service de santé des armées, des communautés professionnelles territoriales de santé, des établissements de santé, sociaux et médico-sociaux, des équipes de soins primaires, des maisons et centres de santé, des services de santé au travail, des médecins prenant en charge les personnes en cause, des pharmaciens, des dispositifs spécifiques d'appui ainsi que des laboratoires et services autorisés à réaliser les examens de biologie ou d'imagerie médicale, ouvre un large champ justifié par la masse des démarches à entreprendre pour organiser la collecte des informations nécessaires à la lutte contre le développement de l'épidémie. Mais le législateur a également inclus les organismes qui assurent l'accompagnement social des intéressés. Or, s'agissant d'un accompagnement social, qui ne relève pas directement de la lutte contre l'épidémie, rien ne justifie que la communication des données à caractère personnel traitées dans le système d'information ne soit pas subordonnée au recueil du consentement des intéressés, formalité qui n'est pas nécessaire s'agissant des organismes médicaux. Dès lors, le Conseil constitutionnel considère que leur présence dans l'énumération établie par la loi méconnaît le droit au respect de la vie privée et est donc contraire à la Constitution.

Sur la forme, le législateur a prévu que le décret d'application de la loi serait pris après avis public conforme de la Commission nationale de l'informatique et des libertés. Or, en vertu de l'article 21 de la Constitution et sous réserve de son article 13, le Premier ministre exerce le pouvoir réglementaire à l'échelon national. Ces dispositions n'autorisent pas le législateur à subordonner à l'avis conforme d'une autre autorité de l'État l'exercice, par le Premier ministre, de son pouvoir réglementaire. Dès lors, le mot « conforme» figurant à la première phrase du paragraphe V de l'article 11 est contraire à la Constitution.

Dans cette période de crise d'une particulière gravité, le Conseil constitutionnel tient compte de l'ampleur de la pandémie pour vérifier l'équilibre entre deux principes à valeur constitutionnelle qui peuvent apparaître comme antagonistes : la vie privée et la protection de la santé. Toutefois, il n'abandonne pas pour autant son rôle de censeur, la crise ne faisant pas disparaître l'État de droit.

JURISPRUDENCE ADMINISTRATIVE

Conseil d'État, Ordonnance du 18 mai 2020, Quadrature du Net, Ligue des Droits de l'Homme

L'emploi de drones pour contrôler l'exécution des mesures prises dans le cadre de l'état d'urgence sanitaire est constitutif d'un traitement de données à caractère personnel. Il est donc subordonné aux dispositions de la loi du 6 janvier 1978, sauf à modifier techniquement les appareils afin que les images ne permettent pas d'identifier les personnes.

L'association « La Quadrature du Net » et la Ligue des droits de

l'Homme ont demandé au juge des référés du tribunal administratif de Paris de suspendre l'exécution de la décision du préfet de police ayant institué, depuis le 18 mars 2020, un dispositif visant à capturer des images par drones et à les exploiter afin de faire respecter les mesures de confinement. Elles demandent au juge des référés d'enjoindre au préfet de police de cesser immédiatement, à compter du prononcé de l'ordonnance, de capter des images par drones, de les enregistrer, de les transmettre ou de les exploiter, puis de détruire toute image déjà captée dans ce contexte. Par une ordonnance n° 2006861 du 5 mai 2020, le juge des référés du tribunal administratif de Paris a rejeté leur demande en s'appuyant sur les arguments du Préfet de police. Celui-ci a fait valoir « que les images captées sont prises en utilisant un grand angle et qu'elles ne permettent donc pas l'identification d'un individu. Aucun des éléments de l'instruction ne permet de mettre en cause cette affirmation. Il ne résulte d'aucune des pièces du dossier que les services de la préfecture de police auraient utilisé les drones dans des conditions permettant d'identifier les individus au sol. Lorsqu'ils sont utilisés dans un cadre judiciaire, les appareils sont capables d'identifier les individus, mais tel n'est pas le cas dans le cadre d'emploi choisi depuis le début du confinement. Dans ces conditions, même si la préfecture de police a, par ce dispositif, procédé à la collecte, à l'enregistrement provisoire et à la transmission d'images, elle ne peut être regardée comme ayant procédé à un traitement de données à caractère personnel, au sens des dispositions précitées du règlement (UE) 2016/679, de la directive (UE) 2016/680 et de la loi du 6 janvier 1978. Il n'apparaît pas, dès lors, qu'elle aurait porté une atteinte illégale aux libertés fondamentales que sont le droit à la vie privée et le droit à la protection des données personnelles, faute notamment que les traitements en cause aient été autorisés et organisés par un texte

de droit interne ».
Le juge des référés du Conseil d'État est saisi par la voie d'appel. La Haute juridiction rappelle que l'état d'urgence sanitaire conduit les différentes autorités compétentes à prendre, en vue de sauvegarder la santé de la population, toutes dispositions de nature à prévenir ou à limiter les effets de l'épidémie. Mais ces mesures qui peuvent limiter l'exercice des droits et libertés fondamentaux doivent être nécessaires, adaptées et proportionnées à l'objectif de sauvegarde de la santé publique qu'elles poursuivent. Le droit au respect de la vie privée, qui comprend le droit à la protection des données personnelles et la liberté d'aller et venir, constitue une liberté fondamentale.

Le Conseil d'État étudie la fiche technique de la Direction de l'ordre public et de la circulation (DOPC) de la Préfecture de police, relative aux modalités d'engagement des drones lors de la surveillance du respect du confinement Covid-19 dans Paris, qui a été versée au débat contradictoire ainsi que des éléments échangés au cours de l'audience publique. Il constate que l'unité des moyens aériens de la Préfecture de police a été engagée afin de procéder à une surveillance du respect des mesures de confinement mises en place à compter du 17 mars 2020. Depuis le 18 mars 2020, un drone de la flotte des quinze appareils que compte la préfecture de police a ainsi été utilisé quotidiennement pour effectuer cette mission de police administrative. La Préfecture de police continue de recourir à ces mesures de surveillance et de contrôle dans le cadre du plan de déconfinement mis en œuvre à compter du 11 mai 2020. L'ensemble des vols sont réalisés à une hauteur de 80 à 100 mètres de façon à donner une physionomie générale de la zone surveillée, qui est filmée en utilisant un grand angle sans activation du zoom dont est doté chaque appareil. En outre, dans le cadre de cette doctrine

d'usage, les drones ne sont plus équipés d'une carte mémoire, de sorte qu'il n'est procédé à aucun enregistrement ni aucune conservation d'image. Un seul drone est utilisé à la fois. Il ne filme pas de manière continue mais seulement deux à trois heures en moyenne par jour. La mise en œuvre de ce dispositif de surveillance repose sur la mobilisation simultanée d'une équipe sur site et de personnels situés au centre d'information et de commandement de la Préfecture de police. La première est composée de trois personnes, le télépilote en charge de manier le drone, un télépilote adjoint et un agent chargé de leur protection. Le télépilote procède au guidage de l'appareil à partir de son propre écran vidéo ou en effectuant un vol à vue afin qu'il accède au site dont l'opérateur a demandé, depuis la salle de commandement, le survol. Lorsque le drone survole le site désigné, le télépilote procède à la retransmission, en temps réel, des images au centre de commandement afin que l'opérateur qui s'y trouve puisse, le cas échéant, décider de la conduite à tenir. Il peut également être décidé de faire usage du haut-parleur dont est doté l'appareil, afin de diffuser des messages à destination des personnes présentes sur le site.

La surveillance par drones n'est pas une atteinte grave et manifestement illégale aux libertés fondamentales

Pour le Conseil d'État, le recours à ces mesures de surveillance est seulement destiné à donner aux forces de l'ordre, chargées de faire respecter effectivement les règles de sécurité sanitaire, une physionomie générale de l'affluence sur le territoire parisien en contribuant à détecter, sur des secteurs déterminés exclusivement situés sur la voie ou dans des espaces publics, les rassemblements de public contraires aux mesures de restriction en vigueur pendant

la période de déconfinement. La finalité poursuivie par le dispositif litigieux n'est pas de constater les infractions ou d'identifier leur auteur mais d'informer l'état-major de la Préfecture de police afin que puisse être décidé, en temps utile, le déploiement d'une unité d'intervention sur place, chargée de procéder à la dispersion du rassemblement en cause ou à l'évacuation de lieux fermés au public, afin de faire cesser ou de prévenir le trouble à l'ordre public que constitue la méconnaissance des règles de sécurité sanitaire. Ainsi, pour la haute juridiction, la finalité poursuivie est, en particulier dans les circonstances actuelles, nécessaire pour la sécurité publique. Il est donc légitime. Un usage du dispositif de surveillance par drone effectué conformément à la doctrine d'emploi fixée par la note du 14 mai 2020 n'est pas de nature à porter, par lui-même, une atteinte grave et manifestement illégale aux libertés fondamentales.
Mais, poussant plus loin l'examen, le Conseil d'État va prendre une position contraire à celle de la Préfecture de police. Il considère, en effet, que les images prises par les drones constituent un traitement de données à caractère personnel.

La collecte des images est un traitement de données à caractère personnel

Le Conseil d'État rappelle que la directive sur les données à caractère personnel les définit comme « toute information se rapportant à une personne physique identifiée ou identifiable » et précise qu'est réputée être une «personne physique identifiable » « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques

propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Les drones dotés d'un zoom optique peuvent collecter des données identifiantes et sont dépourvus de dispositif technique permettant d'éviter, pour un autre usage, que les personnes soient identifiables. Les données recueillies sont donc des données à caractère personnel. Elles font l'objet d'un traitement qui, comme le précise la directive du 27 avril 2016, est « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ». Les drones captent, transmettent des images qui sont des données à caractère personnel. Par ce moyen, la Préfecture de police opère un traitement de données à caractère personnel qui relève des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Son article 31 impose une autorisation par arrêté du ministre compétent ou par décret, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL). Compte tenu des risques d'un usage contraire aux règles de protection des données personnelles qu'elle comporte, la mise en œuvre, pour le compte de l'État, de ce traitement de données à caractère personnel sans l'intervention préalable d'un texte réglementaire en autorisant la création et en fixant les modalités d'utilisation devant obligatoirement être respectées ainsi que les garanties dont il doit être entouré, caractérise une atteinte grave et manifestement illégale au droit au respect de la vie privée. Partant,

le Conseil d'État ordonne à la Préfecture de police de cesser de procéder aux mesures de surveillance par drone, du respect, à Paris, des règles de sécurité sanitaire applicables à la période de déconfinement tant qu'un texte réglementaire n'aura pas été pris ou que des modifications techniques n'auront pas été apportées aux appareils afin de rendre impossible l'identification des personnes filmées.

.

Par le lieutenant Océane GERRIET

Le Conseil d'État déclare conformes des recommandations relatives à l'usage des réseaux sociaux visant à assurer le respect de l'obligation de réserve

Conseil d'État, 25 mars 2020, n° 421149, Publié au recueil Lebon
Conseil d'État, 25 mars 2020, n° 411070, Publié au recueil Lebon

La Charte de déontologie des membres de la juridiction administrative ayant pour objectif de fixer des bonnes pratiques visant à garantir le respect du devoir de réserve, mais également à prémunir ses utilisateurs contre les risques des réseaux, ne méconnaît pas la liberté d'expression.

Ces deux arrêts ont trait à la Charte de déontologie des membres de la juridiction administrative, adoptée le 14 mars 2017 après avis du collège de déontologie de la juridiction administrative. D'une part, un avocat, ancien conseiller d'État honoraire, conteste la légalité de cette Charte, estimant qu'elle méconnaît le principe d'impartialité et le droit au recours effectif et que le vice-président méconnaît sa compétence, notamment en adoptant des dispositions exigeantes relatives aux recommandations quant à l'exercice de la profession d'avocat (CE, 25 mars 2020, n° 411070). D'autre part, par des requêtes introduites en 2018 et 2019, le syndicat de la juridiction administrative conteste les recommandations relatives à l'usage des réseaux sociaux (CE, 25 mars 2020, n° 421149).

Sur la légalité et la portée de la Charte

D'emblée, la juridiction rappelle que **l'article L. 131-4 du Code de justice administrative** donne compétence au vice-président pour établir une telle charte « énonçant les principes déontologiques et les bonnes pratiques propres à l'exercice des fonctions de membre de la juridiction administrative », de sorte que le moyen invoqué n'est pas fondé.

En outre, le moyen soulevé relatif à son inconstitutionnalité ne peut être qu'écarté au regard de la décision rendue par le Conseil constitutionnel le 20 octobre 2017 à la suite d'une question prioritaire de constitutionnalité dans laquelle il la déclare conforme à la Constitution. La défense estimait que cette dernière méconnaissait le principe d'impartialité des juridictions et le droit au recours effectif, car c'est le Conseil d'État lui-même qui est chargé de traiter les recours s'y afférant. Ce dernier rappelle qu'il résulte « d'un principe général de procédure qu'aucun membre d'une juridiction administrative ne peut participer au jugement d'un recours dirigé contre une décision administrative ou juridictionnelle dont il est l'auteur ou à l'élaboration de laquelle il a participé ». Cela est garanti par **l'article L. 131-9 du Code de justice administrative** imposant aux magistrats de « s'abstenir de siéger » s'ils s'estiment en situation de « conflit d'intérêts ». Sur ce point, le Conseil constitutionnel précise également que « quelles que soient les prérogatives du vice-président sur la nomination ou la carrière des membres de la juridiction administrative, **les garanties statutaires reconnues à ces derniers** (…) assurent leur indépendance à son égard » de sorte que la charte ne méconnaît pas le principe d'impartialité et de droit au recours effectif.

Ensuite, le requérant estime que la recommandation selon laquelle

les avocats, anciens membres des juridictions, ne peuvent exercer devant leur juridiction pendant 5 ans, voire 10 ans pour les plus hautes fonctions, est excessive, car elle excède la durée d'incompatibilité fixée à 3 ans par la loi du 13 juillet 1983. Cependant, le Conseil État estime que la durée recommandée par la charte n'est pas excessive, car elle vise à « préserver (…) l'indépendance, l'impartialité et le bon fonctionnement des juridictions administratives », ainsi qu'à éviter aux magistrats des mises en causes d'ordre déontologique. Sur ce point, il est intéressant de souligner que cette durée de 5 ans est similaire à celle présente dans le statut de leurs homologues de l'ordre judiciaire mais que cette durée est plus élevée que celle imposée par la Charte des juges de la Cour européenne des droits de l'Homme (qui fixe un délai de 2 ans). Ainsi, il est permis de s'interroger sur la proportionnalité de la durée de 10 ans imposée pour les plus hautes fonctions.

Enfin, s'agissant de la portée de la Charte, les magistrats rappellent qu'elle n'a pas vocation à « se substituer aux principes et dispositions textuelles, notamment statutaires, régissant l'exercice de leurs fonctions » **mais simplement « à rappeler les principes** et obligations d'ordre déontologique qui leur sont applicables » tout **en préconisant « des bonnes pratiques** propres à en assurer le respect », **« susceptibles d'être prises en compte », de sorte que la méconnaissance de ladite charte n'est pas en soi « constitutive d'un manquement disciplinaire »**. En outre, en étendant l'application de cette Charte aux anciens membres des juridictions administratives, le vice-président n'a pas méconnu l'ensemble des dispositions précitées ni commis d'erreur d'appréciation puisqu'elle ne s'applique que dans des cas précis d'« atteinte à la dignité de leurs anciennes fonctions » ou d'atteinte au « fonctionnement et [à]

l'indépendance de la juridiction administrative ».

Sur la légalité de la recommandation relative à l'usage des réseaux sociaux

Une nouvelle fois, les magistrats écartent l'illégalité externe soulevée, rappelant que le vice-président du Conseil d'État a compétence pour adopter une telle recommandation, conformément aux dispositions précitées et que la modification apportée à la Charte a bien été examinée par la commission supérieure du Conseil d'État.
Sur le fond, le syndicat de la juridiction administrative met en cause les paragraphes suivants : « la plus grande retenue (...) dans l'usage des réseaux sociaux sur Internet lorsque l'accès à ces réseaux n'est pas exclusivement réservé à un cercle privé aux accès protégés » ; « dans tous les cas, il convient de s'abstenir de prendre part à toute polémique qui, eu égard à son objet ou à son caractère, serait de nature à rejaillir sur l'institution » ; « s'agissant de l'actualité juridique et administrative, il convient pour les membres de la juridiction administrative de faire preuve non pas seulement de modération dans les propos qu'ils sont conduits à tenir sur les réseaux sociaux, mais d'une vigilance équivalente à celle qu'impliquerait leur publication dans une revue scientifique ». Dans un premier temps, le Conseil d'État rappelle que les magistrats sont tenus au **devoir de réserve** qui vise notamment à « éviter (…) la diffusion de (…) propos [portant] atteinte à la nature et à la dignité des fonctions qu'ils exercent ». Cette restriction à la liberté d'expression est communément admise à l'égard des agents publics[1/2], y compris à l'égard des magistrats[3]. Elle est donc

1. CE, 11 janvier 1935, Bouzanquet.
2. CE, 28 juillet 1993, requête n° 97189.

conforme à l'article 11 de la déclaration des droits de l'Homme et du citoyen et aux exigences de la Convention européenne des droits de l'Homme[4/5]. Dans un second temps, si les correspondances privées relèvent de la vie privée et échappent au disciplinaire, le Conseil d'État rappelle que l'utilisateur doit au préalable « correctement paramétrer [son] compte afin d'en contrôler l'accessibilité et de s'assurer du nombre restreint et de la fiabilité des contacts ». Sur ce point, il est intéressant de souligner qu'il est dans la continuité de la jurisprudence judiciaire[6] (bien que cette notion de « nombre restreint » soit débattue, car fluctuante[7]). Un bon paramétrage de compte permet ainsi à l'utilisateur d'être relativement protégé. Toutefois, il est vrai que la charte de déontologie va plus loin, allant jusqu'à conseiller de ne pas « mentionner leur qualité de magistrat » sur les réseaux. Cette recommandation ne vise pas à interdire mais à avertir qu'à partir du moment où l'utilisateur en fait usage, il s'expose mais expose également l'institution qu'il représente, comme l'illustre la sanction prononcée à l'encontre d'un officier qui utilisait un pseudonyme tout en se prévalant de sa qualité d'ancien de l'école spéciale militaire de Saint-Cyr et de l'école des officiers de la gendarmerie nationale[8]. En effet, il est très aisé, grâce à Internet, de réaliser des recoupements d'informations pour identifier un utilisateur de réseau social. En ce sens, le Conseil d'État souligne

3. Article L. 231-1 du Code de justice administrative : « les membres des tribunaux administratifs et des cours administratives d'appel sont des magistrats dont le statut est régi (…) pour autant qu'elles n'y sont pas contraires, par les dispositions statutaires de la fonction publique de l'État ».

