LA VEILLE JURIDIQUE

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

RUBRIQUE

DROIT DE L'ESPACE NUMÉRIQUE

ANNÉE 2019

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

PAR LE LIEUTENANT OCÉANE GERRIET

CREOGN

TABLE DES MATIÈRES

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

Janvier

Février

Juin

Septembre

Octobre

Novembre

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

JANVIER 2019

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

JURISPRUDENCE JUDICIAIRE

Cour de cassation, Chambre sociale (arrêt n° 17-14.631), 19 décembre 2018, Fédération Sud des activités postales et des télécommunications Sud PTT/ société Médiapost

Un système de géolocalisation mis en œuvre par l'employeur n'est légal que s'il est le seul moyen permettant d'assurer le contrôle de la durée du travail des salariés. Il ne peut être justifié lorsque le salarié dispose d'une liberté dans l'organisation de son travail.

La société Médiapost, filiale du groupe La Poste, avait mis en place un système Distrio pour enregistrer, toutes les dix secondes, la localisation des postiers distributeurs, au moyen d'un boîtier mobile que ces employés portaient sur eux lors de leur tournée et qu'ils activaient eux-mêmes. Ce dispositif, contesté par la Fédération Sud des activités postales et des télécommunications (Sud PTT), avait été validé par la cour d'appel de Lyon, laquelle avait considéré le dispositif justifié par la nature de la tâche à accomplir et proportionné au but recherché par l'employeur. Mais la Cour de cassation lui donne tort. Selon l'article L. 1121-1 du Code du travail, *« nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »*. Pour la Haute juridiction, l'utilisation d'un système de géolocalisation pour assurer le contrôle de la durée du travail

n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, même moins efficace que la géolocalisation. Par ailleurs, elle n'est pas justifiée lorsque le salarié dispose d'une liberté dans l'organisation de son travail. La Cour de cassation confirme ainsi sa jurisprudence en la matière (cass.soc., n° 10-18036, du 3 novembre 2011).

JURISPRUDENCE ADMINISTRATIVE

Tribunal administratif de Cergy-Pontoise (N° 1801344, 1801346, 1801348, 1801352) du 4 février 2019

La procédure, prévue par l'article 6-1 de la Loi pour la confiance dans l'économie numérique (LCEN), pour des infractions de provocation directe ou d'apologie d'actes de terrorisme, définies par l'article 421-2-5 du Code pénal, ne peut être mise en œuvre dès lors que les faits ne peuvent être qualifiés d'infractions terroristes au sens de l'article 421-1 du Code pénal.

Par quatre requêtes jointes, la personnalité qualifiée, désignée par la Commission nationale de l'informatique et des libertés (CNIL) au titre de l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 (LCEN), a demandé au tribunal administratif d'annuler des décisions de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), prises à l'automne 2017, enjoignant l'éditeur du site Internet Indymedia, ainsi que des exploitants de moteurs de recherche et annuaires, d'opérer le retrait ou de déréférencer des sites faisant une provocation ou l'apologie de plusieurs incendies criminels ayant

visé des casernes de gendarmerie (Grenoble, Meylan, Limoges) ou la police municipale de Clermont-Ferrand.
Comme le prévoit la LCEN, lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes relevant de l'article 421-2-5 du Code pénal le justifient, l'autorité administrative peut demander à toute personne mentionnée au III de l'article 6 de la présente loi (éditeur) ou aux personnes mentionnées au 2 du I du même article 6 (hébergeurs) de retirer les contenus qui contreviennent à ces mêmes articles 421-2-5 et 227-23. Elle en informe simultanément les personnes mentionnées au 1 du I de l'article 6 de la présente loi (FAI). En l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, l'autorité administrative peut notifier aux personnes mentionnées au même 1 la liste des adresses électroniques des services de communication au public en ligne contrevenant auxdits articles 421-2-5 et 227-23. Ces personnes doivent alors empêcher sans délai l'accès à ces adresses. L'autorité administrative transmet les demandes de retrait et la liste mentionnée, respectivement, aux premier et deuxième alinéas, à une personnalité qualifiée, désignée en son sein par la CNIL pour la durée de son mandat dans cette commission et chargée d'en contrôler la légalité. La personnalité qualifiée s'assure de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste. Si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée peut alors saisir la juridiction administrative compétente, en référé ou sur requête.
Dans les cas d'espèce, le chef de cabinet du ministre de l'Intérieur, par quatre décisions du 8 février 2018, a refusé de suivre les

recommandations de la personnalité qualifiée.
Pour la première fois depuis la promulgation de la loi du 13 novembre 2014 qui a introduit les procédures de retrait, de blocage ou de déréférencement dans la LCEN, l'autorité qualifiée a fait usage de son droit en demandant au juge administratif de constater que la qualification juridique des faits ainsi retenue par l'autorité administrative est erronée, de sorte que les décisions contestées ont été prises en méconnaissance des dispositions de l'article 6-1 de la LCEN.
Le tribunal administratif a été appelé à apprécier la qualification juridique des faits, conformément à la règle d'interprétation stricte de la loi pénale. Pour le tribunal, *« il ressort des pièces du dossier que les incendies criminels revendiqués dans les quatre publications litigieuses sont inspirés par une pensée libertaire et contestataire selon laquelle les forces de sécurité intérieure et, plus généralement, les institutions incarnent un ordre auquel il ne faut pas se soumettre […] »*. Il n'est pas possible, selon la juridiction, de rattacher à une organisation terroriste préexistante les incendies criminels revendiqués dans les publications litigieuses, au regard de leur ampleur, de leur mode d'exécution et de la revendication les accompagnant. En l'absence de tout autre élément matériel révélant l'existence d'une entreprise terroriste, les faits, bien que pénalement répréhensibles, ne peuvent être analysés comme des actes de terrorisme au sens des dispositions précitées de l'article 421-1 du Code pénal.
En conséquence, le tribunal administratif donne raison à l'autorité qualifiée. On notera que, pour les affaires de Grenoble et de Meylan, les informations judiciaires ont été ouvertes pour *« destruction en bande organisée du bien d'autrui par un moyen dangereux pour les personnes »*, infraction prévue par les articles

322-8 1°, 322-6 al.1, 132-71 du Code pénal et réprimée par les articles 322-8 al.1, 322-15,322-16 et 322-18 dudit Code. Le juge judiciaire territorialement compétent n'a pas retenu le caractère terroriste ; la juridiction nationale spécialisée ne s'est pas saisie des faits, comme c'est le cas lorsque la qualification terroriste est établie.

JURISPRUDENCE EUROPÉENNE

CJUE, Affaire C-507/17 Google LLC, venant aux droits de Google Inc. contre Commission nationale de l'informatique et des libertés (CNIL)

Si elle suit les conclusions de l'avocat général, la Cour de justice de l'Union européenne (CJUE) devrait expliciter l'arrêt *Google Spain* en décidant que l'exploitant d'un moteur de recherche n'est pas tenu, lorsqu'il fait droit à une demande de déréférencement, d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur de telle sorte que les liens litigieux n'apparaissent plus, quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée. En revanche, il serait tenu de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur effectuée dans un lieu situé dans l'Union européenne. Dans ce contexte, cet exploitant devrait prendre toute mesure à sa disposition afin d'assurer un déréférencement efficace et complet. Cela inclut, notamment, la technique dite du « géo-blocage », depuis une adresse IP réputée localisée dans l'un des États membres, quel que soit le nom de domaine utilisé par l'internaute qui effectue la

recherche.

La CJUE doit prochainement statuer sur une demande de décisions préjudicielles émanant du Conseil d'État faisant suite à l'arrêt *Google Spain et Google* (affaire C-131/12 du 13 mai 2014) qui a consacré un « droit à l'oubli » dont il ne précise pas le champ d'application géographique. Il est donc demandé à la Cour de préciser la portée territoriale d'un déréférencement et de déterminer si les dispositions de la directive 95/46 exigent un déréférencement à l'échelle nationale, européenne ou mondiale (l'arrêt s'applique à des faits antérieurs au Règlement général sur la protection des données – RGPD).

1/ La saisine de la CJUE par le Conseil d'État

Une personne physique s'est adressée à la CNIL pour faire droit à une demande de suppression de documents référencés par Google et la concernant. Par décision du 21 mai 2015, la présidente de la CNIL a mis la société Google LLC en demeure de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom de la personne, de liens menant vers des pages web et d'appliquer cette suppression sur toutes les extensions de nom de domaine de son moteur de recherche.

Mais Google n'a pas donné suite à cette mise en demeure, en limitant son action à la suppression partielle des liens. Seuls ont été pris en compte les résultats affichés en réponse à des recherches effectuées sur les déclinaisons de son moteur dont le nom de domaine correspond à un État membre de l'Union (.fr, .eu, .de, etc.). N'ont pas ainsi été concernées les recherches via .com ou .org. Le

moteur de recherche exploité par Google explore différents noms de domaine par des extensions géographiques. Grâce à l'identification de l'adresse IP de l'internaute, lorsque la recherche est effectuée depuis « google.com », Google procède, en principe, à une redirection automatique de cette recherche vers le nom de domaine correspondant au pays à partir duquel cette recherche est réputée être effectuée. L'internaute peut cependant, sans considération de sa localisation, effectuer ses recherches sur les autres noms de domaine du moteur de recherche. Par ailleurs, si les résultats peuvent différer selon le nom de domaine à partir duquel la recherche est effectuée sur le moteur, les liens affichés en réponse à une recherche proviennent de bases de données et d'un travail d'indexation communs.

À l'issue du délai de mise en demeure, Google a proposé une solution de « géo-blocage », consistant à supprimer la possibilité d'accéder, depuis une adresse IP réputée localisée dans l'État de résidence de la personne concernée, aux résultats litigieux obtenus à la suite d'une recherche effectuée à partir de son nom, quelle que soit la déclinaison du moteur de recherche sollicitée par l'internaute. Cette proposition a été jugée insuffisante par la CNIL qui, par délibération du 10 mars 2016, a prononcé à l'égard de Google une sanction, rendue publique, de 100 000 euros.

Google a alors saisi le Conseil d'État d'un recours à l'encontre de la sanction de la CNIL. Devant la juridiction administrative, Google a avancé que le « droit à l'oubli » n'implique pas nécessairement que les liens litigieux soient supprimés, sans limitation géographique, sur l'ensemble des noms de domaine de son moteur.

Le Conseil d'État a sursis à statuer en posant à la CJUE plusieurs questions préjudicielles :

- Le « droit au déréférencement », tel qu'il a été consacré par la CJUE dans son arrêt *Google Spain et Google* sur le fondement des dispositions de l'article 12, sous b), et l'article 14, sous a), de la directive 95/46, doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche est tenu, lorsqu'il fait droit à une demande de déréférencement, d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur de telle sorte que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée, y compris hors du champ d'application territorial de la directive ?

- En cas de réponse négative à cette première question, le « droit au déréférencement », tel que consacré dans l'arrêt précité, doit-il 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 ?

- En outre, en complément de l'obligation évoquée à la deuxième question, le « droit au déréférencement » doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est tenu de supprimer, par la technique dite du « géo-blocage », depuis une adresse IP réputée localisée dans l'État de résidence du bénéficiaire du « droit au déréférencement », les résultats litigieux des recherches

effectuées à partir de son nom, ou même, plus généralement, depuis une adresse IP réputée localisée dans l'un des États membres soumis à la directive 95/46, ce indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche ?

La position de la CNIL ne fait pas l'unanimité. Le G29 relève *« [qu']afin de donner pleinement effet aux droits des personnes concernées définis dans l'arrêt de la Cour, les décisions de déréférencement doivent être exécutées de manière à garantir la protection efficace et complète des droits des personnes concernées et à ce que la législation européenne ne puisse pas être contournée. En ce sens, la limitation du déréférencement aux domaines de l'Union européenne au motif que les utilisateurs ont tendance à accéder aux moteurs de recherche par l'intermédiaire de leurs domaines nationaux ne peut donc pas être envisagée comme moyen suffisant pour garantir de manière satisfaisante les droits des personnes concernées conformément à l'arrêt de la Cour. En pratique, cela signifie que tout déréférencement devrait également être appliqué à tous les domaines concernés, y compris les domaines.com »*. En revanche, la Commission et plusieurs États membres soutiennent que l'instauration d'un droit de déréférencement mondial sur le fondement du droit de l'Union ne serait compatible ni avec celui-ci, ni avec le droit international public et constituerait un précédent dangereux invitant des régimes autoritaires à exiger également la mise en œuvre à l'échelle mondiale de leurs décisions de censure. L'idée d'un déréférencement mondial peut paraître séduisante par sa radicalité, sa clarté, sa simplicité et son efficacité. Néanmoins, cette solution ne convainc pas l'avocat général, car elle tient compte d'un seul côté de la médaille, à savoir la protection des données d'un individu.

2/ Les conclusions de l'avocat général

Pour l'avocat général, ni les dispositions de la directive 95/46 ni l'arrêt *Google Spain et Google* ne précisent *« s'il convient de traiter différemment une demande de recherche effectuée à partir de Singapour qu'une demande effectuée à partir de Paris ou de Katowice »*. Selon lui, une différenciation s'impose selon le lieu à partir duquel la recherche est effectuée. Les demandes de recherche faites en dehors du territoire de l'Union ne devraient pas souffrir d'un déréférencement des résultats de recherche. En dehors de ce territoire (UE), le droit de l'Union ne saurait, en principe, s'appliquer ni, par conséquent, créer des droits et des obligations.

Le « droit à l'oubli » doit être mis en balance avec d'autres droits fondamentaux, ce qui justifie l'absence d'obligation de déréférencement mondial. Si celui-ci était reconnu, les autorités de l'Union ne seraient pas en mesure de définir et de déterminer un droit à recevoir des informations, l'intérêt du public à accéder à une information variant selon sa localisation géographique, d'un État tiers à l'autre. L'avocat général souligne le danger qui se manifesterait si l'Union européenne empêchait des ressortissants de pays tiers à accéder à l'information : *« Si une autorité au sein de l'Union pouvait ordonner un déréférencement à l'échelle mondiale, un signal fatal serait envoyé aux pays tiers, lesquels pourraient ordonner également un déréférencement en vertu de leurs propres lois. Imaginons que, pour une raison quelconque, des pays tiers interprètent certains de leurs droits de manière à empêcher les personnes situées dans un État membre de l'Union d'accéder à une information recherchée. Il existerait un risque réel d'un nivellement*

vers le bas, au détriment de la liberté d'expression, à l'échelle européenne et mondiale ».

Toutefois, Google devrait prendre toute mesure à sa disposition afin d'assurer un déréférencement efficace et complet. Cela inclut, notamment, la technique dite du « géo-blocage », depuis une adresse IP réputée localisée dans l'un des États membres, quel que soit le nom de domaine utilisé par l'internaute qui effectue la recherche.

La solution proposée repose, certes, sur les conclusions de l'avocat général et ne saurait préjuger de la décision finale de la Cour. Celle-ci pourrait trouver dans cette recherche d'équilibre les arguments pour rendre effectif le droit à l'oubli au sein de l'UE sans toutefois lui donner une portée extraterritoriale, dont les conséquences indirectes pourraient être contraires à l'effet escompté.

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

FÉVRIER 2019

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

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

Les effets de la loi de programmation 2018-2022 et de réforme pour la justice sur les investigations numériques

La loi de programmation 2018-2022 et de réforme pour la justice du 23 mars 2019[1] comprend plusieurs articles portant sur les phases d'enquête et d'instruction et, en particulier, sur la mise en œuvre de techniques spéciales d'enquête. Deux d'entre eux ont été censurés par le Conseil constitutionnel[2]. Pour autant, cela n'entraîne pas un retour à la situation *ante*, dans la mesure où certaines parties du texte n'ont pas été rejetées par les Sages. Il est donc aujourd'hui nécessaire de réexaminer les règles relatives aux techniques spéciales d'enquête à la lumière des articles qui subsistent et de la jurisprudence constitutionnelle.

La loi contient des dispositions relatives au recours aux interceptions par la voie des communications électroniques (I), à la géolocalisation (II), à l'enquête sous pseudonyme (III), à l'accès à distance aux correspondances stockées par la voie des communications électroniques et accessibles au moyen d'un identifiant informatique (IV). Elle simplifie et harmonise les règles applicables à certaines techniques spéciales d'enquête (V).

Eu égard à leur dangerosité, elle étend le recours aux techniques spéciales d'enquête pour certaines infractions prévues et réprimées par le Code de la santé publique et le Code de la consommation (VI).

---

1. Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
2. Décision n° 2019-778 DC du 21 mars 2019.

I. Interceptions de communications

S'agissant des interceptions de communications, le Code de procédure pénale (CPP) opère, avant la promulgation de la loi, une distinction selon le type d'enquête et selon les infractions visées :

- Sous l'empire de la loi du 10 juillet 1991, dans sa version initiale, les interceptions sont autorisées lors d'une instruction, pour toute infraction criminelle ou délictuelle dont la peine encourue est égale ou supérieure à deux ans d'emprisonnement, sur décision et sous le contrôle du juge d'instruction. L'interception est possible, pendant une durée renouvelable de quatre mois mais ne pouvant excéder un an, voire deux ans si l'infraction relève de la délinquance ou de la criminalité organisée. D'où l'insertion des articles 100 à 100-8 du CPP dans le titre consacré aux juridictions d'instruction.

- Grâce à la loi du 9 mars 2004[3], les interceptions deviennent possibles – en flagrance ou en préliminaire – pour les besoins d'une enquête relative à une infraction relevant de la délinquance ou de la criminalité organisée (art. 706-73 et 706-73-1 CPP), sur décision et sous le contrôle du juge des libertés et de la détention, pour une durée d'un mois renouvelable une fois (art. 706-95 CPP). Cet article est alors inséré dans la partie du Code relative à la criminalité et à la délinquance organisées, tout en faisant référence aux articles 100 à 100-8 du CPP précités.