4. CEDH, 15 sept 2009, *Mattely /France*, n° 303330/04 ou encore CEDH, 9 janvier 2018, *Catalan c. Roumanie*, n° 13003/04.

5. (S'agissant des magistrats) CEDH, 28 octobre 1999, *Wille c. Liechtenstein*.

6. Civ. 1ère, 10 avril 2013, n° 11-19530.

7. Les forces régaliennes à l'épreuve des réseaux sociaux, *DALLOZ IP/IT*, n°9, 2019..

8. Le devoir de réserve à l'ère des réseaux sociaux, La Veille juridique, n° 70, CREOGN, septembre 2018, p. 35-41.

donc qu'il s'agit de « recommandations de prudence », de « bonnes pratiques » visant à « garantir le respect de l'obligation de réserve sur les réseaux sociaux » et à « prémunir » contre les risques pour ses utilisateurs. Par ailleurs, le manquement à ces recommandations ne peut constituer en lui-même un manquement disciplinaire. Par conséquent, elles ne portent pas atteinte à la liberté d'expression des membres de la juridiction administrative.

Pour aller plus loin, oserions-nous dire que ce type de recommandations est salutaire ?! Nombre d'agents, utilisateurs des réseaux sociaux, s'interrogent sans cesse sur les limites de leur liberté d'expression et pensent, à tort, être protégés par l'usage d'un pseudonyme. Si la jurisprudence administrative et judiciaire pose des jalons, ils ne sont pas exhaustifs. Il convient de constater que cette Charte en reprend les grands principes, permettant d'appréhender les contours de ce devoir de réserve[9] : la qualité de l'auteur (fonction, niveau dans la hiérarchie), la nature des propos (sujets polémiques, politiques, etc.) et leur accessibilité (compte privé ou public, mention de sa qualité ou non). Cette Charte a donc le mérite de préciser les bonnes pratiques en rappelant également le fonctionnement intrinsèque des réseaux sociaux qui exposent, parfois contre leur gré ou par méconnaissance, leurs utilisateurs. À titre d'exemple, elle rappelle que le pseudonyme n'est pas synonyme d'anonymat et appelle à la vigilance sur son utilisation (§47.3). À titre d'illustration supplémentaire, elle rappelle que les conditions « d'archivage » des données ou les mécanismes de recherche des réseaux sociaux permettent parfois de rendre publiques des « relations personnelles ou des opinions privées », ce qui serait susceptible de faire naître un doute sur l'impartialité du magistrat (§47). Enfin, elle rappelle également qu'aujourd'hui, les

9. *op.cit.* note 5.

gens n'hésitent pas à retranscrire ou diffuser des extraits de « cours », de « conférences » ou d'« auditions » auxquels peuvent participer les magistrats administratifs et qu'à ce titre, ils doivent également être vigilants.

Dès lors, cette Charte se veut véritablement pédagogique et protectrice des utilisateurs, comme le souligne le Conseil d'État en affirmant qu'elle ne peut servir de fondement à une sanction disciplinaire mais qu'elle vise « à prémunir [ses membres] contre le risque que des propos publiés (…) reçoivent une diffusion excédant celle (…) envisagée » et les exposer à un manquement.

À l'instar des magistrats, le ministère de la Défense a publié un guide du bon usage des réseaux sociaux, tout comme le ministère de l'Intérieur[10], en articulant également sa démonstration sur la compréhension des risques et les outils pour naviguer en toute sécurité. Pour les gendarmes, il existe un guide du bon usage des médias sociaux mais qui s'adresse principalement aux *community manager* des unités. Peut-être que la charte du gendarme pourrait faire l'objet d'une mise à jour ? En tout état de cause, il n'est pas nié que l'expression des agents publics sur les réseaux sociaux doit être encadrée au regard de l'exigence de leur statut. À ce titre, ces initiatives institutionnelles participent à la compréhension et à l'appréhension des médias sociaux. Ces guides ou chartes ne suffisent toutefois pas. Il suffit de constater quelques propos ou vidéos diffusés ici et là sur Twitter, TikTok, Snapchat, etc[11]. Il faut reconnaître que, depuis la « génération Z », Internet et les réseaux

10. Téléchargeable uniquement sur l'Intranet.

11. À titre d'exemple : des photos et vidéos d'agents en tenue (ou dans les locaux de service) dénudés ou en train d'avoir des relations sexuelles, des vidéos d'agents sur leur temps personnel mais ivres et en tenue, des vidéos de militaires en train de jouer avec leur armement et de mettre en joue des camarades, des échanges dont certains propos sont polémiques, etc.

sociaux constituent une extension du monde réel. La frontière entre le public et le privé se trouve réduite et beaucoup oublient souvent la portée de ce qu'ils diffusent ou écrivent sur les réseaux, parfois même sans avoir la volonté de nuire ou la conscience qu'ils se mettent en danger, eux ou leur famille, en diffusant des photos, des vidéos, des tracés de course à pieds, etc. Ainsi, il est permis de penser qu'il faut renforcer la pédagogie en la matière en formation initiale mais également en formation continue, en incluant un module spécifique appréhendant, par exemple, les médias sociaux, tant d'un point de vue sociologique que technologique, juridique et éthique. En effet, les nouvelles technologies évoluent chaque jour (ou presque), tout comme les usages des médias sociaux (après tout, Facebook n'est-il pas déjà dépassé ?). À chaque échelon de la hiérarchie, à tout poste, chacun doit désormais avoir conscience de cette nouvelle agora qui fait partie du quotidien de nos agents, de nos militaires, mais également de nos administrés ou « clients ». Les réseaux sociaux font partie notre vie et des nouveaux modes d'expression et, à ce titre, les administrations et les agents ne peuvent y échapper. Il importe donc de s'y confronter, d'en tirer le meilleur tout en se prémunissant contre le pire.

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

JUIN
2020

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

Par le Gal d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE CONSTITUTIONNELLE

Décision n° 2020-801 DC du 18 juin 2020 relative à la loi visant à lutter contre les contenus haineux sur Internet

Les obligations imposées aux hébergeurs, aux éditeurs et aux plateformes sont contraires à la Constitution, car elles portent atteinte à la liberté d'expression et de communication en étant ni nécessaires, ni adaptées, ni proportionnées.

La genèse

Déposée le 20 mars 2019, la proposition de loi visant à lutter contre la haine sur Internet, dite « loi Avia », a été adoptée le 13 mai 2020, après des débats qui ont souligné une absence d'unanimité, non sur la nécessité de lutter contre la dissémination via Internet de propos manifestement illégaux, ou plus généralement de contenus portant atteinte à la dignité humaine, mais sur les modalités envisagées.
Dès sa présentation, la loi a fait l'objet de réserves ou de critiques, notamment de la part du Conseil d'État et de la Commission nationale consultative des droits de l'Homme. Se sont ajoutées les observations de la Commission européenne, adressées le 22 novembre 2019. La Commission considère, en effet, que la proposition de loi Avia contient des obligations entraînant des restrictions à la libre prestation de services de la société de l'information depuis un autre État membre, au sens de la directive sur le commerce électronique. Elle interfère avec la directive

« Services de médias audiovisuels » (SMA)[1], porte sur un domaine couvert par le futur règlement sur les contenus à caractère terroriste en ligne (CTL) et contrevient au principe, confirmé par la jurisprudence de la Cour de justice de l'Union européenne (CJUE), interdisant aux États membres d'imposer aux prestataires intermédiaires, y compris aux fournisseurs de services d'hébergement, une obligation générale de surveillance des informations qu'ils transmettent ou stockent, ou de recherche active des faits ou circonstances révélant des activités illégales. La Commission ajoute que la présidente de la Commission européenne, Ursula von der Leyen, a annoncé une nouvelle législation européenne sur les services numériques (*Digital Services ActDigital Services Act*), qui pourrait harmoniser certaines normes de responsabilité pour les plateformes en ligne en ce qui concerne les contenus illégaux. On le voit donc, la proposition de loi est fraîchement accueillie par la Commission. Les travaux parlementaires, une fois de plus, mettent en exergue le difficile équilibre entre la sécurité et la liberté.

La loi Avia voulait modifier la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), transposant dans l'ordre interne la directive 2000/31/CE du 8 juin 2000 relative au commerce électronique. La LCEN a prévu un régime de responsabilité des fournisseurs d'accès (FAI), des hébergeurs et des éditeurs tenant compte de leur capacité d'intervention sur le contenu du message véhiculé.

1. Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels »).

Les FAI (Art. 6-I-1 LCEN) sont les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne. Leur responsabilité est fixée *a minima* : ils n'ont pas d'obligation générale de surveillance ou de recherche des infractions, mais doivent informer les internautes de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposer au moins un de ces moyens.
Les hébergeurs (Art. 6-I-2 LCEN) sont les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images de toute nature. Leur responsabilité civile ou pénale est engagée s'ils n'ont pas agi promptement alors qu'ils avaient connaissance d'un contenu manifestement illicite.
Les éditeurs (Art. 6-III-1° LCEN) sont, quant à eux, responsables des contenus mis en ligne, car ils ont un pouvoir sur les auteurs et les contenus sur lesquels ils peuvent intervenir.

Les modifications prévues par la loi Avia

La première modification prévue (paragraphe I de l'article 1er de la loi), relative aux hébergeurs et éditeurs d'un service de communication en ligne, portait sur l'article 6-1 de la loi du 21 juin 2004, en permettant à l'autorité administrative de leur demander de retirer dans un délai d'une heure certains contenus à caractère terroriste ou pédopornographique et, en l'absence de retrait dans un délai de vingt-quatre heures, de notifier la liste des adresses des contenus incriminés aux FAI qui devaient alors sans délai en empêcher l'accès. Le manquement à cette obligation entraînait une peine d'un an d'emprisonnement et de 250 000 euros d'amende.
La seconde modification concernait les plateformes. Aux termes de

l'article L 111-7(I) du Code de la consommation : « Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers; 2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service ». La définition englobe de très nombreuses plateformes en ligne : médiaux sociaux, partage de vidéos, places de marché et moteurs de recherche. Le paragraphe II de l'article 1er de la loi créait un article 6-2 dans la LCEN qui imposait, sous peine de sanction pénale, à certains opérateurs de plateforme en ligne de retirer ou de rendre inaccessibles dans un délai de vingt-quatre heures des contenus illicites en raison de leur caractère haineux ou sexuel. Dans ce délai, les opérateurs, dont l'activité repose sur le classement ou le référencement (moteurs de recherche), au moyen d'algorithmes informatiques, de contenus proposés ou mis en ligne par des tiers et dont l'activité sur le territoire français dépasse des seuils déterminés par décret, étaient tenus de retirer ces contenus de la page de résultats de recherche qu'ils renvoient en réponse à une requête.

Les contenus illicites étaient signalés, sous sa responsabilité, par n'importe quel internaute. Ils étaient illicites parce qu'ils constituaient une des infractions énumérées par la loi Avia[2]. Étaient

2. Selon la loi, il s'agissait des contenus contrevenant manifestement aux dispositions mentionnées aux cinquième, septième et huitième alinéas de l'article 24, à l'article 24 bis et aux troisième et quatrième alinéas de l'article 33 de la loi du 29 juillet 1881 sur la liberté de la presse, aux articles 222-33, 227-23 et 421-2-5 du Code pénal ainsi que, lorsque l'infraction porte sur un contenu à caractère pornographique, à l'article 227-24 du même Code.

ainsi visés :
- l'apologie à la commission de certains crimes ;
- la provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée ou à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap ou de provocation à la discrimination à l'égard de ces dernières personnes ;
- la contestation de crimes contre l'humanité, définis par l'article 6 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945 et commis, soit par les membres d'une organisation déclarée criminelle en application de l'article 9 dudit statut, soit par une personne reconnue coupable de tels crimes par une juridiction française ou internationale ;
- la négation, la minoration ou la banalisation de façon outrancière de l'existence d'un crime de génocide, d'un autre crime contre l'humanité que ceux précités, d'un crime de réduction en esclavage ou d'exploitation d'une personne réduite en esclavage ou d'un crime de guerre lorsque ce crime a donné lieu à une condamnation prononcée par une juridiction française ou internationale ;
- l'injure commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée ou envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou identité de genre ou de leur handicap ;
- le harcèlement sexuel, la transmission d'une image ou d'une représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique ;
- la provocation directe à des actes de terrorisme ou d'apologie de

ces actes ;
- la diffusion d'un message à caractère pornographique susceptible d'être vu ou perçu par un mineur.

La troisième modification insère dans la loi du 21 juin 2004 un article 6-4 définissant les conditions dans lesquelles l'administration peut demander à un opérateur d'empêcher l'accès à un site reprenant un contenu dont un juge a considéré qu'il relevait des infractions prévues au premier alinéa du paragraphe I de l'article 6-2 cité *supra*. Il s'agit de lutter contre les « sites miroirs » qui contournent les interdits.

La sage décision des Sages

La loi est déférée le 18 mai devant le Conseil constitutionnel qui rend sa décision le 18 juin et déclare le texte partiellement contraire à la Constitution. À dire vrai, c'est la quasi-totalité des mesures envisagées qui est amputée.
Pour sa démonstration, le Conseil rappelle des principes déjà énoncés dans des décisions précédentes et qui mettent en évidence le nécessaire équilibre entre la préservation des libertés et la nécessité de protéger la société :

• L'article 11 de la Déclaration des droits de l'Homme et du citoyen de 1789 dispose que « la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ». En l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la

participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services et de s'y exprimer ;

• Sur le fondement de l'article 34 de la Constitution, il appartient au législateur d'édicter des règles concernant l'exercice du droit de libre communication et de la liberté de parler, d'écrire et d'imprimer. Il peut ainsi instituer des règles permettant de faire cesser des abus de l'exercice de la liberté d'expression et de communication qui portent atteinte à l'ordre public et aux droits des tiers. Mais, tenant compte du fait que la liberté d'expression et de communication conditionne la démocratie et est l'une des garanties du respect des autres droits et libertés, le législateur ne peut apporter à cette liberté que des restrictions nécessaires, adaptées et proportionnées à l'objectif poursuivi. Cette trilogie de conditions au regard de la finalité est très classique et fonde la notion d'ordre public.

S'agissant des pouvoirs que la loi voulait accorder à l'autorité administrative, le Conseil admet que la diffusion d'images pornographiques représentant des mineurs (article 227-23 du Code pénal) et la provocation à des actes de terrorisme ou l'apologie de tels actes (article 421-2-5 du Code pénal) constituent des abus de la liberté d'expression et de communication qui portent gravement atteinte à l'ordre public et aux droits des tiers. La loi voulait faire cesser de tels abus. Mais plusieurs considérations viennent contrarier sa détermination : le caractère illicite de leurs contenus ne repose pas sur leur caractère manifeste – exigence déjà énoncée par le Conseil constitutionnel – et relève de la seule appréciation de l'administration. En outre, le recours contre la décision de l'administration n'est pas suspensif, le délai d'une heure laissé à l'éditeur ou à l'hébergeur pour retirer ou rendre inaccessible le

contenu visé est incompatible avec l'intervention d'un juge appelé à statuer (l'intervention d'un juge était réclamée par les détracteurs de la loi). Par ailleurs, l'hébergeur ou l'éditeur qui ne défère pas à cette demande dans le délai d'une heure peut être condamné à une peine d'emprisonnement d'un an et à 250 000 euros d'amende. Pour toutes ces raisons, le Conseil constitutionnel a considéré que le législateur avait porté à la liberté d'expression et de communication une atteinte qui n'est pas adaptée, nécessaire et proportionnée au but poursuivi. Cette disposition est donc inconstitutionnelle.

Poursuivant l'examen du texte, les Sages ont également déclaré contraires à la Constitution les obligations imposées par le paragraphe II de l'article 1er, lequel crée un article 6-2 dans la loi du 21 juin 2004 imposant à certains opérateurs de plateforme en ligne, sous peine de sanction pénale, de retirer ou de rendre inaccessibles dans un délai de vingt-quatre heures des contenus illicites en raison de leur caractère haineux ou sexuel.

Tout en reconnaissant que le législateur a voulu prévenir la commission d'actes troublant gravement l'ordre public et éviter la diffusion de propos faisant l'éloge de tels actes, le Conseil souligne tout d'abord l'absence d'intervention préalable d'un juge. Il constate que le risque pénal pesant sur l'opérateur le conduirait à examiner tous les contenus signalés, en procédant à une qualification juridique souvent complexe ou exigeant une analyse contextuelle, cela dans un délai trop bref. Ainsi, « compte tenu des difficultés d'appréciation du caractère manifestement illicite des contenus signalés dans le délai imparti, de la peine encourue dès le premier manquement et de l'absence de cause spécifique d'exonération de responsabilité, les dispositions contestées ne peuvent qu'inciter les opérateurs de plateforme en ligne à retirer les contenus qui leur sont signalés, qu'ils soient ou non manifestement illicites ». Elles portent donc une atteinte à l'exercice de la liberté d'expression et

de communication qui n'est pas nécessaire, adaptée et proportionnée.

Par « effet domino », les dispositions de la loi qui s'appuyaient sur les articles censurés ou les précisaient sont elles-mêmes inconstitutionnelles. Il en est ainsi, par exemple, de l'article 8 de la loi qui insérait dans la loi du 21 juin 2004 un article 6-4 définissant les conditions dans lesquelles l'administration pouvait demander à un opérateur d'empêcher l'accès à un « site miroir ».

Que reste-t-il de la loi Avia ?

Sont déclarés contraires à la Constitution les paragraphes I et II de l'article 1er, les articles 3, 4, 5, 7, 8 et 9…
Demeurent les dispositions relatives à la création d'un Parquet spécialisé dans la poursuite des infractions de haine en ligne, celle d'un observatoire de la haine en ligne et la simplification de la procédure de signalement.

Décision n° 2020-845 QPC du 19 juin 2020 relative au recel d'apologie du terrorisme

Le délit de recel d'apologie d'actes de terrorisme porte à la liberté d'expression et de communication une atteinte qui n'est pas nécessaire, adaptée et proportionnée.

La genèse

Dans *La veille juridique n° 86* d'avril 2020 (*supra*, p. 60-64), nous avons évoqué les doutes de la Cour de cassation, relatifs à la combinaison des articles 321-1 et 421-5 du Code pénal réprimant

l'un le recel, l'autre l'apologie du terrorisme. Après avoir eu des certitudes, illustrées notamment par son arrêt du 7 janvier 2020, la Cour de cassation a eu des doutes, dont témoigne la question prioritaire de constitutionnalité, objet de son arrêt du 24 mars 2020. Le 7 janvier[3], elle avait rejeté un pourvoi en considérant « qu'entre dans les prévisions des articles 321-1 et 421-2-5 du code pénal le fait de détenir, à la suite d'un téléchargement effectué en toute connaissance de cause, des fichiers caractérisant l'apologie d'actes de terrorisme ». Toutefois, s'appuyant sur l'article 10 de la Convention européenne des droits de l'Homme, elle a estimé qu'une condamnation ne pouvait intervenir que si le receleur manifestait de manière caractérisée son adhésion à l'idéologie exprimée dans ces fichiers.

Mais, par un arrêt du 24 mars 2020 (n° 782 (19-86.706), la Chambre criminelle de la Cour de cassation a saisi le Conseil constitutionnel par une question prioritaire de constitutionnalité (QPC) ainsi rédigée :

« Les dispositions combinées des articles 321-1 et 421-2-5 du code pénal, telles qu'interprétées par la jurisprudence de la Cour de cassation, en ce qu'elles incriminent, sous la qualification de recel d'apologie du terrorisme, la consultation de sites internet faisant l'apologie du terrorisme, ou la possession d'un support informatique ou numérique sur lequel serait téléchargé le produit d'une telle consultation, sont-elles contraires aux droits et libertés que la Constitution garantit et, plus précisément, au principe de la liberté d'opinion et de communication garanti par l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789, et méconnaissent-elles l'autorité de la chose jugée des décisions du Conseil constitutionnel ? ».

3. Ch. criminelle n° 2789 (19-80.136), M.X, 7 janvier 2020.

Le Conseil a eu à se prononcer à deux reprises sur la consultation habituelle des sites provoquant au terrorisme ou en en faisant l'apologie. Par décision n° 2016-611 QPC du 10 février 2017, il a censuré les dispositions de l'article 421-2-5-2 du Code pénal, dans sa rédaction issue de la loi du 3 juin 2016, en considérant qu'elles portaient à l'exercice de la liberté de communication une atteinte qui n'est pas nécessaire, adaptée et proportionnée. En outre, comme il l'a rappelé dans sa décision n° 2017-682 QPC du 15 décembre 2017, censurant la deuxième version de l'article incriminé, l'intention terroriste de l'auteur de l'infraction doit être établie par une adhésion à l'idéologie véhiculée par les sites en question.

La décision du Conseil constitutionnel

Pour le requérant et les associations intervenantes, il n'y aurait pas de différence substantielle et fondamentale entre la consultation d'un site Internet terroriste et le téléchargement ou la détention sur un support informatique du contenu de tels sites. Rien ne distinguerait ce délit de recel de celui de consultation habituelle de sites Internet terroristes jugé contraire à la liberté de communication dans les décisions du 10 février 2017 et du 15 décembre 2017[4]. Ils dénoncent le fait que la répression du délit de recel d'apologie d'actes de terrorisme serait aggravée par rapport à celle du délit inconstitutionnel de consultation habituelle de sites Internet terroristes, puisqu'aucune cause exonératoire n'est prévue, que l'infraction n'a pas à être commise de manière habituelle et qu'elle se fonde sur la seule détention matérielle du message en cause, sans exiger qu'il ait été consulté par l'intéressé.

4. Décisions du Conseil constitutionnel n°s 2016-611 QPC du 10 février 2017 et 2017-682 QPC du 15 décembre 2017.

Dans sa décision du 18 mai 2018[5], le Conseil constitutionnel a spécialement examiné les mots *« ou de faire publiquement l'apologie de ces actes »* figurant au premier alinéa de l'article 421-2-5 du Code pénal, dans la même rédaction que celle contestée par le requérant. Il a déclaré ces dispositions conformes à la Constitution dans les motifs et le dispositif de cette décision. Mais l'interprétation de ces dispositions, intervenue depuis cette déclaration de conformité, constitue un changement des circonstances justifiant le réexamen des dispositions contestées. Le Conseil constitutionnel, comme il l'a fait pour la loi Avia (cf. *supra*), met en balance l'atteinte à la liberté d'expression et de communication avec les atteintes qui lui sont portées par le législateur, lesquelles doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi.

S'agissant de la nécessité, le Conseil constitutionnel relève, comme il l'a fait au travers de ses décisions des 10 février et 15 décembre 2017, que la législation comprend de nombreuses dispositions permettant de lutter contre le terrorisme, dans le Code pénal[6],

5. Décision du Conseil constitutionnel n° 2018-706 QPC du 18 mai 2018.

6. L'article 421-2-1 du Code pénal réprime le fait de participer à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'un acte de terrorisme. L'article 421-2-4 du même Code sanctionne le fait d'adresser à une personne des offres ou des promesses, de lui proposer des dons, présents ou avantages quelconques, de la menacer ou d'exercer sur elle des pressions afin qu'elle participe à un groupement ou une entente, prévus à l'article 421-2-1 ou qu'elle commette un acte de terrorisme. L'article 421-2-5, indépendamment de sa combinaison avec l'infraction de recel, sanctionne le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes. Enfin, l'article 421-2-6 réprime le fait de préparer la commission d'un acte de terrorisme dès lors que cette préparation est intentionnellement en relation avec une entreprise individuelle ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur et qu'elle est

comme dans le Code de procédure pénale[7]. En outre, selon l'article 706-23 du Code de procédure pénale, l'arrêt d'un service de communication au public en ligne peut également être prononcé par le juge des référés pour les faits prévus à l'article 421-2-5 du Code pénal lorsqu'ils constituent un trouble manifestement illicite. L'article 421-2-5-1 du même Code réprime le fait d'extraire, de reproduire et de transmettre intentionnellement des données faisant l'apologie publique d'actes de terrorisme ou provoquant directement à ces actes afin d'entraver, en connaissance de cause, l'efficacité des procédures précitées.

Le Conseil constitutionnel évoque également les pouvoirs confiés à l'autorité administrative (techniques de renseignement, mesures de retrait, de blocage ou de déréférencement des sites à caractère terroriste).

L'exigence de nécessité de l'atteinte portée à la liberté d'expression et de communication n'est donc pas vérifiée. En ce qui concerne les exigences d'adaptation et de proportionnalité requises en matière d'atteinte à la liberté d'expression et de communication, la détention des fichiers ou documents apologétiques n'y participe qu'à la condition de donner lieu ensuite à une nouvelle diffusion publique. Ni l'adhésion, ni la détention matérielle desdits fichiers ou documents ne sont susceptibles d'établir, à elles seules, l'existence d'une volonté de commettre des actes terroristes ou d'en faire l'apologie. Le délit de recel d'apologie d'actes de terrorisme réprime

---

caractérisée par le fait de détenir, de se procurer, de tenter de se procurer ou de fabriquer des objets ou des substances de nature à créer un danger pour autrui ainsi que par d'autres agissements tels que la consultation habituelle d'un ou de plusieurs services de communication au public en ligne provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie ou par la détention des documents présentant les mêmes provocation ou apologie.

7. En particulier les techniques d'enquêtes et les techniques spéciales d'enquête pour la lutte contre la criminalité organisée.

donc d'une peine qui peut s'élever, selon les cas, à cinq, sept ou dix ans d'emprisonnement, le seul fait de détenir des fichiers ou des documents faisant l'apologie d'actes de terrorisme, sans que soit retenue l'intention terroriste ou apologétique du receleur comme élément constitutif de l'infraction. D'où le caractère inadapté et disproportionné du délit de recel d'apologie d'actes de terrorisme qui porte à la liberté d'expression et de communication une atteinte qui n'est pas nécessaire, adaptée et proportionnée. Les mots*« ou de faire publiquement l'apologie de ces actes »* figurant au premier alinéa de l'article 421-2-5 du Code pénal ne sauraient donc, sans méconnaître cette liberté, être interprétés comme réprimant un tel délit.

Article 421-2-5

« Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne.
Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

Sous cette réserve, les mots « ou de faire publiquement l'apologie de ces actes » figurant au premier alinéa de l'article 421-2-5 du Code pénal, sont conformes à la Constitution.

ACTUALITÉ NUMÉRIQUE

L'opérateur des systèmes d'information interministériels classifiés (OSIIC)

Le service à compétence nationale est créé par le décret n° 2020-455 du 21 avril 2020

Le 1er juillet 2020, un nouveau service à compétence nationale sera opérationnel. Ce service, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), est l'opérateur des systèmes d'information interministériels classifiés. Il n'est pas créé *ex nihilo* mais résulte de la fusion du centre de transmissions gouvernemental, organisme militaire relevant organiquement du chef d'état-major des Armées et placé pour emploi sous l'autorité du SGDSN, et de la sous-direction du numérique, qui dépend de l'Agence nationale de sécurité des systèmes d'information (ANSSI).
Selon l'article 2 du décret, l'opérateur des systèmes d'information interministériels classifiés est chargé de :
1° Concevoir, réaliser et mettre en œuvre, en tous lieux et en tout temps, les moyens interministériels classifiés de communications électroniques nécessaires au Président de la République et au Gouvernement ;
2° Exploiter et mettre en œuvre, en tous lieux et en tout temps, des moyens de communication classifiés entre le Président de la République, les chefs d'État ou de gouvernement étrangers, les responsables des institutions et autres organes de l'Union européenne et ceux des autres organisations internationales ;
3° En lien avec les ministères :
a) Définir un schéma directeur des systèmes d'information interministériels classifiés,

b) Concevoir, réaliser, déployer, exploiter et soutenir en tout temps ces systèmes ;
4° Participer à la mise en œuvre des plans gouvernementaux concourant à la continuité de l'État et de l'action gouvernementale ;
5° Elaborer la stratégie numérique pluriannuelle et le schéma directeur des systèmes d'information du secrétariat général de la défense et de la sécurité nationale et fournir à ce secrétariat général une offre de services numériques ;
6° Exploiter et administrer les réseaux de chiffrement relatifs à son périmètre de responsabilité.
La création de cet opérateur a pour objectif de rationaliser les déploiements de moyens classifiés, d'optimiser le service rendu aux autorités et de faciliter la convergence technologique des systèmes mis en œuvre. L'opérateur assure également la fonction de direction des systèmes d'information pour l'ensemble des entités composant le SGDSN.

StopCovid

Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid »

Après avoir reçu un avis favorable de la Commission nationale de l'informatique et des libertés (CNIL), l'application « StopCovid » a fait l'objet d'un débat au Parlement, le 27 mai, suivi d'un vote non contraignant. Deux jours après, un décret a fixé les principes de l'application.

Le décret autorise le traitement de données dénommé « StopCovid », qui repose sur une application mobile et un serveur central, et dont la responsabilité est confiée au ministre chargé de

la santé (direction générale de la santé). Le traitement a pour finalité d'informer les personnes utilisatrices de l'application qu'il existe un risque qu'elles aient été contaminées par le virus du Covid-19 en raison du fait qu'elles se sont trouvées à proximité d'un autre utilisateur de cette application ayant été diagnostiqué positif à cette pathologie. Les personnes exposées à ce risque sont des « contacts à risque de contamination ». Outre la sensibilisation, l'application leur recommande de s'orienter vers les acteurs de santé compétents aux fins que ceux-ci les prennent en charge et leur prescrivent, le cas échéant, un examen de dépistage. Les données de santé figurent parmi les données à caractère personnel les plus sensibles. Le traitement, qui n'exige pas de consentement, doit donc répondre à une mission d'intérêt public conformément au e du paragraphe 1 de l'article 6 du règlement (UE) du 27 avril 2016 susvisé, et pour les motifs d'intérêt public mentionnés au i du paragraphe 2 de l'article 9 de ce même règlement.

L'utilisation de l'application est facultative, ce qui est sa force au regard des libertés, et sa faiblesse, puisqu'il faudrait s'appuyer sur 60 % de la population pour avoir des résultats probants.

Le décret dresse la liste des données traitées :

1° Une clé d'authentification partagée entre l'application et le serveur central, générée par ce serveur lors du téléchargement de l'application, qui sert à authentifier les messages de l'application ;

2° Un identifiant unique associé à chaque application téléchargée par un utilisateur, qui est généré de façon aléatoire par le serveur central et n'est connu que de ce serveur, où il est stocké ;

3° Les codes pays, générés par le serveur central ;

4° Des pseudonymes aléatoires et temporaires, qui sont transmis chaque jour par le serveur central à l'application lorsqu'elle se connecte à ce dernier ;

5° L'historique de proximité d'un utilisateur, constitué des pseudonymes aléatoires et temporaires émis via la technologie « Bluetooth » par les applications installées sur des téléphones mobiles d'autres utilisateurs qui se trouvent, pendant une durée déterminée, à une distance de son téléphone mobile telle qu'il existe un risque suffisamment significatif qu'un utilisateur qui serait positif au virus du Covid-19 contamine l'autre.

Les pseudonymes aléatoires et temporaires sont collectés et enregistrés par l'application sur le téléphone mobile de l'utilisateur.

6° L'historique de proximité des contacts à risque de contamination par le virus du Covid-19, correspondant aux pseudonymes aléatoires et temporaires enregistrés par l'application dans les quarante-huit heures qui précèdent la date de début des symptômes ainsi que dans la période comprise entre cette date et la date de transfert de l'historique de proximité au serveur central ou, à défaut de renseignement de la date de début des symptômes par la personne dépistée positive, pendant les quinze jours qui précèdent le transfert de l'historique de proximité.

Ces données sont transmises par les utilisateurs diagnostiqués ou dépistés positifs au virus du Covid-19 qui le souhaitent au serveur central. Elles sont alors stockées sur ce serveur et sont notifiées aux applications des personnes identifiées comme « contacts à risque de contamination » à l'occasion de leur connexion quotidienne au serveur.

Ces personnes identifiées comme « contacts à risque de contamination » reçoivent alors, par l'intermédiaire de l'application, la seule information selon laquelle elles ont été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus du Covid-19 au cours des quinze derniers jours ;

7° Les périodes d'exposition des utilisateurs à des personnes diagnostiquées ou dépistées positives au virus du Covid-19, stockées

sur le serveur central. Ces données sont collectées et enregistrées par l'application sur le téléphone mobile de l'utilisateur et stockées sur le serveur central en cas de partage par l'utilisateur de l'historique de proximité des contacts à risque de contamination par le virus du Covid-19 ;
8° Les données renseignées dans l'application par les personnes diagnostiquées ou dépistées positives au virus du Covid-19 qui décident d'envoyer au serveur l'historique de proximité de leurs contacts à risque :
a) La date de début des symptômes si l'utilisateur est en mesure de donner cette information,
b) Le code aléatoire à usage unique donné par un médecin traitant à son patient suite à un diagnostic clinique positif au virus du Covid-19 ou un code aléatoire à usage unique sous forme de QR-code émis par le traitement mentionné à l'article 8 du décret n° 2020-551 du 12 mai 2020, en cas d'examen de dépistage positif au virus du Covid-19, en application de l'article 9 de ce même décret, afin que l'utilisateur de l'application soit autorisé par le serveur à partager son historique de proximité ;
9° Le statut « contacts à risque de contamination » de l'identifiant de l'application, qui est retenu dès lors qu'un utilisateur de l'application a été, conformément aux critères définis par l'arrêté mentionné au 5°, à proximité d'un autre utilisateur, ultérieurement dépisté ou diagnostiqué positif au virus du Covid-19. Cette donnée est stockée par le serveur central, lorsqu'elle lui a été communiquée par l'utilisateur qui accepte de lui transmettre son historique de proximité des contacts à risque de contamination par le virus du Covid-19 ;
10° La date des dernières interrogations du serveur central.

Quelques jours après son lancement, l'application compterait moins

de deux millions d'usagers, ce qui est trop faible pour en assurer l'efficacité. Selon Cédric O, secrétaire d'État au numérique qui a porté le projet, l'application a généré une « poignée » de notifications. Il est vrai que les esprits sont moins mobilisés, alors que la pandémie semble confirmer sa décroissance. L'application pourrait connaître un meilleur succès en cas de seconde vague. Le faible engouement est sans doute lié à une méfiance des Français vis-à-vis du numérique en général et des solutions offertes par l'État en particulier, tandis que nos compatriotes livrent leur vie privée aux GAFAM sans la moindre inquiétude.

La volonté de préserver l'anonymat des utilisateurs est un souci contant des concepteurs, car ils savent que c'est sur ce point que l'application sera scrutée.
D'où les multiples précautions prises pour offrir une « sécurité dès la conception » (*security by desing*), comme l'exige le Règlement général sur la protection des données (RGPD). L'application a fait l'objet de tests et d'audits menés notamment par l'ANSSI. Elle est aussi livrée au *« bug bounty »*. Le principe du *« bug bounty »* repose sur l'association d'hackers qui respectent des règles contractuelles en vue de rechercher des failles informatiques (période de recherche, périmètre, interdiction de modifier, d'extraire des données, confidentialité, etc.). Parce qu'ils respectent la « volonté du maître du système », les hackers ne tombent pas sous le coup de la loi Godfrain (pénétration, maintien frauduleux dans un système de traitement de données, entrave, modification, extraction de données, etc.).
La plateforme « Yes We Hack », la plus importante d'Europe, qui dispose d'une communauté de 15 000 hackers dans 120 pays différents, s'est mise à disposition de l'opération, dès le 27 mai 2020, avec 25 testeurs pour rechercher des vulnérabilités. Depuis

l'ouverture de l'application au public, tous les hackers de « Yes We Hack » traquent les failles. Les primes, allant de 50 à 2 000 euros, selon l'importance des failles découvertes, sont prises en charge par la plateforme, ce qui est une bonne publicité, mais qui témoigne aussi d'un sens de l'intérêt général de ses fondateurs. On notera que, depuis l'annonce faite au FIC 2019 par Florence Parly, « Yes We Hack » est associé au ministère des Armées pour rechercher les failles des systèmes qu'il déploie.