Le texte de la loi, avant la censure du Conseil constitutionnel, harmonisait, quel que soit le type d'enquête, la nature des

3. Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

infractions justifiant des interceptions de correspondances électroniques. Celles-ci pouvaient être autorisées par le juge des libertés et de la détention, sur demande du procureur de la République, pour tous les crimes et les délits punis d'au moins trois ans d'emprisonnement. Ce seuil, fixé par le législateur, figure dans d'autres dispositions déjà retenues par le droit actuel pour de nombreuses autres procédures : mandat de recherche (art. 70 CPP), détention provisoire (art. 143-1 CPP). La suppression de la seule référence à la criminalité et à la délinquance organisées élargissait considérablement les possibilités offertes en préliminaire ou en flagrance.

Le Conseil constitutionnel n'a pas accepté cette extension. Pour sa démonstration, il rappelle que *« le législateur peut prévoir des mesures d'investigation spéciales en vue de constater des crimes et délits d'une gravité et d'une complexité particulières, d'en rassembler les preuves et d'en rechercher les auteurs sous réserve, d'une part que les restrictions qu'elles apportent aux droits constitutionnellement garantis soient proportionnées à la gravité et à la complexité des infractions commises et n'introduisent pas de discriminations injustifiées et, d'autre part, que ces mesures soient conduites dans le respect des prérogatives de l'autorité judiciaire à qui il incombe en particulier de garantir que leur mise en œuvre soit nécessaire à la manifestation de la vérité »*. L'article 44 de la loi est censuré sur la base de plusieurs motifs :

- toutes les infractions visées par l'extension ne présentent pas les critères de particulière gravité et de complexité ;

- le juge des libertés et de la détention, qui autorise ces

interceptions dans le cadre d'une enquête préliminaire ou de flagrance, n'a pas accès à l'ensemble de la procédure et ne peut ordonner la cessation de la mesure d'interception ;

- la procédure d'urgence, telle que prévue par la loi censurée, s'opère sans contrôle ni intervention d'un magistrat du siège durant vingt-quatre heures.

Le Conseil constitutionnel exige que des mesures d'exception soient accompagnées de garanties permettant à un juge d'examiner pendant tout leur déroulé leur nécessité et leur proportionnalité. Plus la technique d'enquête est intrusive dans la vie privée, plus le contrôle doit être renforcé.
Ne sont pas frappées d'inconstitutionnalité les dispositions de la loi qui modifient l'article 100 du CPP et ne prévoient pas de limite basse pour les délits punis d'emprisonnement lorsque l'interception doit avoir lieu sur la ligne de la victime et à sa demande (appels téléphoniques malveillants, harcèlement sexuel ou moral par téléphone, etc.).
La loi du 23 mars 2019 encadre davantage la décision du juge d'instruction qui doit être motivée *« par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires et doit comporter tous les éléments d'indentification de la liaison à à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci »* (nouvelle rédaction de l'article 100-1 CPP).

II. La géolocalisation en temps réel

La géolocalisation en temps réel se distingue de la géolocalisation

en temps différé et de la surveillance[4] . Elle a été autorisée par la loi du 28 mars 2014[5] qui est venue combler le vide juridique consécutif à deux arrêts de la Cour de cassation du 22 octobre 2013[6] tirant les conclusions de la jurisprudence de la Cour européenne des droits de l'Homme[7]. Avant la loi du 28 mars 2014, aucun texte spécifique ne venait encadrer son usage. Dans le cadre d'une information judiciaire, le recours à l'article 81 du CPP semblait autoriser le juge d'instruction à procéder à tous les actes d'information qu'il jugeait *« utiles à la manifestation de la vérité »*. S'agissant des enquêtes préliminaires ou de flagrance, le Parquet s'appuyait sur l'article 41 du CPP, selon lequel *« le procureur de la République procède ou fait procéder à tous les actes d'enquête nécessaires à la recherche et à la poursuite des infractions à la loi pénale »*, et les articles 60-2 et 77-1-1 dudit Code (réquisition judiciaire concernant des données informatiques).

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

4. La surveillance des personnes ou des biens est une technique d'enquête qui est mise en œuvre dans le « monde réel » (art. 706-80 CPP).
5. Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.
6. Cass.crim., 22 octobre 2013, bull.crim 2013, n° 196 et 197.
7. CEDH, 2 septembre 2010, n° 35623/05, *Uzun c/Allemagne*.

imposent d'identifier la liaison à intercepter ».
Si la Cour de cassation a validé la géolocalisation dans le cadre d'une instruction relative à un trafic de stupéfiants, parce qu'elle est mise en œuvre sous le contrôle d'un juge (Cass.crim. 22 novembre 2011, Mohamed X et autres), elle a cependant, à l'occasion des deux arrêts précités, remis en cause cette pratique pour les enquêtes conduites sous la direction du Parquet. Elle était, en effet, contraire à la jurisprudence de la Cour européenne des droits de l'Homme statuant sur la conformité de la géolocalisation à l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales. La Cour n'a pas contesté le bien-fondé de la géolocalisation, *« nécessaire dans une société démocratique »*, mais, constatant que la géolocalisation est une ingérence dans la vie privée – protégée par l'article 8§1 de ladite Convention – elle a exigé l'intervention d'un juge pour en contrôler la procédure. Or, il est désormais acquis que le procureur de la République n'est pas considéré comme un magistrat indépendant[8].
Les arrêts de la Cour de cassation ont provoqué un véritable « séisme », dans la mesure où toutes les géolocalisations en cours, dans le cadre d'une enquête préliminaire ou d'une enquête de flagrance, ont été interrompues, sans préjudice des nullités pouvant être prononcées.
La loi du 28 mars 2014 a créé les articles 230-32 à 230-44 du CPP qui ont posé le principe d'un recours à la géolocalisation, en temps réel, d'une personne sans son consentement, d'un véhicule ou d'un objet, à l'insu de son propriétaire ou de son possesseur[9]. Pour le Conseil

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

constitutionnel[10], *« la mise en œuvre de ce procédé n'implique pas d'acte de contrainte sur la personne visée ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son ; l'atteinte à la vie privée qui résulte de la mise en œuvre de ce dispositif consiste dans la surveillance par localisation continue et en temps réel d'une personne, le suivi de ses déplacements dans tous lieux publics ou privés ainsi que dans l'enregistrement et le traitement des données ainsi obtenues »*.

Selon les termes de cette loi, le juge d'instruction peut l'autoriser pour une durée de quatre mois renouvelable, pour les besoins des procédures relatives aux infractions d'atteintes aux personnes punies d'au moins trois ans d'emprisonnement (Livre 2 du Code pénal), de recel de malfaiteurs (art. 434-66 CP), d'évasion (art. 434-27 CP), de terrorisme, ou relative à tout crime ou délit puni d'au moins cinq ans de prison. Dans le cadre d'une enquête préliminaire ou de flagrance, pour les mêmes infractions que celles précédemment mentionnées, la géolocalisation peut être mise en œuvre sur décision du procureur de la République pour une durée de quinze jours puis, après autorisation du juge des libertés et de la détention, pour une durée d'un mois renouvelable.

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

La circulaire CRIM/2014-7/G-1.04.2014 du 1er avril 2014 précise que deux techniques de géolocalisation en temps réel sont mises en

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

œuvre dans le cadre d'une procédure pénale :

- le suivi dynamique d'un terminal de télécommunications ;

- le suivi dynamique par un système (balise) placé sur un moyen de transport[11] ou sur tout autre objet, soit par sa propre technologie (par exemple un smartphone, une tablette, un véhicule par son GPS), soit par l'intermédiaire d'une balise.

Toute personne (et pas uniquement la personne soupçonnée) peut être concernée, dès lors que la mesure relève des *« nécessités de l'enquête »*. Les données issues d'une géolocalisation mise en œuvre sur le territoire national et s'étant poursuivie sur le territoire d'un autre État ne peuvent, lorsque cette mesure n'a pas fait l'objet d'une acceptation préalable ou concomitante de celui-ci au titre de l'entraide pénale, être exploitées en procédure qu'avec son autorisation[12].

La loi du 23 mars 2019 procède à la même modification que celle initialement envisagée pour les interceptions de communication. Le seuil de la peine d'emprisonnement encourue est désormais de trois ans, quelle que soit l'infraction concernée. Toutefois, pour renforcer les garanties, la durée pendant laquelle le procureur de la République peut seul autoriser la mise en œuvre de cette technique est abaissée de quinze à huit jours, afin de permettre, à l'issue de ce délai, l'intervention plus rapide du juge des libertés et de la

11. Cass.crim., (n° 15-87755), 7 juin 2016, George X..., Juan Y... *« un mis en examen est irrecevable à contester la régularité de la géolocalisation en temps réel d'un véhicule volé et faussement immatriculé sur lequel il ne peut se prévaloir d'aucun droit »*.
12. Cass.crim., (n° 15-85.070), 9 février 2016, M. X.

détention.
Par similitude, l'article 67 bis-2 du Code des douanes, qui autorise la géolocalisation dans le cadre des enquêtes douanières, est modifié pour abaisser le seuil à 3 ans d'emprisonnement au lieu de 5.

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

III. L'enquête sous pseudonyme

L'enquête sous pseudonyme est souvent dénommée de manière impropre « cyberinfiltration » ou « cyberpatrouille ». Elle n'entre pas *stricto sensu* dans la catégorie des « techniques spéciales d'enquête », car elle ne nécessite pas l'autorisation préalable d'un magistrat et n'est pas limitée dans le temps. Si elle peut apparaître comme son pendant numérique, elle ne doit pas être confondue avec l'infiltration prévue par les articles 706-32, 706-81 et s. du Code de procédure pénale et par l'article 67 bis du Code des douanes en matière de stupéfiants. Après avoir été limitée à certaines infractions, l'enquête sous pseudonyme est aujourd'hui plus largement admise, sans être pour autant banalisée. C'est la conséquence de l'usage croissant d'Internet par les auteurs de la

criminalité et de la délinquance aux conséquences les plus graves. Le dénominateur commun de toutes les infractions ouvrant droit à l'enquête sous pseudonyme est leur commission par un moyen de communication électronique.
Avant la loi 23 mars 2019, le corpus juridique l'encadrant se constitue par strates successives :

- La loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance offre pour la première fois aux enquêteurs la possibilité d'opérer de manière anonyme sur Internet pour lutter contre la traite des êtres humains, le proxénétisme, le recours à la prostitution des mineurs (art. 706-35-1 CPP) et contre différentes infractions dont sont victimes ces derniers : provocation de mineur à un usage illicite de stupéfiants, à détenir, offrir, céder, provocation à la consommation habituelle d'alcool, provocation d'un mineur à commettre un crime ou un délit, corruption de mineur, propositions sexuelles à mineur de 15 ans, pédopornographie, messages à caractère violent ou pornographique (art. 706-47-3 CPP) ;

- L'utilisation d'un pseudonyme est ensuite autorisée par l'article 59 de la loi n° 2010-476 du 12 mai 2010, relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne. Elle s'applique aux infractions commises à l'occasion de paris ou de jeux d'argent en ligne ;

- La Loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) du 14 mars 2011 crée l'article 706-25-2 du Code de procédure pénale qui permet l'enquête sous pseudonyme pour lutter contre la provocation et l'apologie du

terrorisme, réprimées alors par l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse[13];

- L'ordonnance du 19 décembre 2013 étend l'enquête sous pseudonyme aux infractions relatives aux produits de santé, notamment à la vente de faux médicaments sur Internet[14];

- La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme introduit deux modifications importantes. D'une part, elle transfère les infractions de provocation et d'apologie du terrorisme de la loi de 1881 vers le Code pénal à son article 421-2-5 CP, ce qui entraîne l'abrogation de l'article 706-25-2 du CPP mentionné *supra*. D'autre part, elle étend l'enquête sous pseudonyme à toutes les infractions relevant de la criminalité ou de la délinquance organisée (art. 706-73 et 706-73-1 CPP), y compris les délits d'atteintes aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'État commis en bande organisée (loi Godfrain, art. 323-4-1). L'article 706-87-1 CPP reprend dans son champ les infractions relevant du terrorisme, celles-ci étant visées par l'article 706-73 du même Code.

---

13. Cet article est abrogé par l'article 8 de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme qui transfère ces infractions vers le Code pénal.

14. Ordonnance n° 2013-1183 du 19 décembre 2013 - art. 23 : Dans le but de constater les infractions mentionnées aux articles L. 5421-2, L. 5421-3, L. 5421-13, L. 5426-1, L. 5432-1, L. 5432-2, L. 5438-4, L. 5439-1, L. 5451-1, L. 5461-3 et L. 5462-3 du Code de la santé publique, ainsi qu'à l'article L. 213-1 du Code de la consommation lorsque l'infraction porte sur un des produits mentionnés à l'article L. 5311-1 du Code de la santé publique, lorsque celles-ci sont commises par un moyen de communication électronique.

- Plus récemment, la loi n° 2016-1087 du 8 août 2016[15] autorise ce mode d'enquête dans le but de constater les infractions mentionnées à l'article L. 415-3 du Code de l'environnement, ainsi qu'à l'article L. 441-1 du Code de la consommation sous la double condition que l'infraction porte sur tout ou partie d'animaux ou de végétaux mentionnés aux mêmes articles et que celles-ci soient commises par un moyen de communication électronique (art. 706-2-3 CPP).

L'enquête sous pseudonyme n'est pas le monopole des officiers (OPJ) et agents de police judiciaire (APJ). Elle peut être mise en œuvre par certains agents des douanes (art. 67 bis-I Code des douanes), par des agents de l'Autorité des marchés financiers – AMF (art. L. 621-10-1 du Code monétaire et financier), par des inspecteurs de l'environnement (art. L. 172-11-1).

- S'agissant des douanes, la loi de finances rectificative pour 2012[16] modifie l'article 67 bis-1 du Code des douanes pour permettre aux agents habilités d'acquérir sous pseudonyme des produits stupéfiants en ligne. La loi du 3 juin 2016, quant à elle, crée l'article 67 bis 1-A qui permet d'utiliser un pseudonyme pour les enquêtes visant certaines infractions douanières (contrebande – art. 414 –, opérations financières entre la France et l'étranger portant sur des fonds acquis illégalement – art. 415 –, transferts illicites d'argent vers ou depuis l'étranger – art. 459). La loi du 3 juin 2016[17] autorise

15. Loi n° 2016-1087 du 8 août 2016 pour la reconquête de la biodiversité, de la nature et des paysages, art. 130.
16. Loi n° 2012-1510 du 29 décembre 2012, art.13.
17. Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

ces mêmes agents à recourir aux enquêtes sous pseudonyme pour constater les délits douaniers visés aux articles 414 (contrebande, importation, exportation sans déclaration de marchandises prohibées ou hautement taxées), 415 (opérations financières frauduleuses avec des fonds provenant notamment d'une infraction liée aux stupéfiants) ou 459 (infractions relatives aux relations financières avec l'étranger) du Code des douanes.

- La loi du 26 juillet 2013 de séparation et de régulation des activités bancaires crée l'article L. 621-10-1 du Code monétaire et financier permettant aux enquêteurs et aux contrôleurs de l'AMF de faire usage d'un pseudonyme pour accéder aux informations et éléments disponibles sur les services proposés par des personnes ou des entités dont la liste est dressée par l'article L. 621-9 du même Code.

- La loi du 8 août 2016[18] créé l'article L. 172-11-1 du Code de l'environnement permettant aux inspecteurs de l'environnement habilités, dans des conditions précisées par arrêté des ministres de la Justice et chargé de l'Écologie, d'agir avec un nom d'emprunt pour constater diverses atteintes à l'environnement, commises par un moyen de communication électronique, punies d'une peine de deux ans d'emprisonnement (art. 415-3 C. environnement) ou de sept ans, lorsqu'elles sont aggravées en étant commises en bande organisée (art. L. 415-6 C. environnement).

Mais la loi du 23 mars 2019, n'agissant que sur les articles du CPP concernant les OPJ et APJ, ne modifie pas ces dispositions

18. Loi n° 2016-1087 du 8 août 2016 pour la reconquête de la biodiversité, de la nature et des paysages.

particulières.

Par le nouvel article 230-46 du CPP, elle unifie tous les dispositifs existants au sein du Code de procédure pénale[19]. Le recours à l'enquête sous pseudonyme s'applique à des infractions définies non plus par leur nature, mais par la peine encourue, puisqu'il est désormais rendu possible aux fins de constater les crimes et délits punis d'une peine d'emprisonnement, sans effet de seuil[20], commis par un moyen de communication électronique.

L'enquête sous pseudonyme est toujours réservée à des enquêteurs relevant de services spécialisés. La formulation de l'article est plus simple et plus précise. L'élargissement des possibilités de recours à l'enquête sous pseudonyme est cependant compensé par des règles plus strictes si les enquêteurs doivent acquérir (« coup d'achat ») tout contenu, produit, substance, prélèvement ou service, même illicite, ou transmettre en réponse à une demande expresse, des contenus illicites : l'autorisation du procureur de la République ou du juge d'instruction est désormais requise. La loi rappelle que cette autorisation ne doit pas avoir pour effet d'inciter à la commission d'une infraction.

En effet, les cyberenquêteurs ne peuvent, à peine de nullité, commettre d'infraction pour révéler une infraction[21], ni inciter la

---

19. Est en particulier abrogée la section 2 bis du titre XV « de l'enquête sous pseudonyme » qui était consacrée aux infractions mentionnées aux articles 706-72, 706-73 et 706-73-1 (criminalité et délinquance organisée).