5e rapport d'activité de l'autorité qualifiée de la CNIL, 2 février - 31 décembre 2019

Alexandre Linden, ancien conseiller près la Cour de cassation, vient de rendre son 5e rapport d'activité relatif à l'application des mesures administratives portant sur les contenus à caractère pédopornographique et ceux provoquant au terrorisme ou en en faisant l'apologie. On rappellera que ces mesures n'écartent pas une action judiciaire. Le paragraphe 8 du I de l'article 6 de la loi pour la confiance dans l'économie numérique dispose, en effet, que « l'autorité judiciaire peut prescrire en référé ou sur requête, aux hébergeurs ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ».
Mais l'article 6-1 de la loi pour la confiance dans l'économie numérique (créé par l'article 12 de la loi du 13 novembre 2014) ouvre une voie administrative : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) peut demander respectivement aux hébergeurs, aux fournisseurs d'accès ou aux moteurs de recherche, de retirer les sites litigieux, d'en bloquer l'accès ou d'opérer leur

déréférencement. Cette mesure de police administrative est placée sous le contrôle d'une personne qualifiée désignée au sein de la Commission nationale de l'informatique et des libertés (CNIL) qui présente chaque année un rapport d'activité.

Contrairement aux années précédentes, la période de référence part du 2 février 2019 et s'achève le 31 décembre 2019. Depuis les origines, le rapport examinait une période à cheval sur deux millésimes (entre le 1er mars et le 1er février 2019 pour le précédent rapport). Cette particularité était due au délai nécessaire à la première mise en œuvre des mesures de retrait, blocage et déréférencement instituées par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme (d'où le commencement le 1er mars 2015). Le respect de l'année civile est plus cohérent, en même temps qu'il prépare la reprise de la mission par le Conseil supérieur de l'audiovisuel (CSA), mission qui pourrait être ultérieurement transmise à l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), si la fusion entre la Hadopi et le CSA est réalisée par le projet de loi « Communication audiovisuelle et souveraineté culturelle à l'ère numérique » en cours d'examen.

Il est donc difficile d'opérer des comparaisons, la série n'étant plus continue.

Période	Demandes de retrait	Retraits effectués	Demandes de blocage	Demandes de déréférencement
Fév 2019-décembre 2019	11 874 (7 542)	8 105 (5 479)	420 (405)	5 883 (4 432)
2018-2019	18 014 (7 923)	13 421	879	6 581
2017-2018	35 110 (2 371)	7 724	763	3 115
2016-2017	2 561 (372)	2 305	874	2 077
2015-2016	1 439 (121)	1 179	312	855

Les chiffres entre parenthèses correspondent à la pédopornographie qui demeure le motif majoritaire.

Selon Alexandre Linden, la nette diminution constatée entre 2018 et 2019 du nombre de demandes de retrait, de déréférencement et de blocage de contenus s'explique, d'une part, par le nombre beaucoup plus faible de contenus publiés sur Internet par les organisations terroristes et par leurs sympathisants, d'autre part, en raison des actions coordonnées par EUROPOL en 2019, qui ont fortement impacté certains vecteurs de diffusion utilisés par les terroristes (par exemple Telegram).

Pour la première fois, la personnalité qualifiée avance, pour mesurer l'efficacité du dispositif, le nombre de pages de renvoi affichées par le ministère de l'Intérieur, dès lors qu'un internaute souhaite accéder à une URL ayant fait l'objet d'une des mesures de blocage administratif : 2 524 687 en matière de pédopornographie (99,97 % des affichages), 767 en matière de terrorisme (0,03 % des affichages). Là encore, on mesure l'importance relative de la pédopornographie.

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

SEPTEMBRE 2020

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

Par le G^al d'armée (2S) Marc Watin-Augouard

CJUE (grande chambre), 16 juillet 2020 (affaire C-311/18), Data Protection Commissioner/ Facebook Ireland Ltd, Maximillian Schrems

Le transfert de données à caractère personnel vers des pays tiers et à des fins commerciales peut s'effectuer sur la base de clauses types de protection (CTP) qui ne sont pas, en elles-mêmes, contraires à la Charte de l'Union. Il doit être remis en cause par « l'exportateur » ou l'autorité nationale de contrôle, dès lors que la législation de « l'importateur » n'en respecte pas les principes, notamment en n'offrant pas de recours devant un juge indépendant. Le Bouclier de protection de données (*Privacy Shield*), quant à lui, n'est pas valide au regard de la Charte, eu égard à l'insuffisant encadrement des mesures de surveillance prises par les autorités américaines.

Du *Safe Harbor* au *Privacy Shield*

La Cour de justice de l'Union européenne (CJUE) a été saisie d'une demande de questions préjudicielles relatives à un litige opposant le *Data Protection Commissionner* (DPC – CNIL irlandaise) à Facebook Ireland Ltd et à M. Maximilian Schrems au sujet d'une plainte introduite par celui-ci concernant le transfert de ses données à caractère personnel par Facebook Ireland vers Facebook Inc., société établie aux États-Unis.

Maximilian Schrems, citoyen autrichien, est déjà connu pour être à l'origine de l'invalidation par la CJUE du Safe Harbor, premier accord sur les données à caractère personnel entre l'Union et les États-

Unis. Cet étudiant autrichien est un utilisateur de Facebook qui a signé un contrat habituel avec Facebook Ireland, filiale de Facebook Inc., lequel stipule que les données à caractère personnel des utilisateurs de Facebook résidant sur le territoire de l'Union sont, en tout ou en partie, transférées vers des serveurs appartenant à Facebook Inc., situés sur le territoire des États-Unis, où elles font l'objet d'un traitement.

Le 25 juin 2013, il a saisi le DPC afin d'interdire à Facebook « d'exporter » ses données vers les États-Unis. L'affaire Snowden venait d'éclater, mettant en évidence les pratiques de surveillance généralisée de la part des services américains. Mais l'autorité de contrôle irlandaise a rejeté sa plainte au motif que la Commission européenne avait constaté, par sa décision 2000/520/CE du 26 juillet 2000, dite *Safe Harbor*, que les États-Unis assuraient un niveau adéquat de protection. Sur son recours, la Haute Cour d'Irlande a saisi la CJUE d'une demande de décision préjudicielle relative à la validité de cette décision. Par l'arrêt du 6 octobre 2015[1], la Cour a censuré la décision de la Commission.

Commencent alors des négociations devant aboutir à un nouvel accord. La décision d'exécution (UE) 2016/1250, Bouclier de protection des données (BPD – plus communément dénommé *Privacy ShieldPrivacy Shield*) est adoptée par le Conseil, le 12 juillet 2016, après approbation du Parlement européen. Son article premier constate que « les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis ». Le Bouclier de protection des données se compose des principes publiés par le ministère américain du commerce, le 7 juillet 2016, et des observations et engagements officiels, l'ensemble figurant dans les

1. CJUE Data Protection Commissioner/Maximillian Schrems, 6 octobre 2015 (C-362/14).

annexes de la décision. En vertu des dispositions du BPD, les données à caractère personnel des Européens sont transférées depuis l'Union vers des organisations établies aux États-Unis. Ce sont donc les autorités américaines qui établissent une liste d'entités qui s'autocertifient[2]…

Le G29 (aujourd'hui Comité européen de la protection des données – CEPD) souligne, dès la publication de la décision, les dangers que les lois américaines relatives à la surveillance font peser sur les données des Européens. Mais la Commission considère que toute ingérence des autorités publiques américaines dans l'exercice des droits fondamentaux des personnes pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois et, partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes, sont limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective contre des ingérences de cette nature.

Le BPD fait l'objet chaque année d'une évaluation. Le dernier rapport du 23 octobre 2019[3] est très favorable, si l'on en croit les propos de la commissaire européenne Věra Jourová : « Avec quelque 5 000 sociétés participantes, le bouclier de protection des données est une réussite. L'examen annuel nous permet de vérifier que tout fonctionne correctement. Nous poursuivrons le dialogue sur la diplomatie numérique avec nos homologues américains afin de rendre le bouclier plus solide, notamment en matière de contrôle, d'application de la législation et, à plus long terme, pour améliorer

2. Elles figurent sur la liste des organisations adhérant au Bouclier de protection des données, tenue à jour et publiée par le ministère américain du commerce (DoC), ce qui témoigne de leur « indépendance ».

3. Rapport COM(2019) 495 final de la Commission au Parlement et au Conseil sur la troisième évaluation annuelle du *Privacy Shield* du 23 octobre 2019.

la convergence de nos systèmes ».

L'invalidation du *Privacy Shield*

À la suite du premier arrêt Schrems invalidant le Safe Harbor, la Haute Cour demande à Maximillian Schrems de reformuler sa demande, considérant qu'une grande partie de ses données sont transférées, comme le reconnaît Facebook inc., sur le fondement des 12 clauses types de protection des données figurant en annexe de la décision 2010/87/UE de la Commission du 5 février 2010, dite décision CPT[4]. Ces clauses types, lorsqu'elles sont respectées, sont considérées comme offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants. Elles autorisent le transfert de données, indépendamment d'une décision d'adéquation. Les clauses doivent permettre aux autorités de contrôle de soumettre les importateurs de données et les sous-traitants ultérieurs à des vérifications et, lorsque cela se révèle approprié, de prendre des décisions auxquelles ces derniers devront se plier.
Maximillian Schrems souligne le fait que le droit américain impose à Facebook Inc. de mettre les données à caractère personnel qui lui sont transférées à la disposition des autorités américaines, telles que la *National Security Agency* (NSA) et le *Federal Bureau of Investigation* (FBI). De ce fait, ses données étant utilisées dans le cadre de différents programmes de surveillance, leur transfert

4. Décision CPT, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46, modifiée par la décision d'exécution (UE) 2016/2297 de la Commission, du 16 décembre 2016 adoptée à la suite de l'arrêt du 6 octobre 2015, Schrems (C-362/14), invalidant le *Safe Harbor*.

serait incompatible avec les articles 7, 8 et 47 de la Charte. C'est l'avis énoncé par le Commissaire dans son « projet de décision » du 24 mai 2016. Le 31 mai, celui-ci saisit la *High Court* (Haute Cour) qui, par décision du 4 mai 2018, adresse à la CJUE un renvoi préjudiciel. À son renvoi est annexé un arrêt, qu'elle a prononcé le 3 octobre 2017, qui présente le résultat de l'examen des preuves produites devant elle, auquel le gouvernement américain a participé de manière contradictoire.

L'action des services de renseignement américains mise en cause par la *High Court*

L'arrêt du 3 octobre 2017 de la *High Court* met en exergue les textes en vigueur aux États-Unis qui permettent aux services de renseignement américains d'accéder aux données à caractère personnel transférées outre-Atlantique : le FISA et l'*Executive Order* n° 12333.

Le FISA

Il s'agit tout d'abord du *Foreign Intelligence Surveillance Act* (FISA), du 25 octobre 1978 qui, sous le contrôle de l'*United States Foreign Intelligence Surveillance Court* (FISC), autorise les programmes de surveillance de type PRISM ou UPSTREAM, certifiés chaque année par l'Attorney General et le Directeur du renseignement national (DNI). Comme le souligne la *High Court*, le programme PRISM oblige les fournisseurs de service Internet à fournir à la NSA toutes les communications envoyées et reçues par un « sélecteur », une partie d'entre elles étant également transmise au FBI et à la *Central Intelligence Agency* (CIA) (agence centrale de renseignement). En ce qui concerne le programme UPSTREAM, les entreprises de télécommunications exploitant la « dorsale » de l'Internet (réseau de

câbles sous-marins, terrestres, commutateurs et routeurs) doivent autoriser la NSA à copier et à filtrer les flux de trafic Internet pour recueillir des communications envoyées par un ressortissant non américain visé par un « sélecteur », reçues par lui ou le concernant. Ces flux concernent aussi bien les métadonnées que les contenus.

L'*Executive Order* n° 12333

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

Pour la *High Court*, les activités de la NSA fondées sur l'E.O. 12333 ne font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels. La juridiction estime par ailleurs que le médiateur institué dans le cadre du Bouclier de protection de données ne constitue pas un tribunal, au sens de l'article 47 de la Charte. De ce fait, les citoyens de l'Union n'ont pas accès aux mêmes recours que ceux dont disposent les ressortissants américains contre les traitements de données à caractère personnel par les autorités américaines. Le droit américain ne leur assure pas un niveau de protection substantiellement équivalent à celui garanti par le droit fondamental consacré à cet article.

La *High Court* souligne que la directive stratégique présidentielle n° 28 (*Presidential Policy directive* 28-PPD28), publiée le 17 janvier 2014, relative au contrôle des activités de services de

renseignement intéressant les étrangers (donc les Européens) ne confère pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux.

La décision CJUE

Conformément aux conclusions de l'avocat général, Henrik Saugmandsgaard, la CJUE ne remet pas en cause la décision de la Commission relative aux clauses contractuelles types (CPT), mais elle invalide la décision BPD (*Privacy Shield*).

Tout d'abord, la Cour considère que les questions préjudicielles qui lui sont transmises se réfèrent aux dispositions de la directive 95/46. Toutefois, il est établi que le commissaire n'avait pas encore adopté de décision finale sur cette plainte lorsque cette directive a été abrogée et remplacée par le Règlement général sur la protection des données (RGPD), avec effet au 25 mai 2018. En conséquence, il y a lieu d'y répondre au regard des dispositions du RGPD, et non de celles de la directive 95/46.

La Cour écarte l'objection relative aux dérogations offertes par le RGPD. La possibilité que les données à caractère personnel transférées entre deux opérateurs économiques à des fins commerciales subissent, au cours ou à la suite du transfert, un traitement à des fins de sécurité publique, de défense et de sûreté de l'État par les autorités du pays tiers concerné, ne saurait exclure ledit transfert du champ d'application du RGPD. L'article 2[5] du Règlement ne s'applique, en effet, qu'aux États de l'Union.

5. « Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué : par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. […] ».

La Cour va examiner la décision CPT puis la décision Bouclier de protection de données (BPD), deux voies offertes pour exporter les données. Ces deux modes de transfert sont prévus respectivement par les articles 46 et 45 du RGPD.

S'agissant de la décision CPT, la Cour souligne que les clauses contractuelles ne lient pas les États tiers puisqu'ils ne sont pas parties au contrat, ce qui n'est pas le cas de la décision d'adéquation qui est le fruit d'un accord entre un État tiers et l'UE. Elles doivent faire bénéficier d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par le RGPD, lu à la lumière de la Charte. Le niveau de protection assuré doit être évalué en fonction de l'accès aux données exportées par les autorités du pays tiers et de la pertinence du son système juridique. Il appartient à l'autorité de contrôle (CNIL en France) d'exercer ses pouvoirs, notamment en suspendant ou en interdisant un transfert de données à caractère personnel, dès lors qu'elle constate que ce transfert est effectué en violation de la législation de l'Union européenne (en particulier les articles 45 et 46 du RGPD ainsi que la Charte) ou de l'État membre en matière de protection des données. La CJUE renvoie donc le responsable du traitement ou son sous-traitant établis dans l'Union et l'autorité de contrôle vers leurs responsabilités. L'examen de la décision 2010/87/UE de la Commission, du 5 février 2010[6], au regard des articles 7, 8 et 47 de la Charte des droits fondamentaux, ne révèle aucun élément de nature à affecter la validité de cette décision. Ce n'est pas le texte

6. Décision 2010/87/UE de la Commission, du 5 février 2010, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, modifiée par la décision d'exécution (UE) 2016/2297 de la Commission, du 16 décembre 2016 (pour tenir compte du RGPD).

qui doit être censuré mais, le cas échéant, son application.

Il en va autrement en ce qui concerne la décision BPD. La Commission a accepté que l'adhésion aux principes du Bouclier de protection des données puisse être limitée par *« les exigences relatives à la sécurité nationale, l'intérêt public et le respect de la législation »*. Elle a consacré la primauté du droit américain, selon lequel les organisations américaines autocertifiées, recevant des données à caractère personnel depuis l'Union, sont tenues d'écarter, sans limitation, ces principes lorsque ces derniers entrent en conflit avec lesdites exigences. La Commission n'a pas soulevé le problème de l'analyse des flux par les autorités américaines, considérant que les garanties offertes par le médiateur étaient suffisantes. La CJUE relève que les activités de la NSA fondées sur l'E.O. 12333 ne font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels. Elle estime que le médiateur du Bouclier de protection de données ne constitue pas un tribunal, au sens de l'article 47 de la Charte. Le droit américain n'assure pas aux citoyens de l'Union un niveau de protection substantiellement équivalent à celui garanti par le droit fondamental consacré par cet article. Pour ces raisons, elle constate l'invalidité de la décision BPD au regard du droit de l'Union et en particulier de la Charte.

La CJUE ne craint pas d'instaurer un vide juridique. Selon elle, l'article 49 du RGPD établit, de manière précise, les conditions dans lesquelles des transferts de données à caractère personnel vers des pays tiers peuvent avoir lieu en l'absence d'une décision d'adéquation en vertu de l'article 45 dudit Règlement ou de garanties appropriées au titre de l'article 46 du même Règlement.
Mais les motifs de l'invalidation du *Privacy ShieldPrivacy Shield*, combinés aux exigences relatives aux transferts sur la base des

clauses types, vont poser des difficultés aux entreprises qui utilisent cette voie. Elles seront, en effet, contraintes de constater que l'activité des services américains est de nature à entraîner la suspension des transferts. Les organismes de contrôle, telle la CNIL auront la même obligation. En attendant la conclusion d'un troisième accord d'adéquation (qui suppose une réforme de la législation américaine), seul le transfert de données anonymisées (donc sortant du champ du RGPD) peut se concevoir.

L'après-Brexit ne manquera pas de poser la question du transfert des données vers le Royaume-Uni, celui-ci sortant du champ du RGPD le 31 décembre 2020 et procédant également à des actions de surveillance qui n'offrent pas non plus de garanties pour les citoyens européens.

JURISPRUDENCE ADMINISTRATIVE

Conseil d'État (10ème et 9ème chambres réunies), arrêt n° 430810 du 19 juin 2020, Google LLC/ CNIL

En l'absence d'une autorité chef de file au sens du Règlement général sur la protection des données (RGPD), la Commission nationale de l'informatique et des libertés (CNIL) est compétente pour infliger à Google une amende de 50 millions d'euros pour défaut de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité à l'égard des utilisateurs d'Android.