20. Le Sénat voulait fixer un seuil de 3 ans d'emprisonnement, ce qui aurait exclu l'enquête sous pseudonyme pour les infractions en matière d'acquisition ou de consultation d'images pédopornographiques, délit puni de deux ans d'emprisonnement.

21. L'article 706-32 permet aux OPJ et APJ, avec l'autorisation d'un magistrat, d'acquérir des stupéfiants, de mettre à la disposition des délinquants des moyens juridiques, financiers ou matériels.

personne à en commettre une[22].

Cette évolution de la procédure pénale n'est pas remise en cause par le Conseil constitutionnel : le législateur n'a pas méconnu le droit à un procès équitable et a opéré une conciliation équilibrée entre l'objectif de recherche des auteurs d'infractions et le droit au respect de la vie privée.

IV. L'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique

La loi du 3 juin 2016[23] crée de nouvelles dispositions qui permettent d'accéder aux correspondances électroniques stockées, sans passer par la mise en œuvre préalable d'une interception judiciaire ou de la perquisition. Ces correspondances sont

---

22. Cass. Crim., n° 2211 du 30 avril 2014. Un forum « cardeprofit » a été mis en place par le FBI dans le cadre d'une stratégie d'infiltration pour identifier des cybercriminels échangeant des offres d'achats, de vente et d'échange de biens et services liés à la fraude à la carte bancaire (*carding*). L'OCLCTIC est informé par le FBI de l'implication d'un individu résidant en France et utilisant un pseudonyme dans le commerce illicite de numéros de cartes bancaires sur Internet, ce qu'une perquisition à Toulouse a permis de confirmer. La Cour de cassation relève qu'aucun élément de la procédure ne démontre que ce site avait pour objet d'inciter les personnes le consultant à passer à l'acte. La personne en cause avait déjà manifesté sur d'autres sites son intérêt pour les techniques de fraude à la carte bancaire. Le site a simplement permis de rassembler les preuves. Porte atteinte au principe de loyauté des preuves et au droit à un procès équitable la provocation à la commission d'une infraction par un agent de l'autorité publique. La déloyauté rend irrecevables en justice les éléments de preuve ainsi obtenus.
23. Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

accessibles par un identifiant informatique, sans qu'il soit ici nécessaire de mettre en œuvre un dispositif technique comme dans le cas de la captation de données informatiques (voir *infra* articles 706-102-1 à 706-102-9 CPP).

Un arrêt de la Cour de cassation du 8 juillet 2015[24] a, en effet, considéré que *« l'appréhension, l'enregistrement et la captation de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception prise par le juge d'instruction ne peuvent relever des articles 100 à 100-5 du code de procédure pénale relatifs aux interceptions »*. Ces opérations doivent être réalisées conformément aux dispositions légales des perquisitions. Il fallait donc modifier le droit, car les modalités de la perquisition (présence de la personne mise en cause ou son représentant, respect des heures légales) ne pouvaient être mises en œuvre, sous peine de compromettre le nécessaire secret de l'opération.

En outre, les correspondances ne sont pas obligatoirement stockées sur un terminal, mais peuvent être consultées directement sur un serveur de messagerie. Elles peuvent correspondre à une adresse électronique qui n'est plus en service. La référence à l'identifiant informatique tient compte du développement d'applications telles que Whatsapp ou Skype qui permettent également des échanges.

Les nouveaux articles 706-95-1 à 706-95-3 ont créé un cadre légal limité aux seules infractions relevant du champ de la criminalité

24. Cass.crim. n° 3648 du 8 juillet 2015 (14-88.457). En l'espèce, une commission rogatoire avait été délivrée à la police judiciaire concernant des courriers électroniques échangés par un détenu opérant avec un matériel informatique clandestin. Les enquêteurs ont recueilli l'ensemble des données contenues dans le fichier associé à son adresse mail, y compris celles stockées antérieurement à l'autorisation d'interception.

organisée (art. 706-73 et 706-73-1 CPP). Dans ces conditions, les investigations ne pouvaient, à peine de nullité, avoir un autre objet que la recherche et la constatation de ces infractions, alors que la pluralité des acteurs n'est pas le seul facteur de gravité d'une infraction. Ainsi, pour un meurtre (crime), cette procédure était inapplicable, alors qu'elle pouvait être utilisée pour un délit commis en bande organisée.
La loi du 23 mars 2019 modifie les articles 706-95-1 et 706-95-2 du CPP en disposant que toute infraction qualifiée de crime peut faire l'objet d'une telle mesure.
Le magistrat compétent – juge des libertés et de la détention (art. 706-95-1) ou juge d'instruction (706-95-2) – ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service ou organisme habilité ou tout agent qualifié d'un opérateur de communications électroniques de procéder à ces opérations.
Le Conseil constitutionnel n'a pas été saisi sur cette évolution législative qui n'est donc pas remise en cause.

V. Une harmonisation des dispositions relatives « à certaines techniques d'enquête » partiellement censurée

La loi supprime les différences entre les régimes juridiques, en regroupant dans une même section intitulée « dispositions communes » les règles désormais applicables à l'utilisation d'un IMSI catcher pour le recueil des données techniques de connexion et des interceptions de correspondance émises par la voie des communications électroniques (art. 706-95-20 CPP), les sonorisations et fixations d'images (art. 706-96 à 706-98 CPP) et les captations de données informatiques (art. 706-102-1 CPP). L'harmonisation porte sur les conditions d'autorisation, de durée,

de mise en œuvre et de conservation des données désormais précisées par les nouveaux articles 706-95-11 à 706-95-19 du CPP.
Le législateur voulait étendre à toutes les infractions qualifiées de crime la mise en œuvre de ces trois techniques d'enquête. Le Conseil constitutionnel a censuré cette extension en reprenant son argumentation : de telles mesures ne peuvent être mises en œuvre que si les infractions concernées sont d'une particulière gravité et complexité. *« Tel n'est pas le cas d'infractions ne présentant pas ces caractères »*, selon les Sages, qui reprennent dans leurs considérants les arguments relatifs à l'insuffisance du contrôle de l'exécution de la mesure par un magistrat du siège.
L'article 706-95-12 prévoit deux formes d'autorisation : par le juge des libertés et de la détention, lors d'enquêtes préliminaires et de flagrance, et par le juge d'instruction, lors d'une information. Ces deux magistrats doivent procéder par ordonnance écrite et motivée (art. 706-95-13) ; ils exercent leur autorité et leur contrôle pendant toute la durée de la mise en œuvre de la mesure (art. 706-95-14 CPP). Pour toutes ces techniques d'enquête – en cas de risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens – une procédure d'urgence (aujourd'hui uniquement prévue, au stade de l'enquête, pour le recueil des données techniques de connexion) était ouverte par la loi au profit du procureur de la République qui devait obtenir, dans un délai de vingt-quatre heures, une confirmation par ordonnance motivée du juge des libertés et de la détention (art. 706-95-15 CPP[25]). Mais le Conseil constitutionnel a sanctionné cette disposition en reprochant au législateur – comme dans le cas des interceptions de sécurité (voir *supra*) – de ne pas prévoir le contrôle et l'intervention

25. Cette procédure d'urgence est également prévue durant l'instruction, auquel cas l'avis préalable du procureur de la République n'est pas requis (art. 706-95-15).

d'un juge du siège pendant les vingt-quatre premières heures.
Ces deux censures n'affectent pas le reste du dispositif d'harmonisation. S'agissant de la durée de l'autorisation (art. 706-95-16), elle est uniquement différenciée selon qu'il s'agit d'une enquête du Parquet (un mois renouvelable) ou d'une information judiciaire (quatre mois renouvelables). En ce qui concerne la mise en œuvre des techniques et la conservation des données, les articles 706-95-17 et suivants autorisent le recours à tout agent qualifié, imposent de dresser procès-verbal des opérations, de retranscrire les données utiles à la manifestation de la vérité[26], de supprimer celles non utiles et relatives à la vie privée et de détruire les enregistrements à l'issue du délai de prescription.
L'harmonisation n'est pas synonyme d'unification, les trois techniques concernées étant très différentes dans leur nature et leur objectif.

5.1. Le recueil des données de connexion en temps réel

Le recours aux IMSI catchers[27] par les services de renseignement a fait l'objet de débats passionnés lors de l'examen de la loi du 24 juillet 2015, dans la mesure où ces dispositifs mobiles permettent de collecter massivement, et de manière indifférenciée, des données personnelles dans un large périmètre, qu'il s'agisse de données de connexion ou, pour certains de ces appareils, de correspondances. L'IMSI catcher est une sorte de fausse antennes-relais mobile qui se substitue, dans un rayon de quelques kilomètres, aux antennes des opérateurs permettant ainsi de

26. Opération qui peut désormais être mise en œuvre par des agents de police judiciaire agissant sous la responsabilité d'un OPJ.
27. *International Mobile Subscriber Indentity* (identité internationale du souscripteur mobile stocké dans la carte SIM).

disposer de données émises ou reçues par les terminaux, ainsi leurrés, qui y sont connectés. Il permet de recueillir les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur. Si certains dispositifs possèdent des fonctionnalités leur permettant de procéder à la géolocalisation des terminaux et à l'interception de communications, ces usages relèvent, pour les enquêtes judiciaires, des dispositions du Code de procédure pénale relatives aux mesures de géolocalisation et à l'interception des correspondances mentionnées *supra*.
L'emploi de ces appareils, particulièrement attentatoire à la vie privée hors du cadre légal, est normalement interdit par l'article 226-3 du Code pénal, sous réserve d'une autorisation délivrée par le Premier ministre (art. R. 226-1 CP). Cette autorisation est donnée après avis d'une commission consultative (R. 226-2 CP) qui réunit les ministères régaliens, et dont l'Agence nationale de la sécurité des systèmes d'information (ANSSI) assure le secrétariat.

Déjà prévu dans le cadre de la loi du 24 juillet 2015, relative au renseignement, le recours à l'IMSI catcher (anc. 706-95-4, auj. art. 706-95-20 CPP) a été permis, dans le cadre de la police judiciaire, par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme[28]. Il était, en effet, paradoxal que des officiers de police judiciaire, agissant sous le contrôle de l'autorité judiciaire, disposent de moins de capacités d'investigations que les agents des services de renseignement. Seuls certains services ou unités sont habilités à mettre en œuvre un tel dispositif. Le décret du 26 août 2016 en dresse la liste[29]. La gendarmerie nationale a

28. Voir circulaire NO : JUSD1635582C du 2 décembre 2016 de présentation des dispositions de la loi n° 2016-731 du 3 juin 2016.
29. Décret n° 2016-1159 du 26 août 2016 pris pour l'application de l'ancien article 706-95-8 du Code de procédure pénale.

volontairement limité cette possibilité au GIGN et à deux groupes d'observation et de surveillance (Ile-de-France et Provence-Alpes-Côte d'Azur), tandis que la police nationale ouvre nettement l'éventail des possibilités (DCPJ, DIPJ, DRPJ, FIPN, service de soutien opérationnel et logistique de la DRPP, Direction opérationnelle des services et techniques et logistique de la PP). Deux choix très différents qui posent la question de la compétence technique des personnes susceptibles d'agir.

5.2. La sonorisation et la captation d'images

Instituées par la loi du 9 mars 2004, dite loi Perben II[30], initialement limitées à l'instruction, la sonorisation et la captation d'images ont été étendues à la phase d'enquête par la loi du 3 juin 2016. Les OPJ et APJ peuvent mettre en place un dispositif technique ayant pour objet – sans le consentement des intéressés – la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé (art. 706-96 et s. CPP). Le lieu d'habitation est particulièrement protégé, puisque le juge des libertés et de la détention doit être saisi par le juge d'instruction, dès lors que l'opération doit être accomplie en dehors des heures légales[31](6h-21h). Cette technique spéciale d'enquête a recours à des moyens numériques mais ne va pas chercher la preuve « dans le numérique ».

---

30. Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

31. Art. 59 du CPP fixant les heures légales des perquisitions et visites domiciliaires.

5.3. La captation de données informatiques

La captation de données informatiques (articles 706-102-1 à 706-102-9 CPP) est une technique d'enquête instituée par l'article 36 de la loi du 14 mars 2011 (LOPPSI) en s'inspirant directement des articles 706-96 à 706-102 du Code de procédure pénale relatifs à la sonorisation et à la fixation d'images de certains lieux ou véhicules. Elle ne pouvait être initialement opérée qu'au cours d'une information judiciaire, sur ordonnance motivée du juge d'instruction, et pour des infractions relevant de la criminalité et de la délinquance organisées, inventoriées aux art. 706-73 et 706-73-1 du CPP. Pour lutter contre la criminalité organisée, la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme a étendu la possibilité de telles captations aux enquêtes, sur décision du juge des libertés et de la détention.

S'agissant des atteintes aux systèmes de traitement automatisé de données (STAD), seules celles visant les systèmes mis en œuvre par l'État, et contenant des données à caractère personnel, peuvent autoriser une captation de données, ce qui est très restrictif. La loi du 3 juin 2016 n'a pas couvert les systèmes des opérateurs d'importance vitale (OIV), par respect du principe de légalité, la liste des OIV étant secrète.

Concrètement, la captation se matérialise par la mise en place d'un dispositif technique qui peut être installé *in situ* ou, grâce à un logiciel (*keylogger*), par le biais d'une transmission par un réseau de communication électronique. Eu égard à la complexité de sa mise en œuvre, seuls quelques unités ou services sont habilités par l'article D.15-1-6 du Code de procédure pénale[32] .

32. La Direction centrale de la police judiciaire (DCPJ) les directions régionales de la police judiciaire (DIPJ), la Direction générale de la sécurité intérieure (DGSI), les offices centraux de police judiciaire de la police et de la gendarmerie, la force

Cette technique – qui n'est pas une perquisition à distance – permet, à l'insu de l'intéressé, d'accéder en tous lieux à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans le système informatique. Le décret n° 2015-1700 du 18 décembre 2015 précise les conditions de traitement des données, lesquelles peuvent relever de la loi du 6 janvier 1978 eu égard à leur caractère personnel. Contrairement à la perquisition, la captation n'est pas limitée dans la durée[33] et elle s'affranchit de l'obligation de présence de la personne concernée.

La captation peut être réalisée en tout lieu public ou privé, y compris dans les cybercafés ou sur les bornes d'accès publiques[34], et concerner tout « système informatique » (objet connecté par exemple).

À cet accès aux données par les « stocks » s'ajoute un accès par les « flux ». La principale novation de l'article 706-102-1 repose sur la possibilité de capter des données en temps réel. Elle a pour effet de mettre l'enquêteur dans la situation de quelqu'un qui observerait l'écran en étant placé derrière l'utilisateur d'un ordinateur, prendrait connaissance d'un contenu avant qu'il ne soit chiffré et serait témoin, en temps réel, des échanges sur des forums de discussion, « chat », etc. La captation permet aussi de prendre connaissance des textes qui seront ultérieurement placés

d'intervention de la police nationale, la Sous-direction de la police judiciaire, le Service technique de recherches judiciaires et de documentation (auj. SCRCGN), les sections de recherche et les sections d'appui judiciaire de la gendarmerie, le GIGN.

33. Sous réserve de ne pas dépasser les limites fixées par l'article 706-102-3 du CPP qui ne sauraient excéder 2 ans.

34. Dans sa délibération n° 2009-200 du 16 avril 2009, la CNIL s'est inquiétée de la capacité ainsi donnée de capter toutes les images affichées sur l'écran de tous les ordinateurs d'un point d'accès public à Internet et ce, à l'insu des utilisateurs.

sur un périphérique (clef USB, CD-Rom, etc.). C'est une technique d'enquête assez proche des interceptions judiciaires.
La loi, dans sa rédaction de 2011, permettait d'accéder aux données telles qu'elles s'affichent sur l'écran par « saisie de caractère ». L'évolution des modes de communication par voie électronique a conduit le législateur à élargir la captation aux sons et aux images reçus et émis par des périphériques audiovisuels. Des applications téléphoniques (par exemple Skype), souvent utilisées par les cybercriminels, échappaient au champ des interceptions judiciaires. Les sociétés proposant ces services ne sont pas, en effet, des opérateurs téléphoniques au sens de l'article L. 33-1 du Code des postes et télécommunications électroniques. Elles n'ont pas à se déclarer auprès de l'Autorité de régulation des communications électroniques et des postes (ARCEP) et ne sont pas soumises au régime des interceptions. Ces sociétés, généralement établies à l'étranger, refusent de répondre aux demandes de déchiffrement émises par les autorités françaises. La loi du 13 décembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a corrigé cette anomalie en rendant possible la captation, non seulement des frappes de caractères et des données, mais aussi des images et des sons reçus et émis lors de l'utilisation d'un service audiovisuel en ligne. Le terme « audiovisuel » est supprimé par loi du 2 mars 2019 afin de couvrir la captation de données émises ou reçues par tout type de périphérique. Cette modification est jugée conforme à la Constitution par la décision du 21 mars 2019.