Par délibération du 21 janvier 2019 (n° SAN-2019-001), la formation restreinte de la CNIL a prononcé à son encontre une sanction pécuniaire d'un montant de 50 000 000 d'euros et décidé de rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

La saisine du Conseil d'État

En mai 2018, les associations None of Your Business (dont Maximilian Schrems est un des principaux animateurs) et La Quadrature du Net ont saisi la CNIL de deux plaintes collectives déposées en application de l'article 80 du RGPD (représentation de plaignants par une association). En cause, la conformité à la loi du 6 janvier 1978 et au RGPD des traitements opérés par Google LLC à partir des données personnelles des utilisateurs du système d'exploitation Android.
À la suite d'un contrôle effectué par la CNIL, le 21 septembre, la présidente a engagé une procédure de sanction qui a abouti à la délibération constatant les manquements aux articles 6, 12 et 13 du RGPD.
Cette délibération est contestée devant le Conseil d'État.

Les motifs évoqués par Google

Google conteste tout d'abord la régularité de la saisine de la CNIL en soulignant que, l'établissement principal de Google étant situé en Irlande, c'est l'autorité de contrôle de ce pays qui aurait dû être saisie en vertu du principe de l'autorité chef de file prévu par le RGPD. La CNIL n'aurait pas correctement appliqué les procédures de coopération et de cohérence prévues par le chapitre VII du RGPD lorsque plusieurs pays de l'Union sont concernés par un traitement de données à caractère personnel.
Google reproche également à la CNIL une erreur de droit pour avoir retenu que le consentement pour les traitements aux fins de personnalisation de la publicité n'était pas valablement recueilli et pour avoir lui avoir reproché un manquement aux obligations de transparence et d'information telles que prévues par les articles 12

et 13 du RGPD.

La décision du Conseil d'État

S'agissant de la compétence de la CNIL, le RGPD dispose que, lors d'un traitement transfrontalier de données à caractère personnel opéré au sein de l'Union européenne, l'autorité de contrôle de l'établissement principal dans l'Union du responsable de ce traitement est, en tant qu'autorité chef de file, compétente pour contrôler le respect des exigences du RGPD. La société Google Ireland Limited ne pouvait être considérée comme son établissement principal au sein de l'Union européenne. À la date de la délibération de la CNIL, la société Google Ireland n'exerçait pas un pouvoir de direction ou de contrôle, quant aux finalités et aux moyens des traitements litigieux, sur les autres filiales européennes de la société Google LLC de nature à la regarder comme une administration centrale au sens du RGPD. L'autorité de régulation irlandaise a confirmé cette analyse par un droit de réponse exercé le 27 août 2018 dans le quotidien *Irish Times*. La société Google LLC qui, seule, déterminait leurs finalités et moyens, ne disposait pas, à la date de la sanction attaquée, d'établissement principal au sein de l'Union européenne. Comme le souligne le Conseil d'État, la CNIL a soumis les plaintes dont elle était saisie à ses homologues européens via le système européen d'échange d'information en vue de la désignation d'une éventuelle autorité chef de file. Aucune autorité de contrôle européenne n'a alors décidé de saisir le comité européen de la protection des données ni fait part d'une appréciation divergente de celle de la CNIL quant à l'absence d'établissement principal de Google LLC en Europe. La CNIL était donc compétente. Il en irait différemment aujourd'hui, le *Data Protection Commissioner* (autorité de régulation irlandaise) serait

compétent.
Le mécanisme prévu aux articles 60 à 62 du RGPD, afin d'encourager la coopération entre les différentes autorités européennes de contrôle de protection des données et d'assurer une application cohérente du Règlement dans l'ensemble de l'Union, ne s'applique qu'en cas de désignation d'une autorité chef de file ou d'opérations conjointes des autorités de contrôle. Tel n'est pas le cas en l'espèce.
Sur les griefs relatifs au consentement et à la transparence, Google avance pour sa défense un dispositif à plusieurs niveaux, avec un premier « étage » relatif aux règles de confidentialité et conditions d'utilisations d'où part une arborescence par lien hypertexte qui apporte des précisions. Pour le Conseil d'État, le premier niveau d'information proposé aux utilisateurs apparaît excessivement général eu égard à l'ampleur des traitements opérés par la société, au degré d'intrusion dans la vie privée qu'ils impliquent et au volume et à la nature des données collectées. Les informations essentielles relatives à certains traitements ne sont accessibles qu'à la suite de nombreuses actions, ou ne le sont qu'à partir de liens hypertextes eux-mêmes difficilement accessibles. Par l'éparpillement de l'information qu'elle organise, l'arborescence apparaît de nature à nuire à l'accessibilité et à la clarté de celle-ci pour les utilisateurs.
Pour appuyer sa démonstration, le Conseil d'État relève que pour « obtenir l'ensemble des informations pertinentes relatives au traitement personnalisé des annonces, un utilisateur doit d'abord effectuer trois actions à partir du premier niveau d'information, avant de revenir au document initial et d'effectuer deux nouvelles actions, soit un total de cinq actions, tandis que six actions sont nécessaires pour obtenir une information exhaustive quant à la géolocalisation. Les informations relatives à la durée de conservation des données, qui doivent être obligatoirement fournies en vertu du a) du 2° de l'article 13 du RGPD, ne sont

accessibles qu'à partir d'un lien hypertexte disponible à la soixante-huitième page du document "Règles de confidentialités" ».
Enfin, un consentement donné au moyen d'une case cochée par défaut n'implique pas un comportement actif de la part de l'utilisateur et ne peut dès lors être considéré comme procédant d'un acte positif clair permettant valablement le recueil du consentement.

ACTUALITÉ NUMÉRIQUE

L'Union européenne inflige ses premières sanctions à la suite de cyberattaques

Le 30 juillet 2020, un peu plus d'un an après leur publication, le Conseil de l'UE vient de mettre en application la décision-cadre et le règlement en date du 17 mai 2019 permettant d'infliger des mesures restrictives visant les personnes physiques ou morales, entités ou organismes qui sont responsables de cyberattaques ou de tentatives de cyberattaques. Ces mesures concernent six personnes physiques et trois personnes morales.

Les textes mis en application

Le 19 juin 2017, le Conseil européen a adopté les conclusions relatives à un cadre pour une réponse diplomatique conjointe face aux actes de cybermalveillance. La « boîte à outils cyberdiplomatique » répond à la nécessité de protéger l'Union, ses États membres et leurs citoyens à l'égard des acteurs étatiques et non étatiques qui mènent des cyberattaques. Elle concourt à la prévention des conflits, à la coopération et à la stabilité dans le cyberespace en précisant les mesures pouvant être décidées dans le

cadre de la Politique étrangère et de sécurité commune (PESC), y compris les mesures restrictives, pour prévenir les actes de cybermalveillance et y répondre.

Lors du sommet numérique de Tallinn (29 septembre 2017), Jean-Claude Juncker, alors président de la Commission européenne, a déclaré que « les cyberattaques ne connaissent pas de frontières, pourtant, nos capacités de réaction varient fortement d'un pays à l'autre, ce qui crée des failles et des vulnérabilités qui favorisent les cyberattaques. L'UE doit se doter de structures plus robustes et plus efficaces pour améliorer sa cyber-résilience et réagir aux cyberattaques ». Il ajoutait : « Nous ne voulons pas être le maillon faible de la lutte contre cette menace mondiale ».

Les 19 et 20 octobre 2017, toujours à Tallinn, le Conseil européen a demandé une approche commune de la cybersécurité au sein de l'UE qui s'est traduite par le *Cybersecurity Act*, approuvé par le Parlement européen, le 12 mars 2019 (voir *La Veille juridique du CREOGN n° 78 , mai 2019, p. 20-24).*

Le 17 mai 2019, le Conseil de l'Union européenne a pris une décision-cadre et un règlement qui s'inscrivent dans la logique de la « boite à outil cyberdiplomatique ».

La décision (PESC) 2019/797 du Conseil, du 17 mai 2019, concerne les mesures restrictives contre les auteurs des cyberattaques qui menacent l'Union ou ses États membres. Pour le Conseil, « les mesures relevant de la politique étrangère et de sécurité commune (PESC), y compris, si nécessaire, les mesures restrictives, adoptées dans le cadre des dispositions pertinentes des traités, conviennent à un cadre pour une réponse diplomatique conjointe de l'Union face aux actes de cybermalveillance, le but étant d'encourager la coopération, de faciliter la réduction des menaces immédiates et à long terme, et d'influencer le comportement d'agresseurs potentiels à long terme ».

Ces mesures ont pour but de dissuader et contrer les cyberattaques qui ont une origine externe au territoire de l'Union et visent l'Union ou ses États membres (la cybercriminalité interne n'est donc pas concernée). Mais elles peuvent aussi être mises en œuvre, si cela est jugé nécessaire, pour réaliser les objectifs de la PESC figurant dans les dispositions pertinentes de l'article 21 du traité sur l'Union européenne, lorsque les cyberattaques visent des pays tiers ou des organisations internationales.

Les mesures restrictives fixées par la décision portent sur l'interdiction d'entrée ou de passage en transit sur le territoire des États membres et sur le gel des fonds et ressources économiques appartenant aux personnes physiques ou morales, entités ou organismes qui sont responsables de cyberattaques ou de tentatives de cyberattaques. S'agissant du gel des fonds et ressources, le règlement (UE) du Conseil du 17 mai 2019, concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, apporte les précisions relatives à sa mise en œuvre.

Comme le précise la décision-cadre, les mesures ciblées doivent être distinguées de l'imputation à des tiers de la responsabilité des cyberattaques, décision politique souveraine prise au cas par cas. Chaque État membre demeure libre d'apprécier l'implication d'un État tiers.

Les décisions du 30 juillet 2020

Le 16 avril 2018, le Conseil a fermement condamné les cyberattaques, connues sous le nom de « WannaCry » et de « NotPetya », qui ont causé des dommages et des pertes économiques importants dans l'Union. Rançongiciel pour la première, destruction de données pour la seconde, ces

cyberattaques constituent des références par leur ampleur et leurs conséquences. NotPetya, visant principalement l'Ukraine, a eu des effets collatéraux importants, notamment en France (Saint-Gobain, SNCF, Auchan, BNP).

Le 4 octobre 2018, les présidents du Conseil européen et de la Commission européenne et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont ensemble condamné une tentative de cyberattaque visant l'Organisation pour l'interdiction des armes chimiques (OIAC) aux Pays-Bas. Dans une déclaration au nom de l'Union le 12 avril 2019, la haute représentante a exhorté les acteurs à cesser d'entreprendre des cyberactivités malveillantes qui visent à saper l'intégrité, la sécurité et la compétitivité économique de l'Union, y compris les actes d'espionnage portant atteinte à la propriété intellectuelle. Ces « vols cybernétiques » sont notamment ceux commis par le groupe dénommé « APT10 » (« Advanced Persistent Threat 10 »), impliqué dans l'opération « Cloud Hopper » qui a visé les entreprises via le cloud. Pour le Conseil, « l'opération Cloud Hopper a ciblé les systèmes d'information de sociétés multinationales sur six continents, y compris des entreprises situées dans l'Union, et a obtenu un accès non autorisé à des données commercialement sensibles, entraînant des pertes économiques importantes ».

Les sanctions imposées comprennent une interdiction de pénétrer sur le territoire de l'UE et un gel des avoirs. En outre, il est interdit aux personnes et aux entités de l'UE de mettre des fonds à la disposition des personnes et entités inscrites sur la liste.

Les six personnes physiques et les trois personnes morales sont inscrites sur la liste des personnes physiques et morales, entités et organismes figurant à l'annexe I de la décision (PESC) 2020/1127 et du règlement (UE) 2019/796 et jusqu'alors vierge. Deux Chinois et quatre Russes sont visés ainsi que trois organismes : l'un chinois,

l'un nord-coréen, l'un russe. On notera que l'UE n'hésite pas à sanctionner des organes liés aux Etats (Russie en particulier).
Ci-après (p. 147-149) sont reproduits deux extraits qui illustrent la forme que prend cette annexe.

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

Nom	Données d'identification	Les raisons
GAO Qiang	Lieu de naissance: province du Shandong, Chine Adresse : Salle 1102, Manoir de Guanfu, 46 Xinkai Road, Hedong District, Tianjin, Chine Nationalité: chinoise Genre masculin	Gao Qiang est impliqué dans « l'opération Cloud Hopper », une série de cyberattaques à effet significatif provenant de l'extérieur de l'Union et constituant une menace externe pour l'Union ou ses États membres et de cyberattaques ayant un effet significatif contre des États tiers. L'opération « Cloud Hopper» a ciblé les systèmes d'information de sociétés multinationales sur six continents, y compris des entreprises situées dans l'Union, et a obtenu un accès non autorisé à des données commercialement sensibles, entraînant des pertes économiques importantes. L'acteur connu publiquement sous le nom de « APT10 » (« Advanced Persistent Threat 10 ») (alias « Red Apollo », « CVNX », « Stone Panda », « MenuPass » et «Potassium ») a réalisé «Operation Cloud Hopper». Gao Qiang peut être lié à APT10, notamment grâce à son association avec l'infrastructure de commande et de contrôle APT10. De plus, Huaying Haitai, une entité désignée pour fournir un soutien et faciliter « l'opération Cloud Hopper », a employé Gao Qiang. Il a des liens avec Zhang Shilong, qui est également désigné dans le cadre de « l'opération Cloud Hopper ». Gao Qiang est donc associé à la fois à Huaying Haitai et à Zhang Shilong.

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

Nom	Données d'identification	Les raisons
Centre principal des technologies spéciales (GTsST) de la Direction principale de l'état-major général des forces armées de la Fédération de Russie (GU / GRU)	Adresse : 22 Kirova Street, Moscou, Fédération de Russie	Le Centre principal pour les technologies spéciales (GTsST) de la Direction principale de l'état-major général des forces armées de la Fédération de Russie (GU / GRU), également connu sous son numéro de poste sur le terrain 74455, est responsable de cyber-attaques avec un effet significatif provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres et pour les cyberattaques ayant un effet significatif contre des États tiers, y compris les cyberattaques publiquement connues sous le nom «NotPetya» ou «EternalPetya» en juin 2017 et le cyberattaques dirigées contre un réseau électrique ukrainien à l'hiver 2015 et 2016. « NotPetya » ou « EternalPetya » a rendu les données inaccessibles dans un certain nombre d'entreprises de l'Union, de l'Europe au sens large et du monde entier, en ciblant les ordinateurs avec des ransomwares et en bloquant l'accès aux données, entraînant entre autres des pertes économiques importantes. La cyberattaque contre un réseau électrique ukrainien a entraîné la désactivation de certaines parties de celui-ci pendant l'hiver. L'acteur, connu publiquement sous le nom de « Sandworm » (alias

		Les raisons (suite)
		« Sandworm Team », « BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» et «Telebots»), est également à l'origine de l'attaque du réseau électrique ukrainien , « NotPetya » ou « EternalPetya ». Le Centre principal des technologies spéciales de la Direction principale de l'état-major général des forces armées de la Fédération de Russie joue un rôle actif dans les cyber-activités entreprises par Sandworm et peut être lié à Sandworm.« Sandworm Team », « BlackEnergy Group», «Voodoo Bear », « Quedagh », « Olympic Destroyer » et « Telebots »), est également à l'origine de l'attaque du réseau électrique ukrainien , « NotPetya » ou « EternalPetya ». Le Centre principal des technologies spéciales de la Direction principale de l'état-major général des forces armées de la Fédération de Russie joue un rôle actif dans les cyber-activités entreprises par Sandworm et peut être lié à Sandworm.

Encrochat, une enquête exemplaire

EncroChat : le plus gros dossier traité depuis 12 ans par Europol. Le chiffrement de bout en bout au service des criminels mis au clair

Le 2 juillet 2020, lors d'une conférence de presse conjointe d'Europol et d'Eurojust, la gendarmerie nationale et la police néerlandaise ont annoncé avoir mis un terme à l'action de réseaux criminels grâce à la « neutralisation » du chiffrement de bout en bout du réseau téléphonique EncroChat, le « Whatsapp des gangsters », que ces derniers utilisaient. Au-delà de la prouesse technique, cette action a permis l'arrestation de plus de mille personnes, Français, Néerlandais ou Britanniques, la saisie de drogues (10 tonnes de cocaïne et 1 200 kilos de méthamphétamine, plusieurs centaines de kilos de cannabis), le démantèlement de 19 laboratoires de drogues synthétiques, la saisie de dizaines d'armes automatiques, de montres de luxe, de 80 voitures haut de gamme, dont certaines à compartiments cachés, et près de 20 millions d'euros en espèces. Sept conteneurs transformés en chambres de torture ont été découverts aux Pays-Bas.
Plus de 300 enquêtes, également en Espagne, en Allemagne, en Norvège, pourraient être concernées par rebonds. Si le résultat est impressionnant, c'est la technique d'enquête qui mérite un regard particulier.
EncroChat est une entreprise néerlandaise qui offre des services téléphoniques chiffrés, moyennant un abonnement de plus de 2 000 euros par an. Elle a environ 60 000 clients, 90 % d'entre eux étant liés aux milieux criminels. Les modifications apportées par l'entreprise aux smartphones BQ Aquaris X2 ont pour objectif d'empêcher toute traçabilité des conversations et de permettre

d'effacer les données en cas « d'urgence ». Les téléphones fournis sont entièrement modifiés, dépouillés de leurs caméra, micro, système GPS ou port USB. Ils sont alors équipés d'un logiciel de messagerie instantanée chiffrée, couplé à une infrastructure sécurisée. Un code PIN spécial permet la destruction immédiate de toutes les données et un effacement du terminal en cas de saisies consécutives d'un mot de passe erroné. La suppression automatique des messages sur les appareils des destinataires faisait également partie des « garanties » offertes. De ce fait, les intentions d'EncroChat sont manifestes quant à la clientèle servie par cooptation et aux messages d'alerte envoyés pour prévenir les utilisateurs d'une intervention d'autorités gouvernementales.