VI. L'extension de techniques spéciales d'enquête à certaines infractions

La loi, en modifiant l'article 706-2-2 du CPP, permet également le

recours à l'interception de correspondances, au recueil des données techniques de connexion (IMSI Catcher), à la sonorisation et à la fixation d'images, à la captation de données (art. 706-95-1 à 706-103 CPP) pour certains délits du Code de la santé publique qui présentent une gravité telle qu'ils sont punis d'une peine d'emprisonnement d'une durée supérieure à cinq ans : le trafic aggravé de substances vénéneuses (art. L. 5432-1 à L. 5432-3 CSP), de médicaments à usage humain falsifiés (art. L. 5421-13 CSP), de matières premières à usage pharmaceutique falsifiées (art. L. 5438-4 et L. 5438-6 CSP), de médicaments à usage humain sans autorisation de mise sur le marché (art. L. 5421-2 CSP), de préparations de thérapie génique ou cellulaire xénogénique sans autorisation (art. L. 5426-1 CSP), de dispositifs médicaux sans certification (art. L. 5461-3 CSP), de dispositifs médicaux de diagnostic in vitro sans certification (art. L. 5462-3 CSP), de micro-organismes et toxines (art. L. 5439-1 et L. 5439-2 CSP), de substances ne constituant pas des médicaments vétérinaires mais susceptibles d'entrer dans leur fabrication (art. L. 5442-10 CSP) et de médicaments falsifiés à usage vétérinaire (art. L. 5442-14 CSP).
Dans tous ces cas, l'aggravation est la conséquence de leur commission en bande organisée ou de l'utilisation d'un réseau de télécommunication à destination d'un public non déterminé.
Les mêmes dispositions s'appliquent aux délits prévus aux articles L. 451-2 et L. 454-3 du Code de la consommation : les délits aggravés de tromperie (art. L. 454-3 du Code de la consommation) ou de falsification (art. L. 451-2 du même Code) portant sur des produits destinés à l'alimentation, si la substance falsifiée ou corrompue est nuisible à la santé humaine ou animale, ou si les faits ont été commis en bande organisée.

La loi du 23 mars 2019 est une loi de simplification et de clarification des dispositions relatives aux techniques spéciales d'enquête. L'usage croissant des moyens de communication électronique dans la commission des infractions modifie substantiellement les pratiques professionnelles des OPJ, des APJ comme celles des magistrats. Par strates successives, la procédure pénale – comme le droit pénal – s'adapte à ce nouveau contexte. L'irruption des technologies numériques dans l'enquête est loin d'être arrivée à son terme. Conséquence du développement exponentiel des « machines connectées » au sein d'un écosystème numérique, l'hyperconnexion – dont on ne mesure pas encore les conséquences – va sans doute bouleverser en profondeur l'action de la justice et des services enquêteurs.

L'arrivée de la « 5 G » devrait avoir des effets disruptifs. La mise à jour régulière de notre corpus pénal, observée depuis une quinzaine d'années, devrait encore s'accélérer. L'enjeu est de taille ! Ne pas laisser le droit en retrait d'une réalité criminelle mouvante obligera à une plus grande réactivité. En même temps, l'équilibre entre sécurité et liberté sera toujours plus délicat à trouver, en raison du caractère de plus en plus intrusif et contraignant (même si la contrainte est souvent invisible par la personne qui la subit) des techniques nécessaires à la mise en évidence de la preuve numérique « dans » ou « via » le cyberespace, eu égard à leur caractère très intrusif. La loi du 23 mars 2019 s'inscrit dans cette exigence en ajoutant à l'article préliminaire du Code de procédure pénale un nouvel alinéa ainsi rédigé : *« Au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et*

proportionnées à la gravité de l'infraction ». Cet alinéa rappelle aussi la place centrale de l'autorité judiciaire garante de cet équilibre. Si le législateur l'oublie, le juge constitutionnel le sanctionne.

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

MARS
2019

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

Les internautes hésitent de moins en moins à porter devant la justice les contentieux qui les opposent aux réseaux sociaux. Plusieurs décisions de justice témoignent de la volonté du juge d'imposer la loi française aux GAFA (Google, Apple, Facebook, Amazon), entreprises de droit américain, qui fixent des clauses générales d'utilisation sur lesquelles l'internaute n'a aucun pouvoir de négociation, appliquent un droit parfois contraire au droit national et prévoient la compétence d'un juge californien en cas de litige (I). Dans d'autres cas, c'est le contenu des avis donnés par les internautes qui est en cause (II).

I. La contestation des clauses générales d'utilisation

TGI de Paris, jugement du 9 avril 2019, UFC-Que Choisir/Facebook Inc.

La présence au sein des conditions générales d'utilisation du réseau social Facebook d'une « clause de choix de loi » ne peut exclure par convention la protection accordée par les dispositions impératives de la loi de la résidence habituelle du consommateur-utilisateur français du réseau social. Facebook Inc. est une société de droit américain, dont le siège social est à Palo Alto en Californie. Pour les utilisateurs résidant en France, la plateforme en ligne est la société Facebook Ireland, société de droit irlandais (ce qui n'est pas étranger aux problèmes de taxation aujourd'hui au cœur d'un projet de loi).

Les conditions générales d'utilisation (CGU) comprennent quatre

documents :

- la déclaration des droits et responsabilités ;
- la politique d'utilisation des données ;
- les standards de la communauté Facebook ;
- les cookies, pixels et technologies similaires.

En mars 2014, l'UFC-Que Choisir a fait citer Facebook Ireland devant le TGI de Paris en mettant en avant le caractère abusif ou illicite, au regard des dispositions du Code de la consommation, de clauses contenues dans les CGU. Facebook conteste en déniant la compétence du juge français en arguant que la loi applicable au contrat conclu entre la société « FACEBOOK IRELAND LIMITED » et les utilisateurs français du service Facebook est la loi de l'État de Californie (États-Unis) et non la loi française. Pour le TGI, *« en dépit de la présence au sein des Conditions générales d'utilisation du réseau social Facebook d'une "clause de choix" de loi, la protection accordée par les dispositions impératives de la loi de la résidence habituelle du consommateur-utilisateur français du réseau social ne peut être réduite par convention, dès lors que la société Facebook, fournisseur d'un service de réseautage social, propose, via un site accessible en langue française, un contrat destiné aux membres ou futurs membres français du réseau social et manifeste ainsi sa volonté d'entrer en relation contractuelle avec ces derniers »*. Le TGI se déclare donc compétent : l'activité du réseau social Facebook étant dirigée vers la France, la loi française est applicable au contrat litigieux. En application du Code de la consommation, le TGI a déclaré abusives et illicites 430 clauses des CGU, des versions 2013, 2015 et 2016 et condamné Facebook à verser 30 000 euros de dommages-intérêts à UFC-Que Choisir.
L'association avait déjà réussi, par un jugement du 7 août 2018, à

faire condamner, par la même juridiction, Twitter, société américaine basée à San Francisco et soumise au droit de l'État du Delaware. En l'espèce, Twitter, à qui était reproché le caractère abusif ou illicite de 265 des clauses générales d'utilisation, avait contesté l'application du droit de la consommation sous prétexte que le service était gratuit. Pour le TGI, *« en collectant des données déposées gratuitement par l'utilisateur à l'occasion de son accès à la plate-forme et en les commercialisant à titre onéreux, la société Twitter, agissant à des fins commerciales, tire profit de son activité, de sorte qu'il est un "professionnel" au sens de l'article liminaire du code de la consommation, lequel définit le professionnel, comme toute personne physique ou morale, publique ou privée, agissant à des fins entrant dans le cadre de son activité commerciale, y compris lorsqu'elle agit au nom ou pour le compte d'un autre professionnel »*.
C'est exactement le même raisonnement qui a conduit le TGI de Paris à condamner Google pour 38 clauses abusives ou illicites (jugement du 12 février 2019).
On notera que, le 9 avril 2019, la Commission européenne et les autorités chargées de la protection des consommateurs ont salué les modifications apportées par Facebook à ses conditions d'utilisation et de service, qui indiquent désormais clairement comment l'entreprise utilise les données de ses utilisateurs pour développer des activités de profilage et cibler la publicité à des fins de financement. Comme le souligne le communiqué, le réseau de coopération en matière de protection des consommateurs a procédé à une évaluation commune des conditions d'utilisation de Facebook sous l'égide de la Direction générale française de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et a demandé à l'entreprise, ainsi qu'à Twitter et à Google+, d'améliorer un certain nombre de leurs clauses contractuelles.

La question doit, en effet, être tranchée à l'échelle de l'Europe, car c'est un niveau nécessaire et suffisant pour peser sur l'*imperium* des GAFA.

Mais la réponse doit être aussi nationale, par la manifestation de la volonté du juge de ne pas se laisser déposséder et de ne pas laisser le citoyen face à un déni de justice. La volonté du juge français d'imposer la loi française s'est manifestée dès 2000, lorsqu'il a voulu empêcher l'accessibilité par le public résidant en France du site Yahoo.com qui proposait à la vente des objets nazis. Yahoo déniait la compétence du juge français en arguant du fait que le site n'était pas destiné à un public français. La Cour suprême des États-Unis avait alors donné raison à la France. Plus récemment, à propos de la suppression d'un compte présentant le tableau de Gustave Courbet, *L'Origine du monde*, Facebook avait contesté le droit d'en connaître par le juge français en s'appuyant sur la clause attributive de compétence à un tribunal américain du Northern District de Californie ou à un tribunal d'État du comté de San Mateo. Dans son arrêt du 12 février 2016, la cour d'appel de Paris avait jugé abusive la clause ayant pour conséquence d'empêcher 22 millions d'usagers de Facebook de saisir les tribunaux français. Par jugement du 15 mars 2018, le TGI de Paris avait finalement constaté la faute de Facebook mais débouté le plaignant. Dans tous les cas d'espèce évoqués ci-dessus, même si les situations diffèrent, c'est l'applicabilité du droit français et la compétence du juge qui sont en cause. Ne pas abandonner les justiciables au droit américain, c'est faire acte de souveraineté.

II. Le contentieux portant sur les données à caractère personnel et sur les contenus

Les contentieux entre les justiciables et les réseaux sociaux portent souvent sur le traitement de leurs données à caractère personnel et sur les contenus que ceux-ci véhiculent. S'agissant des avis des internautes, la loi pour une République Numérique du 7 octobre 2016 appliquée par un décret du 27 septembre 2017, encadre les plateformes qui publient des avis de consommateurs. La Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) assure un contrôle pouvant être sanctionné pénalement.

Ordonnance de référé du TGI de Paris en date du 12 avril 2019, Mme X./ Google France et Google LLC

La collecte de données à caractère personnel sur Google My Business ne porte pas atteinte à la vie privée. La liberté d'expression des internautes émettant des avis trouve sa limite dans la mise en cause de leur responsabilité individuelle.

En l'espèce, une dentiste assigne en référé la société Google France et Google LLC sur la base de l'article 809 du Code de procédure civile et de l'article 6-1-8 de la Loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Cet article permet à l'autorité judiciaire de prescrire en référé ou sur requête, à tout hébergeur ou, à défaut, à tout fournisseur d'accès 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. La plaignante considère que sa fiche « Google My Business », établie sans son consentement, est le fruit d'un

traitement de données à caractère personnel manifestement illicite et demande donc que celle-ci soit supprimée. Cette fiche, hébergée par Google, accessible via Google Search ou Google Maps, comprend, outre la partie relative à ses coordonnées professionnelles, des avis d'internautes que Mme X. qualifie de dénigrements.

Sur la collecte des données à caractère personnel, le tribunal déboute la plaignante : les informations qui figurent sur sa fiche (nom, adresse professionnelle, numéro de téléphone professionnel) constituent bien des données à caractère personnel mais ne portent pas atteinte à sa vie privée dans la mesure où elles figurent sur des annuaires professionnels et spécialisés. L'atteinte au droit des données personnelles n'est pas manifestement démontrée.

S'agissant des avis des internautes, le tribunal met en avant l'intérêt légitime du consommateur. Sa liberté d'expression serait atteinte par la suppression pure et simple de la fiche concernée, étant entendu que la plaignante est en droit d'agir sur le fondement de la loi du 29 juillet 1881 sur la liberté de la presse (injure ou diffamation) ou du dénigrement en application de l'article 1240 du Code civil, contre les internautes qui porteraient atteinte à son honneur ou à sa réputation ou qui publieraient une critique excessive et fautive de ses services. C'est donc vers eux et non vers Google LLC que la plaignante doit se retourner.

Cour d'appel de Paris, pôle 1-chambre 8, arrêt du 22 mars 2019, M.X/ Google LLC

Cette affaire concerne également une fiche « Google My Business ». Mais, dans le cas d'espèce, la plaignante a volontairement adhéré au service. M. X., chirurgien esthétique à Paris, se plaint de huit commentaires très négatifs, relatifs à son activité professionnelle

et publiés sous pseudonyme par des internautes.
Après avoir obtenu les données d'identification des auteurs, 6 avis litigieux ont été retirés par ces derniers. Mais 2 sont demeurés auxquels de nouveaux avis se sont ajoutés. À titre d'exemple, l'un est ainsi rédigé : *« Homme désagréable, hautain, antipathique, pas à l'écoute ni disponible pour le patient, il donne l'impression qu'il a qu'une envie c'est qu'on lui donne son argent et qu'on s'en aille, ça doit être un bon chirurgien mais aucune envie d'être opérer par un homme comme lui »*. Pour Google, les avis litigieux n'excèdent pas les limites de la libre critique et s'inscrivent dans le cadre de la liberté d'expression.
M. X. a assigné Google LLC devant le juge des référés du TGI de Paris qui l'a débouté par ordonnance du 29 juin 2018. Saisie, la cour d'appel de Paris confirme la position du juge de première instance : *« Pas plus qu'ils ne constituent une diffamation ou des injures, les commentaires publiés n'ont nullement le caractère du dénigrement. Ils relèvent plutôt de la libre critique et de l'expression subjective d'une opinion ou d'un ressenti de patients déçus pour les deux premiers et d'un commentaire extérieur pour le troisième. En cela ils participent de l'enrichissement de la fiche professionnelle de l'intéressé et du débat qui peut s'instaurer entre les internautes et lui, notamment au moyen de réponses que le professionnel est en droit d'apporter à la suite des publications qu'il conteste »*.
La loyauté et la transparence des plateformes numériques sont déterminantes. Pris en application de la loi pour une République numérique du 7 octobre 2016, trois décrets d'application ont été publiés le 29 septembre 2017, dont le décret relatif aux obligations d'information relatives aux avis en ligne de consommateurs[1]. Celui-

1. Décret n° 2017-1436 du 29 septembre 2017 relatif aux obligations d'information relatives aux avis en ligne de consommateurs. Les deux autres décrets : décret n° 2017-1434 relatif aux obligations d'information des opérateurs de

ci modifie le Code de la consommation. Il définit l'avis en ligne comme étant *« l'expression de l'opinion d'un consommateur sur son expérience de consommation grâce à tout élément d'appréciation, qu'il soit qualitatif ou quantitatif »* (art. D.111-16). L'article D. 111-18 impose aux plateformes de veiller à ce que les traitements de données à caractère personnel réalisés dans le cadre du contrôle sur les avis soient conformes à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée. Elles doivent préciser :

1° les caractéristiques principales du contrôle des avis au moment de leur collecte, de leur modération ou de leur diffusion ;
2° la possibilité, le cas échéant, de contacter le consommateur auteur de l'avis ;
3° la possibilité ou non de modifier un avis et, le cas échéant, les modalités de modification de l'avis ;
4° les motifs justifiant un refus de publication de l'avis.

La DGGCRF surveille les avis publiés par les internautes qui, dans certains cas, peuvent tromper le consommateur et fausser la concurrence. Il s'agit de faux avis positifs postés par le principal bénéficiaire ou un complice, ou d'avis négatifs rédigés à des fins malveillantes, notamment par un concurrent. Dans une note de juin 2018 et dans son rapport 2018, publié le 25 mars 2019, elle rappelle que cette pratique est pénalement répréhensible sur la base de l'article L. 121-4 21° du Code de la consommation.
« La DGCCRF travaille à améliorer la confiance dans les actes

plateforme numériques ; décret n° 2017-1435 relatif à la fixation d'un seuil de connexions à partir duquel les opérateurs de plateformes en ligne élaborent et diffusent des bonnes pratiques pour renforcer la loyauté, la clarté et la transparence des informations transmises aux consommateurs.

d'achat sur Internet en créant un outil de détection des faux avis. Les enquêtes conduites depuis 2010 dans ce secteur relèvent régulièrement des pratiques commerciales trompeuses : rédaction de faux avis de consommateurs, modération biaisée des avis, publicité cachée, notamment les "placements produits" non signalés par des "influenceurs" sur les réseaux sociaux. Les opérations menées ont permis de saisir les preuves de rédaction de faux avis pour plusieurs clients, de vente de faux avis sur diverses plateformes (Google, TripAdvisor, Pages Jaunes, etc.) et d'utilisation de faux profils Facebook et de faux comptes Google. 61 établissements ont été visités ; 11 avertissements, 4 injonctions, 2 amendes administratives et 4 procès-verbaux pour pratiques commerciales trompeuses ont été délivrés. En 2018, tout en poursuivant les investigations relatives aux faux avis de consommateurs, l'enquête a porté sur la vérification du respect des nouvelles dispositions qui s'imposent aux gestionnaires d'avis en ligne, parmi lesquelles l'indication de la date de l'expérience de consommation, de la date de publication des avis, de l'existence ou non d'une procédure de contrôle des avis, des caractéristiques principales du contrôle des avis au moment de leur collecte, de leur modération ou de leur diffusion, des critères de classement des avis, etc. » (extrait du rapport DGCCRF 2018).

RÉGLEMENTATION EUROPÉENNE

Le règlement sur la cybersécurité (« *Cybersecurity Act* »)

Le 12 mars 2019, les députés européens ont adopté le « *Cybersecurity Act* », règlement relatif à l'ENISA (agence

européenne chargée de la sécurité des réseaux et de l'information) et à la certification des TIC en matière de cybersécurité.
Ce règlement fait partie du « paquet cyber », annoncé lors du Sommet européen des chefs d'État ou de gouvernement sur le numérique organisé à Tallinn, en Estonie (29 septembre 2017). Ce « paquet » comprenait la taxation des GAFA (la France, comme le Royaume-Uni, ont, depuis, agi de manière unilatérale, faute d'un accord entre les 28), la régulation des réseaux sociaux au regard des discours de haine et d'apologie du terrorisme (projet de règlement en cours), le développement d'entreprises leader, l'innovation numérique au travers d'un fonds d'urgence pour la recherche technologique, le renforcement de la lutte contre la cybercriminalité, la réforme de l'ENISA et la création de labels européens de cybersécurité pour les entreprises.

Les deux derniers points constituent le *« Cybersecurity Act »*, règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité).
L'ENISA a été créée par le règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004, en vue de *« contribuer à la réalisation des objectifs visant à assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publique »*.
Initialement temporaire, l'agence a vu son mandat prorogé en 2008 (règlement (CE) n° 1007/2008 du Parlement européen et du Conseil), jusqu'en mars 2012, puis jusqu'au 13 septembre 2013

(règlement (CE) n° 580/2011 du Parlement européen et du Conseil). À l'issue, le règlement (UE) n° 526/2013 a de nouveau prorogé le mandat de l'ENISA jusqu'au 19 juin 2020.

Le Règlement pérennise l'ENISA en lui donnant, avec des moyens supplémentaires, un rôle plus important en matière de coopération et de coordination, afin d'aider les États membres à mieux faire face aux cyberattaques. Tous n'ont pas atteint à ce jour le niveau de cybersécurité des pays les plus en pointe comme la France et l'Allemagne. Cette montée en puissance de l'ENISA s'opère *« tout en prenant en compte l'importance de préserver et de renforcer les capacités nationales de réaction en cas de cybermenaces de tous types »*. L'ENISA ne saurait se substituer à des agences comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI), non seulement parce qu'elle n'en a pas les moyens, mais aussi en raison du caractère souverain de nombreuses actions qui relèvent de la sécurité nationale. Comme le souligne le considérant 17 du Parlement européen, l'ENISA devrait jouer son rôle *« en fournissant des conseils et en apportant des compétences, ainsi qu'en jouant le rôle de centre d'information et de connaissance de l'Union. Elle devrait promouvoir l'échange de bonnes pratiques entre les États membres et les parties prenantes du secteur privé, proposer des actions politiques à la Commission et aux États membres, agir en tant que point de référence pour les initiatives politiques sectorielles au niveau de l'Union en ce qui concerne les questions de cybersécurité, et favoriser la coopération opérationnelle à la fois entre les États membres et entre ceux-ci et les institutions, organes et organismes de l'Union »*. Les mots « contribuer », « encourager », « faciliter », « sensibiliser », « volontairement », que l'on relève dans le règlement, témoignent d'une volonté d'agir en appui et de ne pas remettre en cause les efforts accomplis par

certains pays de l'Union. L'ENISA a donc une fonction subsidiaire et non supranationale, comme on a pu le craindre il y a encore quelque mois. La France n'aurait jamais accepté un texte allant dans ce sens.

Le Règlement sur la cybersécurité crée également un cadre de certificats européens de cybersécurité pour les produits, les procédés et les services, valables dans tous les pays de l'Union. La certification « européenne » laissait craindre le choix du plus petit dénominateur commun, alors que des États comme la France s'étaient lancés, depuis la création de l'ANSSI et, surtout, depuis la loi de programmation militaire de 2013, dans une politique de certification ambitieuse. Les craintes semblent estompées. Cette certification doit s'appuyer sur des schémas nationaux et internationaux existants, ainsi que sur des systèmes de reconnaissance mutuelle, en particulier le SOG-IS qui regroupe des hauts responsables issus des agences nationales pour la sécurité des systèmes d'information. Le cadre européen de certification de cybersécurité devrait être établi de manière homogène dans tous les États membres afin d'éviter la pratique du « shopping de certifications » en raison des différents niveaux d'exigence dans les différents États membres. Le Règlement prévoit trois niveaux d'assurance pour chaque type de certificat de cybersécurité européen : « élémentaire », « substantiel » ou « élevé ». Un groupe européen de certification de sécurité (GECC) est institué et composé de représentants des autorités nationales de certification de cybersécurité.

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

AVRIL
2019

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

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

Régulation des réseaux sociaux : le rapport de la mission « Régulation des réseaux sociaux - Expérimentation Facebook »

Les réseaux sociaux se développent pour le meilleur comme pour le pire. Leur viralité augmente avec la taille des communautés qu'ils accueillent et sous l'effet des algorithmes qu'ils mettent en œuvre.
Depuis les attentats ayant visé la France, en 2015, le gouvernement français s'est engagé dans un dialogue mêlant fermeté et diplomatie avec les réseaux sociaux.
Pour donner suite au Conseil JAI (« Justice et Affaires intérieures ») extraordinaire du 24 mars 2016, consécutif aux attentats de Bruxelles, la Commission européenne a établi, le 31 mai 2016, un code de bonne conduite avec Facebook, Twitter, Youtube et Microsoft. En particulier, *« les entreprises des technologies de l'information signataires de ce code de conduite s'engagent à continuer la lutte contre les discours de haine illégaux en ligne. Elles poursuivront notamment la mise au point de procédures internes et assureront la formation du personnel pour que la majorité des signalements valides puissent être examinés en moins de 24 heures et, s'il y a lieu, pour retirer les contenus visés ou en bloquer l'accès. Les entreprises concernées s'efforceront aussi de renforcer leurs partenariats actuels avec les organisations de la société civile, lesquelles contribueront à signaler les contenus favorisant les incitations à la violence et à la haine. Par ailleurs, les entreprises des technologies de l'information et la Commission européenne entendent poursuivre leurs travaux pour élaborer et promouvoir des contre-discours indépendants, ainsi que des idées et des initiatives nouvelles, et pour soutenir les programmes éducatifs qui*

encouragent l'esprit critique ».

Comprenant sans doute que la pression internationale augmente, Facebook, Microsoft, Twitter et YouTube s'allient, le 5 décembre 2016, contre la diffusion en ligne des contenus jugés terroristes. Ils s'unissent, en juin 2017, au sein du *Global Internet Forum to Counter Terrorism* (GIFCT) pour détecter les contenus terroristes. Une base de données commune, « base de données de partage d'empreintes numériques » (*hash sharing database*) rassemblant les « signatures » de photos ou vidéos faisant l'apologie du djihadisme, permet d'identifier les contenus déjà supprimés, tandis que l'intelligence artificielle identifie les nouveaux (appariement de photos et de vidéos, techniques de classification par apprentissage automatique basées sur du texte, etc.). L'aide de personnes qualifiées est requise, car l'apport de l'humain est indispensable pour faire la distinction entre la propagande et la liberté d'expression ou d'information.

Le G7 et les majors d'Internet (Google, Facebook, Twitter) se réunissent en octobre 2017, sur l'île italienne d'Ischia, pour sceller un accord ayant pour objectif de supprimer les contenus à caractère terroriste dans les deux heures suivant leur mise en ligne.

Le 12 septembre 2018, la Commission européenne présente un projet de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, en vue de la réunion des dirigeants européens, à Salzbourg, les 19 et 20 septembre. Ce projet fait l'objet d'une résolution législative du Parlement européen en date du 17 avril 2019. Il est désormais suspendu aux décisions du futur Parlement et de la Commission.

Les événements ne tiennent pas compte du tempo du législateur européen : le 15 mars 2019, un attentat à Christchurch (Nouvelle-Zélande) a pour conséquence la mort de 51 personnes. L'auteur,

Brenton Tarrant, a filmé son action en direct avec une caméra GoPro reliée à son smartphone et l'a retransmise pendant 17 minutes en direct sur Facebook Live. Le contenu s'est rapidement propagé, via YouTube, Twitter, Instagram et WhatsApp. Devant l'action tardive de Facebook – qui a pourtant supprimé 1,5 million de vidéos et bloqué les téléchargements – la question de la régulation des réseaux sociaux se trouve à nouveau posée, s'agissant notamment des contenus appelant à la haine ou faisant l'apologie du terrorisme.

Le 15 mai 2019, Jacinda Ardern, Première ministre néo-zélandaise, a rencontré Emmanuel Macron pour lancer « l'Appel de Christchurch » afin que des règles soient mises en œuvre pour contrôler les réseaux sociaux.

Quelques jours auparavant, le 10 mai, le Président de la République avait reçu Mark Zuckerberg pour évoquer avec lui les grandes lignes d'une proposition de loi sur la régulation des réseaux sociaux portée par Laetitia Avia[1].

Cette relation particulière avec le PDG de Facebook s'est notamment manifestée à l'occasion du Forum sur la gouvernance d'Internet qui s'est tenu, à Paris, le 12 novembre 2018, au siège de l'UNESCO. À cette occasion, le Président de la République a annoncé une coopération entre les pouvoirs publics et Facebook : *« la France lancera avec Facebook une expérimentation de terrain inédite durant le 1er semestre 2019. Facebook accueillera*

1. Proposition de loi n° 1785 visant à lutter contre la haine sur Internet, 20 mars 2019. Le texte propose une définition juridique des réseaux sociaux, opérateurs de plateformes en ligne *« proposant un service de communication au public en ligne reposant sur la mise en relation de plusieurs parties en vue du partage de contenus publics »* (article L. 111-7 nouveau du Code de la consommation). Pour la mission, un réseau social peut être défini comme un service en ligne permettant à ses utilisateurs de publier les contenus de leur choix et de les rendre ainsi accessibles à tout ou partie des autres utilisateurs de ce service.

prochainement une délégation de régulateurs français qui auront pour mission, avec les experts de la plateforme, d'élaborer des propositions conjointes, précises et concrètes sur la lutte contre les contenus haineux ou offensants. C'est une première […] ». Mais dès mai 2018, le principe d'une telle évaluation avait été retenu. Le Président de la République avait appelé, lors du salon Vivatech, à la définition d'un nouveau cadre de régulation numérique international, et le Premier ministre avait précisé, dans son discours à l'Université de Tsinghua en juin 2018, que : *« cette régulation du numérique n'a de sens qu'à l'échelle mondiale. La France lancera une consultation internationale pour réfléchir à ces régulations intelligentes »*. Le secrétaire d'État auprès du Premier ministre chargé du numérique a organisé des « États généraux des nouvelles régulations numériques » auxquels a participé le CREOGN, afin d'anticiper et de poser un cadre adapté et adaptable sur la décennie à venir et d'assurer une cohérence d'ensemble en mettant fin à des initiatives trop parcellaires ou trop tardives, en réaction à des critiques ou évènements particuliers. Une mission interministérielle a été chargée de faire des propositions en s'appuyant sur l'expérience originale tirée de la coopération avec Facebook.

I. La mission interministérielle

Une mission interministérielle « Régulation des réseaux sociaux - Expérimentation Facebook » a été confiée à un groupe de travail composé de sept experts et de trois rapporteurs provenant de services des ministères de la Culture, de l'Intérieur, de la Justice, de l'Économie, des services du Premier ministre (Direction interministérielle à la lutte contre le racisme, l'antisémitisme et la haine anti-LGBT – DILCRAH – et la Direction interministérielle du

numérique et du système d'information et de communication de l'État – DINSIC) et d'autorités administratives indépendantes (Autorité de régulation des communications électroniques et des Postes – ARCEP – et Conseil supérieur de l'audiovisuel – CSA).

La mission a porté son regard sur les contenus publics, sachant que des contenus haineux sont également de plus en plus véhiculés au sein des groupes privés ou fermés des réseaux sociaux, avec des échanges protégés par le secret des correspondances privées, chiffrés « de bout en bout », ce qui ne permet guère de modération par la plateforme.

La mission a bénéficié de la collaboration volontaire de la société Facebook, à Paris, à Dublin (siège européen de Facebook) et à Barcelone (l'un des centres de modération des contenus). Sans pouvoir accéder, faute de temps et de cadre juridique adapté, à l'ensemble des données, la mission a pu prendre connaissance de la politique de modération des contenus haineux, de son organisation, des moyens consacrés et des processus internes. Au cœur des échanges, le recours par les modérateurs aux algorithmes de traitements massifs dédiés à la fonction de modération de contenus haineux, les principes de base des algorithmes d'ordonnancement des contenus pour l'usager de Facebook.

À partir de cet examen concret, la mission souhaitait examiner les voies et moyens d'une nouvelle fonction de régulation des réseaux sociaux, complétant les instruments actuels et permettant de concilier les libertés publiques (en premier lieu la liberté d'expression et la liberté de communication) et la sauvegarde de l'ordre public sur les réseaux sociaux.

La mission a présenté sa démarche lors d'un séminaire et d'un atelier citoyens organisés par le Conseil national du numérique les 14 et 15 février 2019. Hasard du calendrier ? elle a remis son rapport à Cédric O, secrétaire d'État chargé du Numérique, le 10

mai, jour de la rencontre entre le Président de la République et Marc Zuckerberg.

II. Les propositions du rapport

Le rapport s'ouvre sur un constat que chacun partage : face aux abus de la liberté d'expression, les grands réseaux sociaux (Facebook, YouTube, Twitter ou Snap) n'apportent pas de réponse pleinement satisfaisante à ce jour. Pour autant, ces réseaux sociaux ne sont pas inactifs, mais tous les réseaux sociaux ne se sont pas dotés d'une équipe de modération à la hauteur des enjeux. Comme le souligne le rapport, leur intervention *« se contente trop souvent de proposer une réponse ex-post (après l'apparition du dommage). Elle manque de crédibilité, du fait de l'asymétrie extrême d'information, provoquant un sentiment de "story telling" qui suscite une suspicion sur la réalité de l'action de la plateforme ».*

Les contenus illicites sont créés par les utilisateurs, mais l'intervention des réseaux sociaux dans la présentation et la mise en avant sélective des contenus[2], l'insuffisance constatée de leurs mécanismes de modération et le manque de transparence du fonctionnement de leur plateforme, doit les inciter à une plus grande responsabilité, même s'ils ne sont pas considérés comme éditeurs, au sens de la loi pour la confiance dans l'économie numérique, car ils n'interviennent pas dans l'élaboration des contenus.

Sans préjudice d'un renforcement de leur vigilance, les pouvoirs publics sont légitimes pour intervenir. Mais, comme le souligne la mission, cette intervention doit faire l'objet de précautions

2. Les réseaux sociaux, par leur fonction d'ordonnancement, accélèrent ou ralentissent la diffusion de certains contenus.

particulières : respecter la diversité des modèles de réseaux sociaux, associer la société civile pour une meilleur transparence et limiter son action par les principes de nécessité et de proportionnalité. Ces principes sont d'ailleurs bien connus, puisqu'ils fondent l'ordre public qui est, par définition, un équilibre entre sécurité et liberté.
La politique répressive de la puissance publique à l'égard des auteurs de contenus illicites doit se conjuguer avec une responsabilisation accrue des réseaux sociaux, laquelle doit s'appuyer sur une régulation *ex ante*.
Selon le rapport, cette régulation doit respecter trois conditions et s'appuyer sur cinq principes.

S'agissant des conditions, le rapport recommande de :

- suivre une logique de conformité selon laquelle le régulateur supervise la bonne mise en œuvre de mesures préventives ou correctrices, sans se focaliser sur la matérialisation des risques ni chercher à réglementer lui-même le service fourni ;
- se concentrer sur les acteurs systémiques capables de créer des dommages conséquents dans nos sociétés sans créer de barrière à l'entrée pour de nouveaux acteurs européens ;
- rester agile pour affronter les enjeux futurs dans un environnement numérique particulièrement évolutif. Le dispositif législatif devra donc viser à créer une capacité institutionnelle à réguler et non une régulation figée sur les problèmes actuels.

La régulation pourrait reposer sur cinq piliers :

1/ Une politique publique de régulation garante des libertés individuelles et de la liberté d'entreprendre des plateformes. Cette

politique publique n'aurait pas pour objet de réglementer l'activité des réseaux sociaux en imposant des contraintes fonctionnelles ou techniques sur les services fournis, mais de les responsabiliser par l'obligation, opposable juridiquement, de mettre en place des moyens et d'en rendre compte. Comme le souligne le rapport, *« aujourd'hui, on peut légitimement considérer que les principaux réseaux sociaux développent une approche d'autorégulation, non pas pour internaliser et assumer pleinement des objectifs d'intérêt général de politiques publiques, mais plutôt pour limiter le risque d'intervention coercitive de la puissance publique et contenir la pression de la société civile afin de ne pas endommager leur réputation. Dans ce contexte, toutes les initiatives prises, quoique pertinentes, manquent de crédibilité et sont difficiles à évaluer »*.

2/ Une régulation prescriptive et ciblée sur la responsabilisation des réseaux sociaux mise en œuvre par une autorité administrative indépendante, reposant sur trois obligations incombant aux plateformes : la transparence de la fonction d'ordonnancement des contenus, celle de la fonction de mise en œuvre des clauses générales d'utilisation (CGU) et de modération des contenus ainsi qu'un devoir de diligence vis-à-vis de ses utilisateurs.
Par cette obligation, proche du *« duty of care »* anglo-saxon, les réseaux sociaux assumeraient une responsabilité vis-à-vis de leurs utilisateurs, concernant des abus d'autres membres et des tentatives de manipulation de la plateforme par des tiers.

3/ Un dialogue politique entre les acteurs, le gouvernement, le législateur, le régulateur et la société civile : le gouvernement, via son pouvoir réglementaire, fixerait les seuils de déclenchement des obligations et définirait les modalités des obligations de transparence des fonctions d'ordonnancement des contenus et de

mise en œuvre des CGU ainsi que l'obligation de défendre l'intégrité du réseau social et de ses membres. Il homologuerait les décisions à caractère réglementaire du régulateur. Le dialogue du gouvernement avec les réseaux sociaux associerait la société civile (monde associatif, territoires, communauté éducative, monde académique).