L'entreprise agissant depuis la France, dans la région de Lille, au profit d'une clientèle mondiale, la gendarmerie nationale a été saisie des faits. Sous le contrôle des magistrats de la Juridiction interrégionale spécialisée de Lille (JIRS), les militaires de la gendarmerie du Centre de lutte contre les criminalités numériques (C3N), du Département sciences de la donnée (DSD), du Service central de renseignement criminel (SCRC), du Bureau des systèmes d'informations et d'investigations (BSII) et du Laboratoire informatique électronique (INL) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) ont été autorisés à mettre en œuvre un « dispositif technique » (couvert par le secret de la défense nationale), destiné à intercepter et à comprendre les conversations téléphoniques sécurisées d'EncroChat.

Les enquêteurs ont eu accès en temps réel aux communications d'environ 60 000 utilisateurs. Près de 120 millions de messages et d'images, presque tous liés à de la criminalité organisée de haut niveau, ont été interceptés, sans que la captation soit détectée. Les travaux de recherche (projet CEREBUS), menés par le SCRC et l'INL de l'IRCGN, ont été facilités grâce à des financements européens.

De cette enquête exemplaire, plusieurs enseignements peuvent être tirés :

• La criminalité organisée utilise tous les moyens numériques, notamment les plus sophistiqués. Les investigations dans l'espace numérique sont désormais au cœur des pratiques professionnelles des enquêteurs. La preuve numérique est, aujourd'hui, la « reine des preuves » ;

• La coopération européenne est une réalité qui se manifeste au travers des équipes communes d'enquête coordonnées par Eurojust et prévues par l'article 13 de la Convention relative à l'entraide judiciaire en matière pénale (29 mai 2000) et par la contribution au financement des recherches techniques. S'il est un domaine qui devrait tempérer les ardeurs des Eurosceptiques, c'est bien celui de la coopération et de la collaboration en matière de lutte contre la cybercriminalité ;

• Le chiffrement de bout en bout est souvent présenté comme un obstacle aux investigations numériques ; dans le cas d'espèce, la démonstration est faite que la meilleure parade réside dans la compétence scientifique et technique des enquêteurs. La gendarmerie nationale a fait un choix stratégique, dont elle perçoit les fruits aujourd'hui. Après avoir démantelé le botnet gênant Retadup (été 2019), elle offre une nouvelle illustration de son savoir-faire. L'augmentation du recrutement « scientifique », notamment à l'École des officiers de la gendarmerie nationale (EOGN), est annonciateur d'une accélération de la mutation de cette institution militaire chargée d'une mission de sécurité.

EncroChat sera assurément au cœur des débats lors du FIC 2021. Un exemple vivant de cybersécurité « collective et collaborative » !

Les décisions de justice accessibles librement en ligne

La loi Lemaire du 7 octobre 2016 a fixé les bases de l'*open data*, c'est-à-dire de la fourniture gratuite sous un format numérique des données, non protégées par le secret, issues des administrations publiques. Les décisions de justice figurent parmi ces informations. Seules les plus significatives étaient jusqu'à présent accessibles, l'essentiel ne pouvant être obtenu qu'à titre onéreux, par le biais notamment de Legaltech. Sont désormais disponibles les décisions rendues publiquement et accessibles à toute personne sans autorisation préalable. Il n'en est pas de même des décisions non définitives, des décisions rendues par les juridictions d'instruction ou de l'application des peines et des décisions rendues par les juridictions pour mineurs ou après des débats tenus à huis clos.

Le décret n° 2020-797 du 29 juin 2020, relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, ouvre de nouvelles perspectives. Le Conseil d'État et la Cour de cassation sont désormais responsables de la mise en ligne dans un délai de 2 mois (décisions du juge administratif) ou de 6 mois (juge judiciaire).

Une des conditions de cette « libération » est l'anonymisation. Celle-ci concerne les auteurs, les victimes et peut porter sur tout autre élément d'identification, dès lors que des considérations de sécurité et de vie privée de tiers ou de leur entourage justifient une occultation.

S'agissant du pénal intéressant davantage les officiers de police judiciaire (OPJ) et les agents de police judiciaire (APJ), sont accessibles les arrêts de la Cour de cassation, les décisions des juridictions de jugement du premier ou du second degré, lorsqu'elles sont définitives et ont été rendues publiquement à la

suite d'un débat public. Le Parquet peut s'y opposer s'il s'agit d'une condamnation effacée par l'amnistie, la réhabilitation ou la révision ou si la condamnation est prescrite. Il en est de même s'il apparaît que la copie est demandée dans l'intention de nuire.
Les décisions seront accessibles via un portail Internet mis en œuvre par le ministère de la Justice. Le traitement massif de données (à l'aide de l'intelligence artificielle) pourrait permettre de mieux mettre en exergue les circonstances de droit et de fait qui fondent une jurisprudence plus homogène. Mais la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice interdit d'effectuer des profilages en utilisant les données d'identité des magistrats et des membres du greffe en vue « d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées ». De même, toute décision à caractère pénal doit tenir compte des circonstances des faits et de la personnalité de l'auteur, conditions constitutionnelles de l'application d'une peine. L'*open data* devra éclairer, mais en aucun cas contraindre la décision par un « enfermement algorithmique ».

Le « dossier pénal numérique »

Le décret n° 2020-767 du 23 juin 2020 crée un traitement de données à caractère personnel dénommé « dossier pénal numérique » mis en œuvre dans chaque juridiction. Prévu par la loi du 20 mars 2019, il a pour finalités de faciliter et d'améliorer le traitement des dossiers pénaux par les magistrats, les greffiers et les personnes habilitées à les assister. Il permettra le recours, pour la conduite de la procédure pénale, au dossier de procédure numérique ainsi qu'à la copie numérisée du dossier, au dossier unique de personnalité relatif aux mineurs et aux minutes dématérialisées. Par ailleurs, le dossier facilitera les échanges

d'informations, au sein des juridictions et entre juridictions, avec les avocats et les parties. Entreront notamment dans la composition du dossier les procès-verbaux et rapports dressés par les officiers ou agents de police judiciaire et les fonctionnaires et agents chargés de certaines fonctions de police judiciaire, les actes d'experts ou de personnes requises. Le décret fixe la liste des données pouvant être enregistrées. Il précise que les données, visées à l'article 6 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ne peuvent être traitées que dans la stricte mesure où ces données sont nécessaires à la poursuite des finalités : il s'agit des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique, les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Sur ces données « sensibles », le Conseil d'État aura prochainement à trancher.

Par le lieutenant Océane GERRIET

Bref rappel sur le contrôle des accès au lieu de travail

La Commission nationale de l'informatique et des libertés (CNIL) a annoncé avoir mis en demeure plusieurs organismes privés et publics « de mettre leurs dispositifs de contrôle des horaires en conformité avec le RGPD » à la suite de plusieurs plaintes reçues[1]. Ces derniers utilisaient en effet un système de badge qui intègre également la prise d'une photo systématique à chaque pointage. Voici l'occasion de faire un bref rappel sur les règles entourant le contrôle des accès au travail.

D'emblée, il convient de rappeler qu'il est tout à fait légitime de vouloir contrôler les accès de son entreprise ou de son administration. Sur ce point, la CNIL avait d'ailleurs rédigé une norme simplifiée sur ce type de traitement récurrent. La base légale communément admise est l'obligation légale, notamment l'obligation de sécurité à laquelle est tenu l'employeur (article L. 4121-1 du Code du travail) et/ou l'intérêt légitime de ce dernier, notamment, d'assurer l'intégrité de ses locaux, voire de préserver la discrétion nécessaire à ses activités.

Toutefois, ce type de traitement doit bien évidemment respecter les principes inhérents à la protection des données personnelles. Si l'entreprise ou l'administration n'a plus à réaliser de déclaration

1. CNIL, Badgeuses photo : mise en demeure de plusieurs employeurs pour collecte excessive de données, *cnil.fr*, 27 août 2020. Disponible sur : https://www.cnil.fr/fr/badgeuses-photo-mise-en-demeure-de-plusieurs-employeurs-pour-collecte-excessive-de-donnees

préalable auprès de la CNIL, elle doit néanmoins faire preuve de responsabilité en entreprenant des démarches de conformité « par défaut », notamment, la tenue d'un registre[2], voire une analyse de risque en cas de risque élevé pour les données[3].

Après avoir rappelé les finalités poursuivies, l'organisme devra s'attacher à justifier chacune des données qu'il entend collecter, le tout dans le strict respect du principe de minimisation des données et c'est précisément sur ce point que la CNIL a effectué une mise en garde. L'article 5.1.c du Règlement général sur la protection des données (RGPD) rappelle que les données traitées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités [du traitement] ». Dans le cas d'espèce, il s'agit essentiellement de permettre l'accès aux locaux professionnels aux seules personnes autorisées et/ou de contrôler leurs horaires de travail, de sorte que l'on comprend aisément que les données relatives à leur identité sont importantes : le nom, le prénom, le genre, la date de naissance (permettant éventuellement de comparer avec une autre pièce d'identité) et une photographie. Cette dernière permet de s'assurer de la correspondance entre le

2. L'article 30 du RGPD exige que « chaque responsable du traitement [RT] (…) [tienne] un registre des activités de traitement effectuées sous [sa] responsabilité ». Ce registre comporte les informations suivantes : nom et coordonnées du RT, les finalités du traitement, la description des catégories de personnes concernées et des catégories de données à caractère personnel, les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales, les éventuels transferts de données, la durée de conservation des données et une description générale des mesures de sécurité techniques et organisationnelles mises en place.

3. Le Comité européen de la protection des données a émis des lignes directrices (WP 248) fixant une liste de 9 critères (indépendants les uns des autres) caractérisant la présence d'un risque pour les données.

porteur de la carte et le badge qu'il présente. Toutefois, les organismes soumis à une mise en demeure sont allés (beaucoup) trop loin en prenant systématiquement leurs employés en photo dès qu'ils passaient leur badge. La CNIL opère alors l'analyse de la nécessité des moyens mis en place au regard de la finalité. D'une part, elle souligne que la simple utilisation du badge suffisait à remplir les finalités poursuivies par le traitement puisqu'elle permet d'assurer le contrôle des accès et des horaires. D'autre part, elle remarque que les photographies réalisées à chaque passage étaient très rarement (voire pas du tout) utilisées par les services de sécurité. Partant, elle ne pouvait que conclure à **l'excessivité** de cette collecte et a ordonné aux organismes concernés de se conformer au RGPD dans un délai de 3 mois.

Cette décision ne surprend pas mais elle ne signifie pas pour autant que des mesures plus strictes ne peuvent pas être prises mais qu'elles doivent être *« dûment justifiées »*. Il est intéressant de souligner que nombre d'entreprises dans des secteurs sensibles peuvent être amenées à utiliser, par exemple, des données biométriques[4] aux fins de renforcer la sécurité de leurs accès. Par principe, et conformément à l'article 9 du RGPD, le traitement de ces données sensibles est prohibé mais comprend, comme tout principe, des exceptions limitativement énumérées dont deux peuvent être évoquées, car adéquates à une telle finalité. D'une part, le traitement est possible lorsqu'il est nécessaire pour des motifs d'intérêt public importants. Il est permis de penser que la protection

4. Définition de l'article 4 du RGPD : « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».

des sites d'intérêts vitaux de l'État pourrait rentrer dans ce cadre, au regard de la sensibilité du lieu et des risque encourus pour la sûreté de l'État. D'autre part, le traitement est possible lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée. À titre d'exemple, on pourrait imaginer le cas où l'entreprise manipule des produits chimiques dangereux, de sorte que seules les personnes habilitées et compétentes doivent accéder aux locaux. Dans une délibération du 10 janvier 2019, la CNIL rappelle les règles inhérentes au traitement de telles données dans le cadre du contrôle des accès. Ainsi, le responsable de traitement doit démontrer que le recours à ces données sensibles est justifié **par l'insuffisance des autres moyens d'identification ou par « des mesures organisationnelles et techniques de protection » qui ne permettent pas d'atteindre le niveau de sécurité exigé**. À ce titre, elle exige du responsable de traitement qu'il « détaille (…) le contexte spécifique » rendant nécessaire ce haut niveau de protection et les raisons du recours à cette technologie dans un document **exhaustif**. Par conséquent, et sans que cela n'étonne, l'autorité de contrôle est particulièrement exigeante vis-à-vis de la mise en œuvre d'un tel traitement.

En tous les cas, ces mises en demeure rappellent que **le principe de minimisation des données** est primordial dans toute démarche de conformité. Cela a, par ailleurs, déjà été rappelé par les hautes juridictions françaises. En effet, la CNIL évoque une jurisprudence de la Cour de cassation[5] et une du Conseil d'Etat[6] ayant eu à apprécier l'opportunité de la mise en place de la géolocalisation pour contrôler le temps de travail des employés. À l'unisson, les magistrats ont estimé que la collecte d'une telle donnée était

5. Soc., 19 décembre 2018, n° 17-14.631.
6. CE, 15 décembre 2017, n° 403776.

excessive eu égard à la finalité qui pouvait être accomplie par d'autres moyens, même « moins efficaces ».

Force est de constater que ces jurisprudences et ce rappel de la CNIL doivent être mis en perspective avec l'essence même du droit de la protection des données. Pour mémoire, le RGPD a consacré ce droit comme « un droit fondamental ». Son premier considérant souligne également qu'un traitement de données à caractère personnel « devrait être conçu pour servir l'humanité ». En ce sens, la CNIL émet une incise intéressante dans sa publication puisqu'elle rappelle aux managers leur rôle essentiel : l'encadrement de leurs employés. Or, cet objectif peut être poursuivi par tout autre moyen et n'a pas besoin de « reposer sur des technologies intrusives ». Ainsi, les nouvelles technologies ne doivent pas apparaître comme une fin en soi mais devraient rester des « outils » et ne pas se substituer aux tâches et aux missions qui relèvent de l'Homme intrinsèquement et du manager ou du chef de surcroît. Une badgeuse, visant à contrôler notamment l'arrivée et le départ de l'employé, ne saurait remplacer l'action du manager qui doit passer voir ses équipes chaque matin pour dire bonjour et s'assurer de leur départ chaque soir. Un tableau de suivi (très utile) ne suffit pas et ne doit pas remplacer les réunions de service (y compris à distance en période de crise sanitaire) qui permettent de faciliter les échanges et de créer / renforcer les liens dans l'équipe. Les applications de messagerie utiles pour communiquer et échanger en tout temps et en tout lieu ne doivent jamais se substituer aux contacts humains et préserver l'oralité. Bref, si les nouvelles technologies s'immiscent chaque jour un peu plus dans notre quotidien, peut-être que le défi de demain sera d'être plus « humain » et non « transhumain »[7] comme l'a rappelé l'édition 2020 du Forum

7. Alain Damasio, Michel Lévy-Provençal, Demain, serons-nous très humains plutôt

international de la cybersécurité dont le thème était : « *Replacer l'humain au cœur [de la cybersécurité] »*.[8]

que transhumains ?, *huffingtonpost.fr*, 5 avril 2015, mise à jour le 5 octobre 2016 [Consulté le 8 septembre 2020]. Disponible sur : https://www.huffingtonpost.fr/alain-damasio/humanisme-transhumanisme_b_6998646.html

8. ObservatoireFIC.com. Disponible sur : https://observatoire-fic.com/fic-2020-replacer-lhumain-au-coeur-de-la-cybersecurite/

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

OCTOBRE 2020

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

Par le G^al^ d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE EUROPÉENNE

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.

Pour les juges de Luxembourg, le droit de l'Union s'oppose à la transmission ou à la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation. Toutefois, pour la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, il est possible de prévoir la conservation ciblée de ces données ainsi que leur conservation rapide. Une telle ingérence dans les droits fondamentaux doit être assortie de garanties effectives et contrôlée par un juge ou une autorité administrative indépendante. Dans des situations dans lesquelles un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, celui-ci peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant, par des mesures législatives, une conservation généralisée et indifférenciée de ces

données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.
La complexité de l'arrêt et l'étendue de ses conséquences sur les pratiques professionnelles des enquêteurs et des services de renseignement nécessitent un examen approfondi par les ministères (Justice, Intérieur, Armées). Cet arrêt fera l'objet d'un examen plus approfondi dans *La veille juridique* du mois de novembre 2020.

I) L'applicabilité de la « directive vie privée et communications électroniques »[1]

La Cour considère que des réglementations nationales imposant aux fournisseurs de services de communications électroniques de conserver des données relatives au trafic et à la localisation ou encore de transmettre ces données aux autorités nationales de sécurité et de renseignement relèvent du champ d'application de la directive. Plusieurs États membres, dont la France, ont soumis des observations écrites à la Cour pour exprimer un avis divergent en faisant notamment valoir que cette directive ne trouverait pas à s'appliquer aux réglementations nationales qui ont pour finalité la sauvegarde de la sécurité nationale, qui relèverait de leur seule compétence, notamment en vertu de l'article 4, paragraphe 2, troisième phrase, TUE.

Pour la CJUE, la « directive vie privée et communications électroniques »[2] ne permet pas que devienne la règle la dérogation

1. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.
2. Article 15, paragraphes 1 et 3, de la directive 2002/58.

à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et à l'interdiction de stocker ces données. Ceci implique que cette directive n'autorise les États membres à adopter à des fins de sécurité nationale, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic[3], que dans le respect des principes généraux du droit de l'Union – parmi lesquels figure le principe de proportionnalité – et des droits fondamentaux garantis par la Charte[4].

II) Fin de la conservation généralisée des données

Le droit de l'Union – notamment l'article 23, paragraphe 1, du règlement général sur la protection des données, lu à la lumière de la Charte – s'oppose à une réglementation nationale imposant, à titre préventif, aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement, la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale. Ces obligations, selon les juges, constituent des ingérences particulièrement graves dans les droits fondamentaux garantis par la Charte, sans que le comportement des personnes dont les données sont concernées présente de lien avec l'objectif poursuivi par la réglementation en cause.

3. Article 5, paragraphe 1, de la directive 2002/58.
4. En particulier, les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la Charte.

III) Un tempérament pour la sécurité nationale

Dans des situations dans lesquelles un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas au fait d'enjoindre aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation. L'État peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant, par des mesures législatives, une conservation généralisée et indifférenciée de ces données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. La décision prévoyant cette injonction doit faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties prévues.