4/ Une autorité administrative indépendante partenaire des autres branches de l'État et ouverte sur la société civile. Elle serait garante de la responsabilisation des réseaux sociaux au bénéfice du gouvernement et de la société civile via le contrôle des obligations de transparence des fonctions d'ordonnancement et de modération des contenus, et de devoir de diligence leur incombant. Elle ne serait ni le régulateur des réseaux sociaux dans leur globalité, ni le régulateur des contenus qui y sont publiés. Elle ne serait pas compétente pour qualifier les contenus pris individuellement. Elle devrait être dotée de pouvoirs d'accès à l'information détenue par les plateformes, disposer d'un pouvoir de sanction administrative (notamment sanction pécuniaire).

5/ Une ambition européenne pour renforcer la capacité des États membres à agir face à des plateformes globales et réduire le risque politique lié à la mise en œuvre dans chaque État membre. Cela repose sur la responsabilisation de la plateforme vis-à-vis du « pays de destination », un cadre commun qui pose des obligations uniformes, définies au niveau européen via un règlement d'application directe, sous le contrôle juridictionnel de la Cour de justice de l'Union européenne (CJUE). L'efficacité du dispositif est, en effet, tributaire d'une application homogène sur l'ensemble du territoire de l'Union.
La proposition de loi Avia sera prochainement examinée par le

Parlement. Après sa promulgation, la France disposera d'une loi, à l'instar de l'Allemagne, qui a voté la Netzwerkdurchsetzungsgesetz (NetzDG), loi particulièrement contraignante pour les réseaux sociaux, entrée en vigueur le 1er octobre 2017. Il est regrettable que chaque État de l'Union soit obligé de légiférer, faute d'un instrument européen commun.

Dans la meilleure hypothèse, le règlement européen sera voté fin 2019 ou au début 2020. Sachant qu'un délai de deux ans sera appliqué pour son entrée en application, la loi commune ne devrait pas être opérante avant 2022… D'ici à cette échéance, le dialogue avec les réseaux sociaux devrait sans doute s'intensifier, sous la pression des gouvernements et même des internautes qui tolèrent de moins en moins les contenus de haine véhiculés sur la Toile. Les réseaux sociaux savent bien que de leur comportement peut dépendre leur survie.

MAI
2019

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 Justice de l'Union européenne (4e chambre), arrêt du 5 juin 2019, affaire C-142/18 Skype Communication Sarl/ Institut belge des services postaux et des télécommunications (IBPT)

La fourniture, par l'éditeur d'un logiciel, d'une fonctionnalité offrant un service « VoIP » (voix sur le protocole Internet), qui permet à l'utilisateur d'appeler, à partir d'un terminal, un numéro fixe ou mobile d'un plan national de numérotation via le Réseau téléphonique public commuté (RTPC) d'un État membre, constitue un « service de communications électroniques ».

En février 2018, la Cour de Justice de l'Union européenne (CJUE) a été saisie d'une demande de décision préjudicielle par la Cour d'appel de Bruxelles, conformément à l'article 267 TFUE, dans le cadre d'un litige opposant Skype Communications Sarl à l'Institut belge des services postaux et des télécommunications. IBPT voulait infliger à Skype une amende administrative pour avoir fourni un service de communications électroniques sans avoir préalablement procédé à la notification requise. Cette obligation découle de la directive 98/34/CE du Parlement européen et du Conseil, du 22 juin 1998, laquelle prévoit une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information.
La demande de la cour d'appel, saisie du contentieux, portait sur l'interprétation de la directive 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), modifiée par la directive 2009/140/CE du Parlement européen et du Conseil, du 25 novembre 2009.

Il convient tout d'abord de rappeler la définition de « service de communications électroniques », telle qu'elle résulte de la directive-cadre. C'est un *« service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus »*. Comme la Loi pour la confiance dans l'économie numérique (LCEN) le précise en France, une distinction est opérée entre l'élaboration de contenus, qui engage une responsabilité éditoriale, et leur acheminement qui est neutre au regard de la responsabilité.

La société Skype Communications édite un logiciel de communication, Skype, qui permet, depuis un ordinateur ou un mobile (tablette, smartphone), de bénéficier d'un service de téléphonie vocale et de téléconférence, d'appareil à appareil. SkypeOut, fonctionnalité payante ajoutée au logiciel Skype, permet à un utilisateur de passer des appels téléphoniques depuis un terminal vers une ligne de téléphone fixe ou mobile, en utilisant la technique VoIP. Toutefois, SkypeOut ne permet pas de recevoir des appels téléphoniques provenant de numéros de téléphone belges. SkypeOut est un service « hors offre du fournisseur d'accès à l'Internet » (« hors offre FAI » ou *« over the top »*), disponible sur Internet sans la participation d'un opérateur de communications. La

communication via SkypeOut passe d'abord par Internet (FAI) puis par un réseau téléphonique public commuté (RTPC). C'est pourquoi l'IBPT, considérant que SkypeOut propose une offre adressée aux résidents belges, reproche à SkypeOut de fournir un service de communications électroniques sans procéder à la notification requise par la directive citée *supra*, ce que conteste Skype Communications.

La cour d'appel de Bruxelles demande à la CJUE de dire *« si l'article 2, sous c), de la directive-cadre doit être interprété en ce sens que la fourniture par l'éditeur d'un logiciel d'une fonctionnalité offrant un service VoIP, qui permet à l'utilisateur d'appeler un numéro fixe ou mobile d'un plan national de numérotation via le RTPC d'un État membre à partir d'un terminal, doit être qualifié de « service de communications électroniques » au sens de cette disposition, dès lors que la fourniture dudit service, d'une part, donne lieu à rémunération de l'éditeur et, d'autre part, implique la conclusion par ce dernier d'accords avec les fournisseurs de services de télécommunications dûment autorisés à transmettre et à terminer des appels vers le RTPC »*.

La CJUE distingue les fonctionnalités de Skype de celles de SkypeOut. Skype permet à ses utilisateurs de passer gratuitement des communications audio et/ou vidéo entre équipements terminaux connectés à Internet et offre des services comme le partage d'écran, la messagerie textuelle instantanée, le partage de dossier ou la traduction simultanée, *« qui ne sauraient être qualifiés de "service de communications électroniques" faute de consister entièrement ou principalement en la transmission de signaux »*. En revanche, bien que l'installation de la fonctionnalité SkypeOut sur un terminal requière l'installation préalable du logiciel Skype, les services respectivement offerts par le logiciel Skype lui-même et par sa fonctionnalité SkypeOut sont distincts dans leur objet et de

meurent totalement autonomes dans leur fonctionnement.

La CJUE, dans un arrêt du 30 avril 2014[1], a déjà jugé que *« pour relever de la notion de "service de communications électroniques", un service devait comprendre la transmission de signaux, étant précisé que la circonstance que la transmission du signal a lieu par le truchement d'une infrastructure qui n'appartient pas au prestataire de services est sans pertinence pour la qualification de la nature du service, puisque seul importe à cet égard le fait que ce prestataire est responsable envers les utilisateurs finals de la transmission du signal qui garantit à ces derniers la fourniture du service auquel ils se sont abonnés »*.

En l'espèce, la CJUE relève que *« s'il est vrai que, sur le plan technique, l'acheminement des appels vocaux émis par l'intermédiaire de SkypeOut est matériellement réalisé, en premier lieu, par les FAI sur Internet, sur un premier segment partant de la connexion Internet de l'utilisateur appelant jusqu'à la passerelle d'interconnexion (Gateway) entre Internet et le RTPC, et, en second lieu, par les fournisseurs de services de télécommunications sur le RTPC, sur un second segment partant de ladite passerelle d'interconnexion jusqu'au point de raccordement mobile ou fixe de l'utilisateur appelé, il demeure que cette transmission intervient en vertu des accords passés entre Skype Communications et lesdits fournisseurs de services de télécommunications et ne saurait intervenir sans la conclusion de tels accords »*.

C'est pourquoi, selon la CJUE, la directive-cadre doit être interprétée en ce sens que la fourniture, par l'éditeur d'un logiciel, d'une fonctionnalité offrant un service VoIP, qui permet à l'utilisateur d'appeler un numéro fixe ou mobile d'un plan national de numérotation via le RTPC d'un État membre à partir d'un

1. CJUE, arrêt du 30 avril 2014, UPC DTH, C 475/12.

terminal, constitue un « service de communications électroniques », au sens de cette disposition, dès lors que la fourniture dudit service, d'une part, donne lieu à rémunération de l'éditeur et, d'autre part, implique la conclusion par ce dernier d'accords avec les fournisseurs de services de télécommunications dûment autorisés à transmettre et à terminer des appels vers le RTPC.

Cour de cassation, chambre commerciale, arrêt du 5 juin 2019, Dataxy/Département de Saône-et-Loire

Ne justifie pas d'un « intérêt légitime » une entreprise qui exploite des noms de domaine comportant le nom d'une collectivité territoriale sans offrir de services en lien avec le territoire de celle-ci.

Un litige opposait le département de Saône-et-Loire à la société Dataxy au sujet de noms de domaines que cette entreprise a fait enregistrer à son profit. Dataxy, bureau d'enregistrement de noms de domaine sur Internet, exerce des activités de géoréférencement de sites en France. En 2004, le département avait demandé l'enregistrement de cinq noms de domaine en fr mais deux lui avaient été refusés en raison de la réservation préalable par Dataxy. En 2011, la collectivité territoriale avait enregistré la marque semi-figurative « saône-et-loire Le département ».
Par un jugement du 22 octobre 2015, le tribunal de grande instance de Nanterre a condamné la société pour contrefaçon par imitation de la marque « saône-et-loire Le département » qu'elle a déposée le 4 avril 2011 et ordonné le transfert des noms de domaine « saône-et-loire », « saone-et-loire » et « saoneetloire » au profit du département de Saône-et-Loire.
La cour d'appel de Versailles (12e chambre) a confirmé le jugement

en premier ressort *« considérant que s'agissant du préjudice causé au département de Saône-et-Loire par le détournement de son nom et la privation de celui-ci pour communiquer sur internet, il s'avère, ainsi que relevé par le tribunal, que le département avait justifié de son intérêt pour les noms de domaine "saoneetloire.fr" et "saone-et-loire.fr" dès janvier 2004, avait pris contact avec la société Dataxy en 2006 pour tenter d'obtenir le transfert des noms de domaine litigieux à son profit, que les agissements de la société Dataxy l'ont empêché de disposer de son nom pour communiquer sur internet auprès du public susceptible d'être intéressé par des informations locales »*.
Par son arrêt du 5 juin 2019, la Cour de cassation confirme l'arrêt de la cour d'appel. Selon la Haute juridiction, l'attribution des noms de domaine sur Internet doit respecter les principes de liberté de communication, de liberté d'entreprendre mais aussi les droits de propriété intellectuelle. Ces principes *« n'ont ni pour objet ni pour effet de restreindre le droit du titulaire de marque d'interdire l'usage sans son consentement, dans la vie des affaires, d'un signe identique ou similaire à la marque, pour des produits ou services identiques ou similaires à ceux pour lesquels elle est enregistrée, si cet usage porte atteinte à la fonction essentielle de la marque, qui est de garantir aux consommateurs la provenance des produits ou des services, en raison d'un risque de confusion dans l'esprit du public, sauf les effets de l'intérêt légitime et de la bonne foi quant au renouvellement de l'enregistrement de noms de domaine sur internet »*. La reprise du signe « saône et loire », conjuguée à l'identité ou à la similarité des services couverts, est, selon la Cour, de nature à créer un risque de confusion, en laissant accroire à une origine commune des services offerts sous les deux dénominations, en forme de déclinaisons de la marque dont le département de Saône-et-Loire est titulaire. La Saône-et-Loire a désormais la pleine disposition des noms de domaines qui la concernent.

DROIT DE L'UNION EUROPÉENNE

Le nouveau règlement européen sur la cybersécurité

Le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019, relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA) et à la certification de cybersécurité des technologies de l'information et des communications, a été publié au Journal officiel de l'Union, le 7 juin 2019.

Il abroge le règlement (UE) 526/2013, « règlement sur la cybersécurité » de 2013.

Parfois dénommé *« European Cybersecurity Act »* (l'Europe est parfois déconcertante lorsqu'elle use de la langue d'un État qui a l'ambition de la quitter…), ce texte a été élaboré pour donner suite aux décisions du Conseil européen de Tallinn des 19 et 20 octobre 2017 qui a souhaité une approche commune de la cybersécurité au sein de l'UE. Deux objectifs avaient alors été fixés : disposer d'une agence dotée de compétences plus étendues et mettre en œuvre une certification de cybersécurité à l'échelle de l'Europe. Quelques jours auparavant, lors du sommet numérique de Tallinn du 29 septembre 2017, Jean-Claude Juncker avait donné le ton : *« 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. Nous ne voulons pas être le maillon faible de la lutte contre cette menace mondiale »*.

Le nouveau règlement respecte la souveraineté nationale. Il était à

craindre que la « nouvelle ENISA » soit un organisme supranational, tandis que les critères de certification favorisent le « moins disant » en optant pour le plus petit dénominateur commun. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) – qui vient de fêter ses dix ans d'existence – ne pouvait voir ses efforts annihilés.

Une agence rénovée

L'institution première de l'ENISA remonte au règlement (CE) n° 460/2004 du Parlement européen et du Conseil. Sa mission est de *« contribuer à la réalisation des objectifs visant à assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publiques »*.
Initialement temporaire, le mandat de l'ENISA est prorogé jusqu'en mars 2012 par le règlement (CE) n° 1007/2008 du Parlement européen et du Conseil, puis jusqu'au 13 septembre 2013[2]. En 2013, la stratégie de cybersécurité de l'Union européenne est adoptée afin d'orienter la politique que l'Union entend mener en réaction aux cybermenaces et aux risques liés à la cybersécurité. Le règlement (UE) n° 526/2013 proroge le mandat de l'ENISA jusqu'au 19 juin 2020.
L'Union adopte en 2016 son premier acte juridique dans le domaine de la cybersécurité sous la forme de la directive (UE) 2016/1148 du Parlement européen et du Conseil, dite directive NIS. Cette

2. Le règlement (UE) n° 580/2011 du Parlement européen et du Conseil a prorogé le mandat de l'ENISA une nouvelle fois jusqu'au 13 septembre 2013.

directive pose des exigences relatives aux capacités nationales de cybersécurité, instaure les premières mesures destinées à renforcer les secteurs d'importance vitale et à améliorer la coopération stratégique et opérationnelle entre les États membres.
La « nouvelle ENISA » s'inscrit aujourd'hui dans cette dynamique. Organisme de l'Union doté de la personnalité juridique, elle est désormais pérennisée. Son mandat (art. 3 du règlement) précise qu'elle doit fournir des conseils en matière de cybersécurité, favoriser la coopération opérationnelle à la fois entre les États membres et entre ceux-ci et les institutions, organes et organismes de l'Union. Elle a aussi pour mission d'apporter des compétences et jouer le rôle de centre d'information et de connaissance de l'Union. Elle doit encourager l'échange de bonnes pratiques entre les États membres et le secteur privé, proposer des actions à la Commission et aux États membres.
L'ENISA devra soutenir le développement et l'amélioration des Centres de réponse aux incidents de sécurité informatique (CSIRT) nationaux et de l'Union prévus par la directive (UE) 2016/1148, afin qu'ils atteignent un niveau de maturité commun élevé dans l'ensemble de l'Union. Elle ne doit pas se substituer aux États membres mais doit être en mesure de leur fournir un appui, à leur demande. L'ENISA devrait participer aux actions de coopération avec l'Organisation de coopération et de développement économiques (OCDE), l'Organisation pour la coopération et la sécurité en Europe (OSCE) ou l'OTAN, sans préjudice du caractère particulier de la politique de sécurité et de défense de tout État membre.

Une certification de cybersécurité européenne

La certification européenne de cybersécurité doit contribuer à

harmoniser les pratiques de cybersécurité au sein de l'Union et rendre plus transparente la cybersécurité des produits TIC, services TIC et processus TIC. Comme le souligne le considérant 65, *« le marché unique numérique, et en particulier l'économie des données et l'IdO, ne peuvent prospérer que si le grand public est convaincu que ces produits, services et processus offrent un certain niveau de cybersécurité. Les voitures connectées et automatisées, les dispositifs médicaux électroniques, les systèmes de contrôle-commande industriels et les réseaux intelligents ne sont que quelques exemples de secteurs dans lesquels la certification est déjà largement utilisée ou est susceptible de l'être dans un avenir proche »*.

L'article 4 du règlement dispose que l'ENISA favorise le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur. Le règlement institue le principe de reconnaissance mutuelle au sein de l'UE des certificats délivrés par un État membre. Il s'agit de construire un cadre européen de certification de cybersécurité homogène pour éviter la pratique du « shopping de certifications » qui joue sur la différence du niveau d'exigence entre les États membres. Du passé le règlement ne fait pas table rase puisqu'il ambitionne de *« créer les conditions d'une transition en douceur des schémas existants relevant de ces systèmes vers les schémas relevant du nouveau cadre européen de certification de cybersécurité »*. Selon le règlement, un « certificat de cybersécurité européen » est un document délivré par un organisme compétent attestant qu'un produit TIC, service TIC ou processus TIC donné a été évalué en ce qui concerne sa conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité.

Un groupe des parties prenantes pour la certification de cybersécurité est établi. Ses membres sont sélectionnés par la

Commission, parmi des experts reconnus représentant les parties prenantes concernées. Cette gouvernance de la certification doit adopter des schémas offrant trois niveaux : un niveau « élémentaire » pour les systèmes non critiques (objets grand public), un niveau « substantiel » et un niveau « élevé » pour les systèmes présentant les plus de risques aux cyberattaques. La Commission publie un programme de travail glissant de l'Union pour la certification européenne de cybersécurité qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité.

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

JUIN
2019

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

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

LÉGISLATION

Loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles

La 5G est annoncée comme une rupture technologique. Son déploiement, dès 2020, devrait accélérer celui des objets connectés, dont le nombre est estimé à près de 80 milliards en 2025. Elle aura pour effet de résoudre le problème de l'engorgement des réseaux de communications électroniques en multipliant le débit par 10, de réduire singulièrement les délais de latence à environ 1 milliseconde (de 15 à 60 ms avec la 4G). Avec elle, les espaces « intelligents », le développement de la robotique, la domotique, l'hôpital ou l'usine 4.0 deviennent des réalités. Les objets connectés – ou plutôt les systèmes connectés – vont, grâce à des réseaux décentralisés et fortement virtualisés, pouvoir échanger des données. Celles-ci seront stockées à proximité de leur lieu de production, dans le *edge computing* qui va supplanter le *cloud computing*, eu égard à la nécessité de les traiter au plus vite, ce qu'exigent notamment les transports « intelligents ».

Au-delà des aspects novateurs, la 5G est au cœur d'un enjeu de souveraineté et de sécurité. La technologie n'est maîtrisée que par un nombre très restreint d'industriels qui se réduit avec les concentrations industrielles au sein des équipementiers.

S'agissant des « cœurs de réseau », mis en exergue par le rapport de Jean-Marie Bockel, en 2012, seuls demeurent en compétition Cisco et Juniper (USA), Nokia (UE), Huawei et ZTE (Chine). Il est clair

aujourd'hui que la Chine a une longueur d'avance et que Nokia n'a pas une surface comparable.
Dans ce contexte, le gouvernement a déposé, le 25 janvier 2019, un amendement « Huawei » dans le cadre de l'examen de la loi Pacte (plan d'action pour la croissance et la transformation des entreprises). Cet amendement avait pour objectif de soumettre à autorisation préalable les équipements de réseau des opérateurs télécoms. Officiellement, ce texte ne visait aucun équipementier en particulier, mais nombre d'observateurs du secteur s'accordaient à dire que son premier but était de limiter l'accès de Huawei au marché français, ce que font de leur côté les Américains, engagés dans une guerre commerciale contre l'équipementier chinois. Mais les sénateurs ont rejeté l'amendement, plus pour des raisons de forme que de fond.
Le texte revient au Parlement par le biais d'une proposition de loi, déposée le 20 février 2019 par le député LREM, Gilles Legendre.
La loi crée un régime d'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques. C'est une nouvelle police administrative spéciale confiée au Premier ministre, dont le bras armé est l'Agence nationale de sécurité des systèmes d'information (ANSSI). Elle prévoit également de nouvelles incriminations à l'égard des équipementiers ne respectant pas ses dispositions.

Un régime d'autorisation préalable

L'article L. 34-11-I (nouveau) du Code des postes et télécommunications électroniques (CPCE) dispose *« qu'est soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou logiciels, permettant de connecter les terminaux des utilisateurs*

finaux au réseau radioélectrique mobile, à l'exception des réseaux de quatrième génération et des générations antérieures, qui, par leurs fonctions, présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages transmis et des informations liées aux communications, à l'exclusion des appareils installés chez les utilisateurs finaux ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils ».
Cette autorisation, pour une durée maximale de huit ans, n'est requise que pour l'exploitation, directe ou par l'intermédiaire de tiers fournisseurs, d'appareils par les opérateurs mentionnés à l'article L. 1332-1 du Code de la défense, qui exercent des activités d'exploitant d'un réseau de communications électroniques ouvert au public. Ces opérateurs publics ou privés – rappelons-le – exploitent, selon l'article précité, *« des établissements ou utilisent des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste »*.

S'il existe un risque sérieux pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau ou la confidentialité des messages transmis, le Premier ministre peut refuser cette autorisation (art L. 34-12 nouveau du CPCE). Ce risque tient compte du niveau de sécurité des appareils, de leurs modalités de déploiement et d'exploitation envisagées par l'opérateur, mais aussi du fait que l'opérateur ou ses prestataires, y compris par sous-

traitance, est sous le contrôle ou soumis à des actes d'ingérence d'un État qui n'est pas membre de l'Union européenne. La Chine n'est pas la seule visée…
Si l'exploitation des appareils est réalisée sur le territoire national sans autorisation préalable ou sans respecter les conditions fixées par l'autorisation, le Premier ministre peut enjoindre à l'opérateur de déposer une demande d'autorisation ou de renouvellement ou de faire rétablir à ses frais la situation antérieure, dans un délai qu'il fixe (art. L. 34-13 du CPCE).

Des manquements assortis de sanctions pénales

L'article L. 39-1-1 du CPCE (nouveau) punit de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait :

- d'exploiter des appareils mentionnés au I de l'article L. 34-11 sans autorisation préalable ou sans respecter les conditions fixées par l'autorisation ;

- de ne pas exécuter, totalement ou partiellement, les injonctions prises sur le fondement du I de l'article L. 34-13.

On notera, une fois de plus, que la logique de codification contribue à disperser la matière pénale relative à l'espace numérique. Pour preuve, le renvoi par la loi au Code pénal, article 226-3, qui réprime la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques, n'est pas applicable à la détention ou à l'acquisition par les opérateurs désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public, des appareils soumis à une autorisation du Premier

ministre en application de la présente loi.
À compter du 1er juillet 2020, le Gouvernement remettra au Parlement un rapport annuel sur l'application de la présente loi. Seront évoqués les impacts du régime d'autorisation préalable sur les opérateurs et l'ensemble de leurs prestataires et sous-traitants, sur le rythme et le coût des déploiements des équipements de quatrième et cinquième générations sur l'ensemble du territoire, sur l'accès des usagers aux services de communications électroniques rendus grâce aux réseaux radioélectriques mobiles et évaluera le nombre d'appareils n'ayant pas pu être installés ou ayant dû être retirés à la suite d'une décision de refus.
Le dispositif mis en place par la France est une réponse nationale qui ne pourra être pleinement pertinente sans une position européenne unitaire. Pour l'heure, les États membres abordent le problème en ordre dispersé. La solution reposerait dans l'émergence d'un champion européen, capable d'offrir dans les mêmes délais ou des délais raisonnables une offre technologique comparable à celle offerte par la « concurrence ». La souveraineté et la sécurité commencent par une stratégie industrielle.

DROIT EUROPÉEN

L'Union européenne face aux cyberattaques extérieures

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 *supra*, p. 57-60).

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 boîte à outils cyberdiplomatique ».

La décision (PESC) 2019/797 du Conseil, du 17 mai 2019, concerne les mesures restrictives contre les 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 leur 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.

La notion de cyberattaque d'origine externe

Les deux textes, en termes identiques, définissent les cyberattaques susceptibles de faire l'objet de mesures restrictives.
Les cyberattaques sont des accès aux systèmes d'information, des atteintes à leur intégrité ou à celle des données et des

interceptions de données qui ne sont pas autorisées par le maître du système ou sont en contravention avec le droit de l'Union ou de l'État membre concerné. Cette définition est en conformité avec la loi Godfrain.
Sont considérées comme une menace extérieure, les cyberattaques qui ont leur origine ou sont menées à l'extérieur de l'Union, utilisent des infrastructures situées à l'extérieur de l'Union, sont menées par toute personne physique ou morale, toute entité ou tout organisme établi ou agissant à l'extérieur de l'Union, sont menées avec l'appui, sur les instructions ou sous le contrôle de toute personne physique ou morale, entité ou organisme agissant à l'extérieur de l'Union.
L'origine des attaques n'est pas seulement étatique. Une organisation mafieuse, un groupe paramilitaire, un mouvement terroriste agissant à des fins propres ou pour le compte d'un État peuvent être à l'origine d'une telle menace.

Les cibles des cyberattaques

Les deux textes s'appliquent aux cyberattaques contre l'Union et à celles contre un État membre.
Les cyberattaques constituant une menace pour l'Union sont notamment celles qui sont dirigées contre ses institutions, organes et organismes, ses délégations auprès de pays tiers ou d'organisations internationales, ses opérations et missions organisées dans le cadre de la politique de sécurité et de défense commune (PSDC) et ses représentants spéciaux.
Les cyberattaques constituant une menace pour les États membres sont mieux précisées dans une énumération non exhaustive puisqu'elles concernent « notamment » :

- les infrastructures critiques, y compris les câbles sous-marins et les objets lancés dans l'espace extra-atmosphérique, qui sont indispensables au maintien des fonctions vitales de la société, ou à la santé, la sûreté, la sécurité et au bien-être économique ou social des citoyens ;
- les services nécessaires au maintien d'activités sociales et/ou économiques critiques, en particulier dans les secteurs de l'énergie (électricité, pétrole et gaz), des transports (aériens, ferroviaires, fluviaux, maritimes et routiers), des activités bancaires ; les infrastructures des marchés financiers, de la santé (prestataires de soins, hôpitaux et cliniques privées), de l'approvisionnement en eau potable et sa distribution, les infrastructures numériques et tout autre secteur essentiel pour l'État membre concerné ;
- les fonctions critiques des États, en particulier dans les domaines de la défense, de la gouvernance et du fonctionnement des institutions, y compris pour ce qui est des élections publiques ou de la procédure de vote, du fonctionnement de l'infrastructure économique et civile, de la sécurité intérieure et des relations extérieures, y compris dans le cadre de missions diplomatiques ;
- le stockage ou le traitement des informations classifiées ;
- les équipes d'intervention d'urgence mises en place par les pouvoirs publics.

Cette énumération n'offre guère d'originalité si l'on se réfère à la directive NIS et, en France, à la loi de programmation militaire en ce qui concerne les opérateurs d'importance vitale (OIV).

L'exigence « d'effets importants »

Pour mettre en œuvre les mesures restrictives, les cyberattaques doivent produire des « effets importants ». Mais ces mesures

peuvent aussi concerner les tentatives de cyberattaques ayant des effets « potentiels » importants.
Pour qualifier ainsi le résultat obtenu, il convient de retenir :

- la portée, l'ampleur, l'incidence ou la gravité des perturbations causées, notamment sur les activités économiques et sociétales, les services essentiels, les fonctions critiques de l'État, l'ordre public ou la sécurité publique ;
- le nombre de personnes physiques ou morales, d'entités ou d'organismes touchés ;
- le nombre d'États membres concernés ;
- l'ampleur des pertes économiques causées, notamment par le pillage de fonds, de ressources économiques ou de propriété intellectuelle ;
- l'avantage économique acquis par l'auteur de l'infraction, à son profit ou au profit de tiers ;
- la quantité ou la nature des données volées ou l'ampleur des violations de l'intégrité des données ;
- la nature des données sensibles sur le plan commercial auxquelles il a été accédé.

Les mesures restrictives

Elles concernent tout d'abord l'entrée ou le passage en transit sur leur territoire des personnes physiques qui sont responsables de cyberattaques ou de tentatives de cyberattaques. Ces personnes sont inscrites dans une « liste noire » sur une annexe, dite « Annexe I », encore vierge. Cette liste sera établie par le Conseil, statuant à l'unanimité sur proposition d'un État membre ou du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité.

Cette restriction à la liberté d'aller et venir peut aussi être prise à l'égard de complices qui ont apporté un soutien financier, technique ou matériel, ont planifié, préparé, dirigé, aidé à préparer, encouragé de telles attaques, en y participant ou en les facilitant par action ou omission. Les personnes physiques associées aux auteurs, coauteurs ou complices sont également visées. Toutefois, cette restriction à la liberté d'aller et venir ne s'applique pas si le déplacement a lieu à l'initiative de l'Union, lorsque des obligations de droit international s'imposent à un État membre, notamment s'il est pays hôte d'une organisation internationale intergouvernementale, de l'Organisation pour la sécurité et la coopération en Europe (OSCE), d'une conférence internationale sous l'égide de l'ONU, ou s'il doit appliquer des règles relatives aux privilèges ou immunités diplomatiques. Il en est de même si des motifs humanitaires sont invoqués ou si le déplacement est justifié aux fins d'une procédure judiciaire.

Le gel des fonds et ressources économiques prévu par la décision est l'objet du règlement. Celui-ci vient préciser les dispositions restrictives d'ordre économique prévues par la décision-cadre. Il définit le cadre territorial de son application : le territoire de l'Union, y compris dans son espace aérien, à bord de tout aéronef ou de tout navire relevant de la juridiction d'un État membre.

Cette délimitation rappelle la compétence géographique de la loi pénale française (art. 113-2 et s.).

Lorsqu'une personne physique ou morale est inscrite sur la « liste noire » évoquée *supra* (« l'annexe I »), il est procédé au gel de tous les fonds et ressources économiques qui lui appartiennent, qu'elle détient ou contrôle. Aucun fonds ou ressource économique ne peut être mis à sa disposition ou débloqué à son profit (art. 3). Mais des dérogations sont prévues, notamment pour satisfaire des besoins fondamentaux des personnes et de leur famille, pour les fonds

versés sur ou depuis le compte d'une mission diplomatique ou consulaire ou d'une organisation internationale bénéficiant d'immunités conformément au droit international (art. 4).

Il est interdit de participer sciemment et volontairement à des actions visant à contourner les mesures de restriction (art. 9). Les entités ou organismes qui procèdent au gel dans les conditions prévues par le règlement bénéficient d'une irresponsabilité. Il en est de même lorsque leur action est contraire aux règles énoncées par le règlement, dès lors que ces personnes morales ne savaient ni ne pouvaient raisonnablement soupçonner que leurs actions enfreindraient les mesures prises (art. 10). Les États membres doivent fixer les sanctions effectives, proportionnées et dissuasives, applicables en cas d'infraction aux dispositions du règlement et prennent toutes les mesures nécessaires pour en garantir l'exécution (art. 15).

La décision et le règlement témoignent d'une volonté commune des Européens de lutter ensemble contre un fléau à l'ampleur et aux conséquences croissantes. Mais trouvera-t-on le consensus s'il faut demain inscrire des entités chinoises ou russes, voire américaines, sur l'annexe I ? Désigner l'auteur d'une cyberattaque est un exercice complexe, tant l'attribution est aujourd'hui encore techniquement difficile. Il faut aussi imaginer les conséquences économiques indirectes. Aux États-Unis, l'entreprise Mondelez est en conflit avec son assureur Zurich qui, après l'attaque NotPetya, a invoqué une clause d'exclusion pour des actes hostiles liés à un gouvernement. Ce refus est lié à la déclaration du Président américain désignant les Russes (voir Veille juridique n° 74, janvier 2019, rubrique « Police administrative », p. 63-65).

Par le lieutenant Océane GERRIET

JURISPRUDENCE

Le code, la force brute et le smartphone !

Commentaire de l'arrêt rendu par la cour d'appel de Paris le 16 avril 2019, n° 18-09267

Le code de déverrouillage de son téléphone portable ne constitue pas « une convention secrète d'un moyen de cryptologie » au sens de l'article 434-15-2 du Code pénal et ne saurait dès lors être réprimé sur ce fondement en cas de refus de communication.

« La pilule rouge » et le Code pénal devient un outil de déchiffrement

« I can only show you the door. You're the one that has to walk through it » expliquait Morpheus à Néo dans le premier épisode de la trilogie dystopique Matrix[1]. À l'image de la matrice, ne suffirait-il pas d'une pilule rouge, le Code pénal, pour briser l'obstacle du mot de passe du téléphone d'un mis en cause et accéder à son contenu ? Dans cet arrêt rendu le 16 avril 2019, la cour d'appel de Paris répond par la négative. Le mis en cause était renvoyé devant le tribunal correctionnel de Créteil, le 10 mars 2017, pour avoir acquis, détenu et transporté sans autorisation des substances classées comme stupéfiants. À l'occasion de l'enquête portant sur ces faits, il

1. « Je ne peux que te montrer la porte. C'est à toi qu'il appartient de la franchir », Les frères Wachowski, Matrix, 1999.

a refusé de communiquer le code secret permettant d'accéder à son téléphone. Ainsi, il a également été poursuivi pour avoir refusé de communiquer la *« convention secrète de chiffrement d'un moyen de cryptologie ».* En effet, il convient de rappeler que l'article 434-15-2 du Code pénal punit de 3 ans d'emprisonnement et de 270 000 euros 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 (…) ».* Cette disposition, introduite par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, voulait renforcer l'arsenal législatif à l'aube des nouvelles technologies. N'oublions cependant pas que le début des années 2000 vibrait encore au Nokia 3310 qui n'a découvert l'écran couleur qu'en 2002… De sorte que cette disposition se révèle vite dépassée à l'heure des smartphones pliables[2]. Ainsi, le prévenu a soulevé une question préalable de constitutionnalité (QPC) au motif que l'article 434-15-2 précité ne permet pas au mis en cause de faire usage de son droit au silence et du droit de ne pas s'auto-incriminer (puisqu'il est sommé de révéler son code), dès lors, il entre en contradiction avec le droit au procès équitable et le droit de se taire prévus aux articles 9 et 16 de la Déclaration des droits de l'Homme et du citoyen du 26 août 1789. Dans un arrêt rendu le 10 janvier 2018, la Cour de cassation a jugé que, cette question n'ayant pas été examinée par une décision du Conseil

2. Sony travaille aussi sur un smartphone pliable. *Journal du geek*, 8 juillet 2019 [consulté le 9 juillet 2019]. Disponible sur : https://www.journaldugeek.com/2019/07/08/sony-travaille-aussi-sur-un-smartphone-pliable-et-des-caracteristiques-ont-fuite/

constitutionnel, elle présentait un caractère sérieux justifiant sa saisine. Cependant, la décision n° 2018-696 QPC rendue par le Conseil constitutionnel le 30 mars 2018 conclut à la conformité des dispositions du Code pénal et ne conforte donc pas les arguments de la défense. De prime abord, les juges de la rue Montpensier rappellent que l'article 434-15-2 susmentionné sanctionne *« **quiconque** ayant connaissance de la convention secrète susceptible d'avoir été utilisé pour préparer, faciliter ou commettre une infraction (…) de refuser de la remettre **aux autorités judiciaires** ou de la mettre en œuvre »*, de sorte que cette obligation pèse sur toute personne, y compris celle suspectée. Sur ce point, le Conseil constitutionnel précise que cette possibilité est soumise à deux conditions, à savoir : d'une part, que *« la demande émane de l'autorité judiciaire »*, garante du procès équitable et, d'autre part, uniquement si ce moyen de cryptologie est susceptible d'avoir été utilisé pour *« préparer, faciliter ou commettre une infraction »*. Cette deuxième condition exige que l'enquête ou l'instruction révèle la nature « délictueuse » des données chiffrées. Partant, ces conditions répondent pleinement à l'objectif de valeur constitutionnelle de prévention des infractions et de recherche des auteurs d'infractions. Par ailleurs, le Conseil constitutionnel rappelle que l'article 29 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique définit la notion de « **moyen de cryptologie** ». En effet, il s'agit de *« **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 »*. Pour les magistrats, 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 cryptées par la personne (ou

l'organisme) ayant connaissance de cette convention. Pour toutes ces raisons, l'article 434-15-2 est donc conforme à la Constitution.