Le risque pour la sécurité nationale est donc considéré comme le plus grave par la CJUE. Pour les services de renseignement, l'arrêt impacte évidemment le statut de la Commission nationale de contrôle des techniques de renseignement (CNCTR) qui, tout en étant une autorité administrative indépendante, ne donne qu'un avis. En lui donnant un pouvoir de décision en lieu et place du Premier ministre, c'est l'architecture même de la police administrative et la responsabilité du gouvernement qui sont remises en cause par un arrêt prononcé par des magistrats européens dont un seul est français. Il ne s'agit pas de remettre en cause la légitimité de la CJUE en fonction de sa composition du moment, mais de souligner qu'en matière de sécurité nationale, la

souveraineté ne saurait être déléguée à d'autres juges que des juges nationaux appliquant un droit national respectueux d'un ordre constitutionnel qui, sous réserve d'un contrôle par la Cour européenne des droits de l'Homme (CEDH), ne saurait être interprété en s'appuyant sur des règles communautaires qui ont été élaborées pour le développement du Marché unique.

IV) Un tempérament pour la lutte contre la criminalité grave

S'agissant de la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, un État membre peut également prévoir la conservation ciblée desdites données ainsi que leur conservation rapide. Une telle ingérence dans les droits fondamentaux doit être assortie de garanties effectives et contrôlée par un juge – ce qui est le cas en France s'agissant du juge des libertés et de la détention ou des juridictions d'instruction – ou par une autorité administrative indépendante. De même, il est possible de procéder à une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication, dès lors que la durée de conservation est limitée au strict nécessaire ou encore de procéder à une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, sans que cela soit dans ce dernier cas limité à un délai particulier.
La directive ne s'oppose pas à une mesure législative permettant le recours à une conservation rapide des données dont disposent les fournisseurs de services, dès lors que se présentent des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà des délais légaux de conservation des données aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, lorsque ces infractions ou atteintes ont déjà été

constatées ou lorsque leur existence peut être raisonnablement soupçonnée. En outre, la Cour juge que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir au recueil en temps réel, notamment, des données relatives au trafic et à la localisation, lorsque ce recueil est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées, d'une manière ou d'une autre, dans des activités de terrorisme et lorsqu'il est soumis à un contrôle préalable, effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, s'assurant qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence, le contrôle doit intervenir dans de brefs délais. Donc, en dehors de l'atteinte grave à la sécurité publique, il faut attendre que l'infraction ait été commise, ce qui n'est guère pertinent en matière de prévention. En outre, les faits doivent relever de la criminalité grave. La « criminalité grave » n'est pas définie par les juges. Si l'on doit se référer à celle de « serious crime » on n'est guère avancé. De nombreuses affaires judiciaires, aujourd'hui résolues, le sont grâce aux données de connexion récupérées sur une période d'un an avant la commission des faits. Ce sont ces données qui conduisent vers l'auteur. La Cour inverse le problème et exige que l'on ait des raisons de soupçonner l'auteur pour exiger la production de données qui n'ont guère d'intérêt pour la compréhension du passé et n'empêchent pas la commission de l'infraction.

V) Effet immédiat et rétroactif

Enfin, la CJUE juge « qu'une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, à l'égard d'une réglementation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, jugée incompatible avec la directive "vie privée et communications électroniques", lue à la lumière de la Charte ».

La Cour rappelle que l'admissibilité et l'appréciation d'éléments de preuve qui ont été obtenus par une conservation de données contraire au droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, relève, en l'état actuel du droit de l'Union, du seul droit national. Toutefois, la Cour précise que la directive « vie privée et communications électroniques », interprétée à la lumière du principe d'effectivité, exige que le juge pénal national écarte des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation incompatible avec le droit de l'Union, dans le cadre d'une telle procédure pénale, si les personnes soupçonnées d'actes de criminalité ne sont pas en mesure de prendre efficacement position sur ces éléments de preuve.

Autrement dit, la plupart des procédures en cours sont fragilisées, ne serait-ce par l'effet de cascade : une donnée de connexion peut entraîner une interpellation, une garde à vue, la production d'une preuve numérique par perquisition ou saisie.

Depuis le 6 octobre 2020, les autorités nationales se réunissent régulièrement, notamment dans les ministères ou à Matignon, pour

trouver une solution juridique. Il est inévitable de modifier rapidement le droit européen et notamment la directive 2002/58 afin d'en exclure clairement le champ de la sécurité nationale (dans toutes ses composantes). Alors que l'Europe est divisée entre les « fédéralistes » et les partisans d'une Europe des nations, le consensus n'est pas pour demain !

Par le Capitaine Matthieu AUDIBERT

JURISPRUDENCE JUDICIAIRE

Code de déverrouillage d'un téléphone portable

Cour de cassation – Chambre criminelle – Arrêt n° 1804 du 13 octobre 2020 n° 20-80.150

Le code de déverrouillage d'un téléphone portable peut constituer « une convention secrète de déchiffrement d'un moyen de cryptologie » au sens de l'article 434-15-2 du Code pénal. Le fait de refuser de communiquer le code de déverrouillage de son téléphone à la demande officielle d'un officier de police judiciaire est une infraction au sens de l'article susvisé, dès lors qu'il est démontré que ce code a un impact sur le chiffrement des données du téléphone et que ce téléphone est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit.

L'article 434-15-2 du Code pénal sanctionne de « trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale (…) ».

Le « moyen de cryptologie » est défini par l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie

numérique (LCEN).
Ainsi, « on entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité ».

Le 8 mars 2017, Malek B. est interpellé par des fonctionnaires de police pour avoir acquis, détenu et transporté sans autorisation des produits stupéfiants. Placé en garde à vue, il refuse de communiquer le code de déverrouillage de l'un de ses téléphones et argue de son droit au silence. Dès lors, il est renvoyé devant le tribunal correctionnel de Créteil le 10 mars 2017 pour avoir acquis, détenu et transporté sans autorisation des produits stupéfiants et pour avoir refusé de communiquer le code de déverrouillage de son téléphone.

Le prévenu a alors soulevé une question prioritaire de constitutionnalité (QPC) devant le tribunal correctionnel en arguant notamment que l'article 434-15-2 précité ne permettrait pas au mis en cause de faire usage de son droit au silence et serait contraire au droit de ne pas s'auto-incriminer. Dans un arrêt du 10 janvier 2018[1], la Chambre criminelle de la Cour de cassation a jugé que cette question n'avait pas été examinée par le Conseil constitutionnel et présentait dès lors un caractère sérieux justifiant sa saisine.
Dans sa décision n° 2018-696 QPC du 30 mars 2018, le Conseil

1. Criminelle, 10 janvier 2018, n° 17-90.019.

constitutionnel rejette les arguments soulevés par la défense de Malek B. En effet, le fondement juridique de cette infraction s'attache, d'une part, à la poursuite par le législateur d'une volonté de protéger la prévention des infractions et, d'autre part, à la recherche de leurs auteurs, ces deux objectifs étant nécessaires à la sauvegarde de droits et de principes à valeur constitutionnelle.

Ainsi, cette infraction ne méconnaît pas le droit ne pas contribuer à sa propre incrimination, ni le droit au respect de la vie privée, les droits de la défense, le principe de proportionnalité des peines ou encore la liberté d'expression. Cette infraction est donc conforme à la Constitution. Toutefois, le Conseil constitutionnel pose deux conditions : d'une part, la demande doit émaner de l'autorité judiciaire, garante du procès équitable, d'autre part, ce moyen de cryptologie doit être susceptible d'avoir été utilisé pour *« préparer, faciliter ou commettre une infraction ».*

Cette seconde condition exige que les investigations préalablement réalisées dans le cadre d'une enquête ou d'une information judiciaire aient mis en évidence un lien entre ces données et la préparation, la facilitation ou la commission d'une infraction.

En outre, le Conseil constitutionnel rappelle que cette disposition n'a ni pour objet d'obtenir des aveux de la part du mis en cause, ni de reconnaître ou poser une présomption de culpabilité, mais simplement de permettre le déchiffrement de données chiffrées par la personne ayant connaissance de cette convention[2].

Sur ce point, il convient de souligner que la Chambre criminelle a adopté la même position que le Conseil constitutionnel au regard de l'article 6 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, par un arrêt du 10

2. LACAZE M. Constitutionnalité du refus de remise d'une convention secrète de déchiffrement, *AJ Pénal*, 2018, p. 257.

décembre 2019[3].

L'article 434-15-2 du Code pénal a fait donc l'objet d'un contrôle de constitutionnalité et d'un contrôle de conventionnalité favorables.

Fort de l'analyse du Conseil constitutionnel, le tribunal correctionnel condamna Malek B. pour cette infraction. Celui-ci fit appel et la Cour d'appel de Paris a alors examiné si le fait pour Malik B. de refuser de communiquer le code de déverrouillage de son téléphone au fonctionnaire de police était constitutif ou non de l'infraction prévue par l'article 434-15-2 du Code pénal.

S'agissant de la réquisition délivrée par les autorités judiciaires, la Cour d'appel relève qu'aucun élément ne ressort de la procédure tendant à démontrer qu'une réquisition avait été adressée par une autorité judiciaire à Malek B. afin qu'il communique le code de déverrouillage de son téléphone, ce dernier n'ayant opposé son refus qu'à un fonctionnaire de police. Ainsi, pour la Cour d'appel de Paris, les officiers de police judiciaire ne font pas partie de l'autorité judiciaire qui comprend les magistrats du Parquet et ceux du siège[4].

Concernant le « moyen de cryptologie », la Cour d'appel s'appuie sur l'article 29 de la LCEN précité pour juger que, concernant les téléphones portables d'usage courant, le code de déverrouillage permet d'accéder aux données qu'il contient, et donc à ses messages, mais ne permet pas en revanche de déchiffrer les données contenues. Le code de déverrouillage n'est pas donc pas, pour la Cour d'appel, une convention secrète de chiffrement d'un

3. Criminelle, 10 décembre 2019, n° 18-86.878.
4. Conseil constitutionnel, 11 août 1993, n° 93-326 DC, §5.

moyen de cryptologie.

Pour ces deux motifs, la Cour d'appel de Paris a prononcé la relaxe de Malek B. s'agissant de l'infraction prévue par l'article 434-15-2 du Code pénal par arrêt du 16 avril 2019[5].

Cet arrêt de la Cour d'appel de Paris était très critiquable. En effet, qu'il s'agisse des téléphones fonctionnant sous Android ou iOS, les données sont automatiquement chiffrées, soit par un système AES-128 bits (Android), soit par AES-256 bits (Apple). Ces systèmes sont directement implémentés dans le smartphone de manière physique via une puce intégrée (Soc « system on a chip » fonctionnant comme un microprocesseur) qui génère elle-même la clé, intrinsèquement inaccessible au constructeur comme à l'utilisateur. Elle est en effet située dans un environnement sécurisé nommé « TEE » (*Trusted Execution Environment*).

Toutefois, considérer qu'un code de téléphone n'est pas une convention secrète de déchiffrement n'est pas évident, ce code ne pouvant être réduit à une simple fonction d'authentification. Pour reprendre les termes de la professeure Agathe Lepage, « certains portables (…) associent le code de déverrouillage à une fonction automatique de protection des données »[6].

Pour abonder en ce sens, la documentation technique des constructeurs, notamment Apple, apporte des précisions. Le guide de sécurité du système d'exploitation iOS, dans sa version de mai 2019, que la société a rendu publique, expose qu'à chaque fois qu'un

5. Paris, 16 avril 2019, n° 18/09267.
6. LEPAGE A., Un an de droit pénal du numérique, *Droit Pénal*, 2019, n° 12.

fichier est créé, le système de protection des données crée une nouvelle clé permettant de le chiffrer (p. 16).
S'agissant du code de déverrouillage, il est indiqué (p. 20) que, par la configuration d'un code sur l'appareil, l'utilisateur active la protection des données de façon automatique. Il est par ailleurs précisé (p. 21) que plus le code est complexe et long, plus la clé de chiffrement l'est. Nous pouvons donc en conclure que, pour ce type d'appareils, la typologie et la dureté du code de déverrouillage ont un impact sur la clé de chiffrement des données contenues dans le terminal. Dès lors, la fonction du code de déverrouillage dépasse le simple mécanisme d'authentification et a un rôle sur le chiffrement et donc le déchiffrement des données présentes dans le téléphone.

Pour les téléphones fonctionnant sous Android, il est possible de chiffrer l'intégralité d'une mémoire de stockage. Cette fonction est nommée « Full Disk Encryption » et existe depuis la version 5.0 d'Android. Le système utilise une clé de chiffrement de 128 bits dénommée clé DEK. Celle-ci est elle-même chiffrée par une clé dite clé KEK. La clé KEK est créée à partir du code de déverrouillage de l'utilisateur. Depuis la version 7 d'Android, il est possible de chiffrer individuellement les fichiers (*File Based Encryption* ou FBE). Avec cette fonction, un fichier est chiffré par AES avec une clé DEK de 512 bits. La clé DEK est ensuite chiffrée par une autre clé de 256 bits (clé KEK). La clé KEK est stockée dans une zone sécurisée du téléphone qui est isolée et indépendante du système Android (zone TEE).
Pour obtenir cette clé KEK afin de déchiffrer les données, il faut trois éléments cumulatifs : le code d'authentification créé lors de la connexion de l'utilisateur, une somme de contrôle (*hash*) calculée à partir d'un fichier stocké dans l'espace de l'utilisateur, un code nommé *Stretched Credential* calculé par une fonction de dérivation

de clé qui utilise le code de déverrouillage de l'utilisateur. Ainsi, ce code de déverrouillage créé par l'utilisateur est indispensable pour récupérer la clé KEK afin de déchiffrer les données. Il a donc un rôle sur le chiffrement des données présentes dans le téléphone[7].

Suite à l'arrêt de la Cour d'appel de Paris, il convient de relever que le Parquet général près la cour d'appel ne s'est pas pourvu en cassation. Toutefois, cet arrêt était susceptible d'engendrer des conséquences fâcheuses pour les enquêteurs. Depuis les révélations d'Edward Snowden, le grand public a largement adopté les applications de communication chiffrées. En outre, les fabricants de téléphones et les concepteurs des systèmes d'exploitation et d'applications ont largement renforcé la sécurité des terminaux. Ainsi, comme le notent Benoist Hurel et Vincent Lemonier, « aujourd'hui, il n'est malheureusement pas exagéré d'affirmer que des enquêtes portant sur des structures criminelles majeures sont rendues impossibles, ou sont extrêmement ralenties, par l'utilisation de messageries cryptées que les enquêteurs ne peuvent pas intercepter en temps réel »[8].

Ainsi, comme le prévoit l'article 620 du Code de procédure pénale et suite à l'ordre formel donné par le ministre de la Justice, le procureur général près la Cour de cassation s'est pourvu en cassation dans l'intérêt de la loi. Ce pourvoi particulier permet au procureur général près la Cour de cassation de dénoncer à la Chambre criminelle des « actes judiciaires, arrêts ou jugements

7. *Connection between PIN/password and encryption keys in Android.* Disponible sur : https://security.stackexchange.com/questions/196230/connection-between-pin-password-and-encryption-keys-in-android

8. HUREL B., LEMONIER V., L'enquête pénale à l'épreuve du chiffrement, *Délibérée*, vol. 4, n° 2, 2018, p. 53-57.

contraires à la loi, ces actes, arrêts ou jugements peuvent être annulés ». Si l'arrêt est rendu en dernier ressort, ce qui est le cas en l'espèce de l'arrêt de la Cour d'appel de Paris, et que le pourvoi est accueilli, « la cassation est prononcée, sans que les parties puissent s'en prévaloir et s'opposer à l'exécution de la décision annulée »[9].

Dans ce pourvoi, deux questions étaient posées à la Chambre criminelle :

• Un officier de police judiciaire peut-il demander à un mis en cause de communiquer le code de déverrouillage d'un téléphone portable et, si la réponse est affirmative, sous quelle forme ?

• Le code de déverrouillage d'un téléphone portable peut-il constituer une convention secrète de déchiffrement d'un moyen de cryptologie ?

Concernant la première question, la Cour d'appel a noté qu'aucune réquisition n'a été adressée par une autorité judiciaire à Malek B. de communiquer son code de déverrouillage, celui-ci ayant seulement refusé de communiquer ce code à la suite d'une demande qui lui a été faite au cours de son audition par un fonctionnaire de police. Sur ce point, la Chambre criminelle considère que la Cour d'appel a justifié sa décision.

Toutefois elle précise que « c'est à tort qu'elle a énoncé que cette réquisition ne pouvait être délivrée par un fonctionnaire de police, alors que la réquisition délivrée par un officier de police judiciaire agissant en vertu des articles 60-1, 77-1-1 et 99-3 du code de

9. Article 621 du Code de procédure pénale.

procédure pénale, dans leur rédaction applicable au litige, sous le contrôle de l'autorité judiciaire, entre dans les prévisions de l'article 434-15-2 du code pénal ». Elle indique également qu'une « simple demande formulée au cours d'une audition, sans avertissement que le refus d'y déférer est susceptible de constituer une infraction pénale, ne constitue pas une réquisition au sens du texte précité ».

Autrement dit, l'officier de police judiciaire qui demande le code de déverrouillage d'un téléphone doit matérialiser sa demande et avertir le mis en cause que son éventuel refus constituerait l'infraction prévue par l'article 434-15-2 du Code pénal.

À ce titre, la motivation de la Chambre criminelle est parfaitement logique.
En effet, il convient de rappeler que les dispositions citées en référence à ce même article, « titres II et III du livre 1er du code de procédure pénale », renvoient aux pouvoirs généraux de réquisitions des officiers de police judiciaire, à savoir les articles 60, 60-1, 60-2 dans le cadre de l'enquête de flagrance, 77-1-1, 77-1-2 dans le cadre de l'enquête préliminaire et 99-3 et 99-4 dans le cadre de l'information judiciaire. En outre, « la police judiciaire est exercée, sous la direction du procureur de la République, par les officiers, fonctionnaires et agents désignés au présent titre »[10]. De plus, « le procureur de la République procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions pénales. À cette fin, il dirige l'activité des officiers et agents de la police judiciaire dans le ressort de son tribunal. Il peut, en outre, requérir tout officier de police judiciaire, sur l'ensemble du territoire national, de procéder aux actes d'enquête qu'il estime nécessaires

10. Article 12 du Code de procédure pénale.

dans les lieux où chacun d'eux est compétent (…) »[11].

S'agissant de la seconde question, la Cour d'appel avait écarté la possibilité pour le code de déverrouillage de constituer une convention secrète de déchiffrement d'un moyen de cryptologie. Elle indiquait qu'un « code de déverrouillage d'un téléphone portable d'usage courant, s'il permet d'accéder aux données de ce téléphone portable et donc aux éventuels messages qui y sont contenus, ne permet pas de déchiffrer des données ou messages cryptés et, en ce sens, ne constitue pas une convention secrète d'un moyen de cryptologie ».
Sur ce point, la Chambre criminelle adopte une position radicalement différente de celle de la Cour d'appel. Elle rappelle que « la convention secrète de déchiffrement d'un moyen de cryptologie contribue à la mise au clair des données qui ont été préalablement transformées, par tout matériel ou logiciel, dans le but de garantir la sécurité de leur stockage, et d'assurer ainsi notamment leur confidentialité ». Elle conclut, dès lors, par une formule lapidaire : « le code de déverrouillage d'un téléphone portable peut constituer une telle convention lorsque ledit téléphone est équipé d'un moyen de cryptologie. »

Faisant œuvre de pédagogie, elle explique le raisonnement *in concreto* que les juges du fond doivent adopter. Ainsi, « l'existence d'un tel moyen peut se déduire des caractéristiques de l'appareil ou des logiciels qui l'équipent ainsi que par les résultats d'exploitation des téléphones au moyen d'outils techniques, utilisés notamment par les personnes qualifiées requises ou experts désignés à cette fin, portés, le cas échéant, à la connaissance de la personne

11. Article 41 du Code de procédure pénale.

concernée ».

Autrement dit, il faut justifier dans la procédure que le code de déverrouillage a un rôle sur le chiffrement du téléphone. Ce qui est le cas, comme nous l'avons démontré, des téléphones fonctionnant sous iOS ou Android. Cela inclut également d'éventuelles applications chiffrées de communication. En outre, la Chambre criminelle précise que ce lien peut être démontré par les résultats d'exploitation des téléphones au moyen d'outils. Il s'agit ici des outils de criminalistique numérique qui équipent les enquêteurs. Connecter le téléphone à ces outils et tenter d'extraire les données sans code de déverrouillage caractérise là encore le lien entre code de déverrouillage et chiffrement des données. Les enquêteurs et les juges du fond doivent donc rentrer dans les caractéristiques des téléphones, la Chambre criminelle jugeant « inopérante » la notion de téléphone d'usage courant.

La Chambre criminelle casse et annule logiquement l'arrêt de la Cour d'appel et ce, dans le seul intérêt de la loi. Cet arrêt n'est donc pas opposable à Malek B. qui demeure relaxé sur ce fondement.

En conclusion, il résulte de cet arrêt que l'infraction est susceptible d'être caractérisée, dès lors qu'une personne refuse de donner le code de déverrouillage de son téléphone sous réserve des quatre conduites suivantes :

- Une demande de remise du code est formulée en procédure :
  • Dans le cadre de l'enquête, par le procureur de la République, l'officier de police judiciaire ou, sous le contrôle de ce dernier, par l'agent de police judiciaire[12],

12. Depuis la loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour

• Dans le cadre de l'instruction préparatoire, par le juge d'instruction ou l'officier de police judiciaire ;

- Il est rappelé à la personne que le refus de répondre à la réquisition est constitutif d'une infraction pénale ;

- Les caractéristiques de l'appareil objet de la réquisition, les logiciels qui l'équipent ou les résultats de son exploitation au moyen d'outils techniques, révèlent qu'il est doté d'un moyen de cryptologie[13] ;

- Le téléphone a été utilisé pour préparer, faciliter ou commettre un crime ou un délit.

Si le chiffrement est utile pour protéger la vie privée, un consensus nécessairement raisonnable doit aboutir. Un chiffrement sans aucune limite servirait davantage les intérêts des malfaiteurs que ceux des citoyens. Cette exception prévue par la loi et exercée sous le contrôle de l'autorité judiciaire permet d'y parvenir à la lumière de l'arrêt rendu par la Chambre criminelle.

---

la justice, l'agent de police judiciaire, dans le seul cadre de l'enquête et sous le contrôle de l'officier de police judiciaire, peut également adresser ce type de réquisition.

13. Ce qui est le cas, comme nous l'avons démontré, de la plupart des téléphones fonctionnant sous iOS ou Android au regard de leurs caractéristiques techniques, le code de déverrouillage du terminal défini par l'utilisateur faisant en effet partie intégrante de la chaîne de chiffrement et de déchiffrement des données qu'il contient.

Par le G^al d'armée (2S) Marc Watin-Augouard

JURISPRUDENCE JUDICIAIRE (SUITE)

Géolocalisation – Information du magistrat

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

La pose d'une balise de géolocalisation par un enquêteur agissant en urgence doit faire l'objet d'une information immédiate du procureur de la République ou du juge d'instruction.

Dans le cadre d'une information judiciaire, des enquêteurs procèdent un matin, à 3H20, à la pose d'un dispositif de géolocalisation sur un véhicule. Ils agissent en vertu des dispositions de l'article 230-35 du Code de procédure pénale. Ils avisent le juge d'instruction à 9h30. Le véhicule fait également l'objet de mesures de sonorisation. Ces dispositifs combinés permettent l'interpellation et la mise en examen de l'auteur. Celui-ci demande à la Cour l'annulation de la mesure de géolocalisation jugée conforme par la chambre de l'instruction.
La Cour considère qu'en cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens et, dans les cas mentionnés aux articles 230-33 et 230-34 du même Code, un officier de police judiciaire (OPJ) peut prescrire ou mettre en place les opérations de localisation en temps réel, par tout moyen technique, d'un véhicule sans le consentement de son propriétaire ou possesseur, à la condition qu'il en informe immédiatement, par tout moyen, le procureur de la

République ou le juge d'instruction. Cette immédiateté se justifie parce qu'elle permet le contrôle effectif du juge sous lequel est placée la mesure de géolocalisation qui constitue une ingérence dans la vie privée. Elle doit être interprétée strictement. Ainsi, « méconnaît l'article 230-35 du code de procédure pénale et viole l'article 8 de la Convention européenne des droits de l'homme, la chambre de l'instruction qui a déclaré régulière la mesure de géolocalisation quand il résultait de ses constatations que les enquêteurs ont procédé à la pose du dispositif de géolocalisation le 28 février 2019 à 3 heures 20 et que le juge d'instruction n'en a été informé que le 28 février 2019 à 9 heures 30, soit 6 heures 10 plus tard ».

Compte Facebook, atteinte à la vie privée du salarié/ Information confidentielle de l'entreprise

Cour de cassation - Chambre sociale - (19-12.058) - Arrêt n° 779 du 30 septembre 2020 - Mme X. / Petit Bateau

La production par un employeur d'images provenant d'un compte Facebook, portant atteinte à la vie privée d'un salarié, peut être indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi, soit la défense de l'intérêt légitime de l'employeur à la confidentialité de ses affaires.

En l'espèce, un chef de projet travaillant pour la marque Petit Bateau publie sur son compte Facebook une photographie de la nouvelle collection printemps/été 2015 présentée exclusivement aux commerciaux de la société. Il est licencié pour faute grave et conteste le mode de preuve en avançant que son compte Facebook est privé, uniquement accessible aux personnes qu'il a acceptées sur

son réseau. Pour sa défense, il considère que la preuve, apportée par un « ami » de la personne travaillant au sein de la société, est déloyale et donc inopposable par l'entreprise qui porte atteinte à sa vie privée. Tout en rappelant que le principe de loyauté dans l'administration de la preuve exclut le recours par l'employeur à un stratagème, la Cour d'appel constate que la publication au cœur du litige a été communiquée à l'entreprise par un courriel d'une autre salariée de l'entreprise autorisée à accéder comme « amie » sur le compte privé Facebook de la personne en cause. Le procédé d'obtention de preuve n'est donc pas déloyal.

La Cour relève que la production par l'employeur d'une photographie extraite du compte privé Facebook d'un salarié, auquel il n'était pas autorisé à accéder, et d'éléments d'identification des « amis », professionnels de la mode, destinataires de cette publication, constitue une atteinte à la vie privée du salarié. Selon les articles 6 et 8 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, les articles 9 du Code civil et du Code de procédure civile, une telle atteinte ne peut être justifiée qu'à la double condition que cette production soit indispensable à l'exercice de la preuve et que l'atteinte soit proportionnée au but poursuivi.

Dans le cas examiné, la Cour relève que la publication constitue une divulgation par la salariée d'une information confidentielle de l'entreprise auprès de professionnels susceptibles de travailler pour des entreprises concurrentes. La production de ces éléments portant atteinte à la vie privée est indispensable à l'exercice du droit à la preuve et proportionnée au but poursuivi : l'intérêt légitime de l'employeur à la confidentialité de ses affaires.

JURISPRUDENCE ADMINISTRATIVE

Plateforme des données de santé

Conseil d'État – N° 444937 – Ordonnance de référé du 13 octobre 2020 – Association nationale du logiciel libre et autres

La Plateforme des données de santé doit conclure, dans un délai de quinze jours à compter de la notification de l'ordonnance, un nouvel avenant aux documents contractuels l'unissant à la société Microsoft Ireland Operations Limited pour préciser que la loi applicable est celle du droit de l'Union ou du droit de l'État membre auquel la société est soumise et que ces modifications s'appliquent à l'ensemble des services fournis par Microsoft susceptibles d'être utilisés pour le traitement de données à caractère personnel du système de santé.

La loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé[1] crée un groupement d'intérêt public (GIP), dénommé « Plateforme des données de santé ». Celui-ci est constitué entre l'État, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs de données de santé et des utilisateurs publics et privés de données de santé, y compris des organismes de recherche en santé. Il est notamment chargé de réunir, organiser et mettre à disposition les données du système national des données de santé mentionné à l'article L. 1461-1 du Code de la santé publique et de

1. La Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé, (art. 41 VIII) crée l'article L. 1462-1 du Code de la santé publique (CSP).

promouvoir l'innovation dans l'utilisation des données de santé. Un avenant à la convention constitutive du groupement d'intérêt public « Institut national des données de santé » portant création du groupement d'intérêt public « Plateforme des données de santé » ou « Health Data Hub » est approuvé le 29 novembre 2019 par un arrêté interministériel. Pour les besoins du stockage et de la mise à disposition des données, la Plateforme des données de santé a signé le 15 avril 2020 avec la société de droit irlandais Microsoft Ireland Operations Limited, filiale de la société américaine Microsoft Corporation, un contrat lui donnant accès à un ensemble de produits « Microsoft Azure » : hébergement des données de santé, concession de licences de logiciels nécessaires au traitement de ces données pour les finalités légalement autorisées. Les données traitées par la Plateforme des données de santé sont hébergées dans des centres de données situés aux Pays-Bas et seront prochainement transférées dans des centres de données situés en France. Elles ne peuvent être traitées que sur la plateforme technologique du groupement d'intérêt public et sur la plateforme de la Caisse nationale de l'assurance maladie, et ne peuvent pas en être extraites. Au sein de ces plateformes, les données ne peuvent contenir ni les noms et prénoms des personnes, ni leur numéro d'inscription au Répertoire national d'identification des personnes physiques, ni leur adresse.

Ce choix est très critiqué, à un moment où la souveraineté est dans tous les discours, mais il est justifié par Cédric O « parce qu'il est le seul capable de répondre aux prérequis au moment où la consultation a été faite ».
La collecte des données de santé et leur traitement en lien avec l'épidémie de Covid-19 ainsi que la collecte et le traitement de données de santé sur le « Health Data Hub » sont au cœur d'un

référé, soutenu par plusieurs associations ou syndicats, référé -liberté qui s'appuie principalement sur l'invalidation du *Privacy Shield* par la Cour de justice de l'Union européenne (arrêt du 16 juillet 2020[2] – voir *supra*, septembre 2020, p. 164-171). La Cour de Luxembourg a, notamment, relevé à propos de cet accord d'adéquation, des ingérences dans les droits fondamentaux des personnes dont les données à caractère personnel sont ainsi transférées, du fait des possibilités d'accès à ces données et d'utilisation de celles-ci par les autorités publiques américaines, dans le cadre de programmes de surveillance, fondés sur l'article 702 du « Foreign Intelligence Surveillance Act » (FISA) ou loi sur la surveillance en matière de renseignement extérieur et, d'autre part, de l' « Executive Order (EO) 12333 ».

Les requérants soutiennent qu'il est porté une atteinte grave et manifestement illégale au droit au respect de la vie privée et au droit à la protection des données personnelles, eu égard à la soumission au droit américain de la société Microsoft choisie pour assurer la solution technique de la Plateforme des données de santé, sans que soient apportées des garanties suffisantes au regard des risques de transfert de données vers les États-Unis et de l'application extraterritoriale du droit américain, dont le *Cloud Act*

---

2. Arrêt de grande chambre du 16 juillet 2020, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems*, C-311/18. La Cour de justice de l'Union européenne a dit pour droit que l'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du règlement 2016/679 doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne par ce règlement, lu à la lumière de la Charte des droits fondamentaux de l'Union européenne.

est une des illustrations les plus topiques. La Commission nationale de l'informatique et des libertés (CNIL) estime, dans ses observations, que le risque ne peut être totalement écarté, rien sur le plan technique ne conduisant à exclure que Microsoft soit amené à faire droit à une demande des autorités américaines fondée sur l'article 702 du FISA.

Le juge des référés est donc saisi en vertu des articles L. 511-1 et L. 521-2 du Code de justice administrative. Il observe que « la Plateforme des données de santé et la société Microsoft Ireland Operations Limited ont conclu, le 3 septembre 2020, un avenant prévoyant, pour les services en ligne "Azure" qu'il énumère, que Microsoft ne traitera pas les données de la Plateforme en dehors de la zone géographique spécifiée par celle-ci sans son approbation et que dans l'hypothèse où un accès aux données serait nécessaire pour les besoins des opérations d'exploitation des services en ligne et de résolution d'incident menées par Microsoft depuis un lieu extérieur à cette zone, il serait soumis à l'autorisation préalable de la Plateforme. La Plateforme des données de santé s'est engagée à l'égard de la Commission nationale de l'informatique et des libertés à refuser tout transfert. Il n'apparaît pas, en l'état de l'instruction, que la Plateforme des données de santé puisse se trouver contrainte, pour des raisons techniques, de donner son accord à un transfert de données de santé ».
Le Conseil d'État relève que, par un arrêté du 9 octobre 2020[3] postérieur à l'introduction de la requête, le ministre des Solidarités et de la Santé a complété l'article 30 de l'arrêté du 10 juillet 2020[4],

3. Art. 1 modifiant le deuxième alinéa du III de l'article 30 de l'arrêté du 10 juillet 2020 : « Aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne ».
4. Arrêté du 10 juillet 2020 prescrivant les mesures générales nécessaires pour faire

relatif aux mesures concernant le traitement des données à caractère personnel du système de santé, pour prévoir qu'aucun transfert de données à caractère personnel ne peut être réalisé en dehors de l'Union européenne.

Avant de rejeter la demande objet du référé, en l'absence d'urgence et d'atteinte grave et manifestement illégale portée à une liberté fondamentale, le Conseil d'État énonce trois observations :
- La Cour de justice s'est seulement prononcée, dans son arrêt du 16 juillet 2020, sur les conditions dans lesquelles peuvent avoir lieu des transferts de données à caractère personnel vers les États-Unis et non sur celles dans lesquelles de telles données peuvent être traitées, sur le territoire de l'Union européenne, par des sociétés de droit américain ou leurs filiales en qualité de sous-traitants, voire de responsables de traitement ;
- Les requérants n'invoquent pas de violation directe du règlement général sur la protection des données mais seulement le risque d'une telle violation, dans l'hypothèse où Microsoft ne serait pas en mesure de s'opposer à une demande d'accéder à certaines données formulées par les autorités américaines, données pseudonymisées par la Caisse nationale d'assurance maladie avant d'être transmises à la Plateforme et chiffrées au moyen des outils mis à sa disposition par Microsoft ;
- Il existe un intérêt public important à permettre la poursuite de l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le SARS-CoV-2 et, à cette fin, de permettre le recours aux moyens

face à l'épidémie de covid-19 dans les territoires sortis de l'état d'urgence sanitaire et dans ceux où il a été prorogé. Disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042106233/

techniques, sans équivalent à ce jour, dont dispose la Plateforme des données de santé par le biais du contrat passé avec Microsoft.

Mais, eu égard à la sensibilité particulière des données de santé et en attendant qu'un nouveau sous-traitant soit choisi, conformément aux annonces du secrétaire d'État chargé de la transition numérique et des communications électroniques, le juge enjoint à la Plateforme des données de santé de continuer de rechercher, en vertu de l'article 28 du Règlement général sur la protection des données, la mise en œuvre par Microsoft des mesures techniques et organisationnelles appropriées pour garantir au mieux la protection des droits des personnes concernées. Par ailleurs, lorsqu'elle autorise des projets appelés à traiter les données rassemblées par la Plateforme des données de santé, la CNIL doit vérifier qu'ils poursuivent une finalité d'intérêt public en lien avec l'épidémie de Covid-19 et que le recours à la Plateforme remplit les conditions.

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

NOVEMBRE 2020

Par le 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…

Par le G^al^ 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.

Dans *La veille juridique* d'octobre 2020 (voir *supra*, p. 164-171), 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. 212-214).

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 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 ».

Par le 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

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.

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 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 permettantd'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

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).

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 :

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

- « 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 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]

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

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

personnes concernées ainsi que la durée de conservation retenue »[9].

La Cour précise deux options envisageables : tout d'abord des 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

9. Point 147.
10. Point 149.
11. Point 150.
12. Points 157-159.

connaissance de l'identité des utilisateurs de ces services ne constituant pas une ingérence grave dans leurs droits.
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.

Sur ce point, la CJUE évoque la conservation rapide de données

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

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].

Ainsi, deux options se présentent :

- Si les données en cause sont soumises à la directive

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.

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 indifférenciée des données[25].

La Cour conclut : le juge national doit écarter « des informations et

22. Point 203.
23. Points 213-228.
24. Point 215.
25. Points 216-220.

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 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

26. Points 221-226.
27. Article 222-33-2-2 du Code pénal.

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 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

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/

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 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

30. Points 152 à 160.
31. Article 53 du Code de procédure pénale.
32. Article 60-1 du Code de procédure pénale.

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, 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 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

---

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

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.

Par le Gal 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[1], 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 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

1. 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.

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.

Par le capitaine Thibaut HECKMANN

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.

Par le Gal 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 ?

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

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