« La pilule bleu » et la technologie met K.O le droit !

Néanmoins, cette position pouvait d'ores et déjà susciter des doutes quant à sa confrontation à l'interprétation de la Cour européenne des droits de l'Homme (CEDH). À titre d'illustration, dans l'arrêt n° 10588/83 *Funke c. France* en date du 25 février 1993, les juges strasbourgeois estimaient que le fait de *« contraindre le requérant à fournir lui-même la preuve d'infractions qu'il aurait commises »* portait atteinte au *« droit de se taire et de ne point contribuer à sa propre incrimination »*, constituant dès lors une violation de l'article 6-1 de la Convention. Dans cet arrêt, elle ajoute également qu'en dépit des *« particularités du droit douanier »*, une telle atteinte ne pouvait être justifiée (§44).

En outre, l'article 434-15-2 interroge vis-à-vis de l'interprétation de la notion de « mise en œuvre de moyen de cryptologie », de surcroît lorsque la Cour de cassation y assimile le code de déverrouillage d'un smartphone. ***Est-ce techniquement exact ?***
Pour cela, il faut rappeler les contours de ces notions. Ainsi, la cryptologie peut être définie comme la science du secret. Elle englobe la cryptographie (l'écriture secrète) et la cryptoanalyse (son analyse). Le chiffrement, quant à lui, est un procédé de cryptographie grâce auquel on peut rendre la lecture de données « illisibles » à toute personne ne détenant pas « la clé de déchiffrement ». Dès lors, « déchiffrer » nécessite une clé, alors que « décrypter » consiste à passer outre cette clé pour traduire le langage « illisible ». Bref, on comprend aisément que le mot de passe d'un smartphone s'apparente plus à une « clé de

chiffrement » permettant de rendre « lisibles ou non » les données. Pour autant, le mot de passe ne constitue pas un chiffrement. En effet, celui-ci est régi par un algorithme à l'égard duquel l'utilisateur n'a aucune prise. Qu'il s'agisse d'Android ou d'IOS, les données sont désormais automatiquement chiffrées, soit par un système AES-128 bits (Android), soit par AES-256 bits (Apple). Ces systèmes sont directement embarqués dans le smartphone grâce à une puce intégrée (appelé SoC *« system on a chip »* fonctionnant comme un microprocesseur) qui génère elle-même la clé, intrinsèquement inaccessible au constructeur, comme à l'utilisateur puisqu'elle se situe dans un environnement sécurisé nommé « TEH » (*Trusted Exécution Environment*). À ce jour, la seule solution pour forcer ces algorithmes est la « force brute » qui consiste à tester toutes les combinaisons possibles. Or, certains systèmes, tels qu'Apple, mettent en place des mécanismes de protection engendrant l'effacement des données au-delà d'un nombre défini de tentatives. C'est d'ailleurs la raison pour laquelle les autorités américaines luttent fermement contre Apple pour exiger une *backdoor*[3] leur permettant d'accéder, en cas de besoin, à toutes les données contenues dans l'appareil.

Pour en revenir à l'arrêt commenté, il faut donc préciser qu'à la suite de la décision rendue par le Conseil constitutionnel, l'affaire a été renvoyée pour être jugée au fond. Ainsi, le tribunal correctionnel de Créteil, par un jugement en date du 10 septembre 2018, a condamné le requérant à 7 mois d'emprisonnement pour avoir acquis, détenu et transporté sans autorisation des substances classées comme stupéfiants, ainsi que pour avoir *« refusé de*

3. The FBI wanted a backdoor to the Iphone. Tim Cook said NO. *The Wired*. 16 avril 2019 [consulté le 9 juillet 2019]. Disponible sur : https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/

t*ransmettre à une autorité judiciaire ou mis en œuvre la convention de déchiffrement des données »*. L'avocat, persévérant, a interjeté appel pour remettre en cause cette condamnation, notamment eu égard à l'absence de caractérisation du délit mentionné à l'article 434-15-2 du Code pénal.

La cour d'appel de Paris prend à revers les juges du fond et livre une analyse technique plus précise. Elle estime 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** »*. En ce sens, le refus de communiquer son mot de passe exclut toute condamnation sur le fondement de l'article 434-15-2 du Code pénal. En outre, il est intéressant de souligner qu'elle précise tout de même qu'*« il ne ressort d'aucun élément de la procédure qu'une réquisition ait été adressée par une autorité judiciaire à M. B. de communiquer ce code de déverrouillage ou de le mettre en œuvre, le prévenu 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 »*. Elle ouvre ainsi une brèche permettant de pallier la non-application des dispositions contestées.

Pourtant, cette brèche ne va pas de soi puisque à l'occasion de l'étude de la QPC n° 2018-696, le gouvernement lui-même avait jugé que cette disposition ne pouvait s'appliquer aux personnes suspectées d'avoir commis ou tenté de commettre une infraction… En effet, une telle possibilité fait obstacle au droit de ne pas s'auto-incriminer garanti par la CEDH. Ainsi, il est évident qu'il existe un

réel doute quant à la compatibilité de cette interprétation avec la jurisprudence de la CEDH.

Par ailleurs, il est intéressant de souligner que, contrairement à ce qu'affirmait le Conseil constitutionnel, les jurisprudences relatives à l'application de l'article 434-15-2 du Code pénal sont rares, voire inexistantes. Dès lors, la notion de « moyen de cryptologie » risque encore de faire parler d'elle et de faire couler l'encre des tribunaux. À titre d'exemple, dans un jugement rendu le 6 juin 2019, le tribunal correctionnel de Belfort prend le contre-pied de la décision de la cour d'appel de Paris et condamne le prévenu à une peine d'emprisonnement de 3 mois pour avoir refusé de communiquer le code de déverrouillage de son Iphone lors de sa garde à vue.

Pour conclure, l'accès à la preuve numérique est devenu un véritable enjeu pour la police judiciaire qui est dépendante des soubresauts technologiques et… législatifs[4] ! Cependant, il faut reconnaître que la France fait partie des pays les plus proactifs en la matière. De son côté, l'Europe cherche également à harmoniser et à mettre en place des systèmes de coopération efficaces pour lutter contre cette preuve particulièrement difficile à saisir.
Néanmoins, le règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale est toujours en cours d'instruction. Il aurait notamment pour objectif de permettre à l'autorité judiciaire des États membres d'accéder à des données stockées à l'extérieur de leurs frontières et/ou par des fournisseurs de services établis dans d'autres États membres.

4. Myriam Quéméner, *L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives*, Dalloz IP/IT 2018.418. 4 juillet 2018.

« Il n'y a qu'une seule règle d'or : la causalité. Action, réaction »[5]. À l'heure où les technologies sont soumises à la loi de Moore, le législateur doit se montrer encore plus vigilant pour que l'horloge juridique ne soit pas dépassée par l'horloge technologique, au risque de créer d'importants vides juridiques…

5. *Parole de l'Oracle*. Les frères Wachowski, Matrix Reloaded, 2003.

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

SEPTEMBRE 2019

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

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

LÉGISLATION

LOI n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles

Afin de préserver les intérêts de la défense et de la sécurité nationale, la loi soumet à une autorisation du Premier ministre l'exploitation sur le territoire national de tous dispositifs matériels ou logiciels permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile, à l'exception des réseaux de quatrième génération et des générations antérieures qui, par leurs fonctions, présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages transmis et des informations liées aux communications, à l'exclusion des appareils installés chez les utilisateurs finaux ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils.
Le texte a été commenté dans la veille juridique de juin 2019, voir *supra* (p. 87-91).

LOI n° 2019-759 du 24 juillet 2019 portant création d'une taxe sur les services numériques et modification de la trajectoire de baisse de l'impôt sur les sociétés

Les entreprises du secteur numérique ne paient pas toujours un

impôt à la hauteur des revenus qu'elles génèrent depuis le territoire français. Au-delà des aspects économiques, c'est une véritable atteinte à la souveraineté nationale, si l'on considère que la fiscalité en est l'un des piliers. Le système du « sandwich irlandais » permet de rapatrier les profits sur cet État qui appartient à l'Union européenne, mais qui se distingue par une fiscalité sur les entreprises très inférieure à celle que nous connaissons en France (12,5 % au lieu de 28 ou 33,3 %). Au sein d'une Europe qui défend le principe du Marché unique, cela peut surprendre… L'Organisation de coopération et de développement économiques (OCDE) a engagé, après le sommet de Saint-Pétersbourg (septembre 2013), un plan d'action visant à lutter contre les pertes de recettes entraînées par les stratégies d'optimisation fiscale. Le « paquet BEPS[1] » (« érosion de la base d'imposition et transfert de bénéfices ») tente d'adapter le système fiscal international à la numérisation de l'économie. Depuis le changement d'attitude des États-Unis, en 2018, les négociations multilatérales progressent et un accord pourrait intervenir d'ici à 2020 ou 2021. Le récent sommet du G20 à Fukuoka a montré que l'existence de la TSN était un facteur de dynamisme dans ces négociations.

Dans ce contexte, la France pensait initialement régler la question en s'appuyant sur sa propre législation, mais la juridiction administrative lui a donné tort. En effet, s'agissant de Google INC., le tribunal administratif de Paris (TA Paris, 19 juillet 2017, Google INC.) a jugé que Google Ireland Limited ne disposait pas en France, en la personne morale de Google France, d'un tel établissement stable respectant deux conditions cumulatives : la dépendance de Google France vis-à-vis de Google Ireland Limited et le pouvoir du premier d'engager juridiquement le second : *« GF ne pouvait*

1. *« Base erosion and profit shifting »*.

engager juridiquement GIL car les salariés de GF ne pouvaient procéder eux-mêmes à la mise en ligne des annonces publicitaires commandées par les clients français, toute commande devant en dernier ressort faire l'objet d'une validation de GIL ».

Face à cette impasse, le gouvernement français a souhaité engager l'Union européenne dans une démarche collective avec les ministres des Finances allemand, italien et espagnol afin d'obtenir une « taxe d'égalisation », dont l'assiette serait le chiffre d'affaires généré en Europe et non plus le profit des entreprises. Lors de la réunion des ministres des Finances européens organisée à Tallinn, en Estonie (16-17 septembre 2017), Bruno Le Maire a signé une lettre conjointe avec les ministres de l'Économie et des Finances de 9 autres États membres : l'Allemagne, l'Autriche, la Bulgarie, l'Espagne, la Grèce, l'Italie, le Portugal, la Roumanie et la Slovénie. À cette occasion, M. Juncker a déclaré : *« Dans le secteur numérique, les taxes doivent être payées là où elles sont dues ». La Commission européenne a fait des propositions, le 21 mars 2018, pour « une taxation équitable et efficace »*. Deux projets de directive devaient, à court terme, mettre en œuvre à titre temporaire une taxe sur le chiffre d'affaires en attendant d'introduire, à long terme, un critère de « présence numérique significative » dans les règles de taxation internationale.

Le taux retenu était de 3 % du chiffre d'affaires et devait rapporter entre 5 à 8 milliards d'euros. Un accord devait aboutir fin 2018. Mais c'était sans compter sur l'opposition de l'Irlande (et pour cause…), de la Finlande, du Danemark et de la Suède et une certaine frilosité de l'Allemagne qui désirait reporter cette taxation après l'échec éventuel d'un accord international conclu au sein de l'OCDE.

Dans ce contexte, la France a décidé de légiférer « à titre temporaire », la loi devenant caduque si l'accord précité est signé.

La loi définit les services taxables :
- les services d'intermédiation[2], notamment les places de marché, qui mettent à disposition, par voie de communications électroniques, une interface numérique qui permet aux utilisateurs d'entrer en contact avec d'autres utilisateurs et d'interagir avec eux, notamment en vue de la livraison de biens ou de la fourniture de services directement entre ces utilisateurs[3] ;
- la publicité ciblée, services commercialisés auprès des annonceurs ou de leurs mandataires, visant à placer sur une interface numérique des messages publicitaires orientés en fonction de données relatives à l'utilisateur qui la consulte ou collectées ou générées à l'occasion de la consultation de telles interfaces.
Ce périmètre exclut les services de mise à disposition de contenus numériques et l'e-commerce.
Seules sont assujetties les entreprises dont le chiffre d'affaires mondial dépasse 750 millions d'euros et qui dépassent le seuil de 25 millions d'euros de services fournis en France. Le taux de la taxe est de 3 % du montant hors TVA des sommes encaissées en contrepartie d'un service taxable fourni en France. La taxe vise à appréhender la valeur générée par le « travail gratuit » des utilisateurs situés en France.
L'utilisateur d'une interface numérique est localisé en France s'il la consulte au moyen d'un terminal situé en France. La localisation en France de ce terminal est déterminée par tout moyen, y compris en fonction de son adresse IP (protocole Internet), dans le respect des règles relatives au traitement de données à caractère personnel.

---

2. Exclus dans le compromis franco-allemand présenté au Conseil, le 21 décembre 2018, qui ne portait que sur la publicité.

3. Est toutefois exclue de la taxation l'utilisation de l'interface pour fournir aux utilisateurs des contenus numériques, des services de communications ou des services de paiement, au sens de l'article L. 314-1 du Code monétaire et financier.

La loi est rétroactive au 1er janvier 2019. Selon les estimations de Bercy, elle devrait rapporter environ 400 millions d'euros.
Cette loi, abusivement appelée « loi GAFA », va concerner une trentaine d'entreprises, selon les estimations avancées lors des débats parlementaires.
À peine était-elle approuvée par le Parlement que le président américain, au-delà de tweets injurieux, a demandé au Département du commerce extérieur une enquête sur son impact, avec une menace non voilée de rétorsions, notamment sur les vins français. Il est soutenu par la Computer and Communications Industry Association. Amazon a annoncé qu'il allait répercuter la taxe sur les boutiques « Market Place ».
La France avance seule au premier rang. D'autres pays ont des projets plus ou moins aboutis. Le Royaume-Uni a annoncé une taxe de 2 % sur les « services numériques » qu'il prévoit de prélever sur les revenus britanniques des grandes enseignes de la technologie tels qu'Amazon, Google et Apple, en fonction des revenus générés par ces services, notamment la publicité et le divertissement en continu. L'entrée en vigueur est prévue en avril 2020. L'Italie a adopté une loi qui n'est pas encore entrée en application.
« La France est un État souverain, elle décide souverainement de ses dispositions fiscales », comme l'a rappelé Bruno Le Maire, le 11 juillet 2019, devant le Sénat. Mais pour éviter une bataille fiscale entre David et Goliath, un accord européen est nécessaire, sauf si un consensus international se dessine. Des progrès ont été accomplis lors du sommet du G7 Finances, à Chantilly, le 18 juillet 2019. Les États se sont mis d'accord pour taxer les activités en présence physique, en particulier les activités numériques.
Cette avancée s'est concrétisée, le 26 août 2019, lors du sommet du G7 de Biarritz. Les négociations secrètes et parallèles menées par Bruno Le Maire et son homologue américain, Steven Mnuchin, ont

abouti à une position commune. L'OCDE, au sein de laquelle les discussions entre 134 pays semblent aboutir, devrait proposer un accord mondial. Dès son entrée en vigueur, pour éviter une double taxation, la France suspendra sa loi et, le cas échéant, remboursera aux entreprises le trop-perçu... Contrairement aux idées reçues, il est encore possible pour un État de faire valoir son droit face aux géants du numérique... La France l'a fait de manière isolée. Hier critiquée, demain suivie. C'est un bel exemple d'expression de la souveraineté à l'heure où elle est remise en cause par un Internet (presque) sans frontière. L'Europe a incontestablement manqué une occasion d'exister sur la scène internationale.

JURISPRUDENCE JUDICIAIRE

Cour de justice de l'Union européenne (affaire C-40/17), arrêt du 29 juillet 2019, Fashion ID GmbH & Co. KG/ Verbraucherzentrale NRW eV

Est considéré comme « responsable de traitement » de données à caractère personnel le gestionnaire d'un site Internet qui insère sur son site un bouton « j'aime » de Facebook par le biais duquel ce réseau social obtient automatiquement des données personnelles de l'utilisateur, qu'il soit ou non titulaire d'un compte, qu'il ait ou non actionné la fonctionnalité. Cette responsabilité est cependant limitée à l'opération ou à l'ensemble des opérations de traitement des données à caractère personnel dont le gestionnaire du site détermine les finalités et les modalités de la collecte et de la communication par transmission des données considérées.

L'arrêt est relatif à un litige opposant Fashion ID, société de vente en ligne d'articles de mode, à la Verbraucherzentrale, association allemande de protection de consommateurs.
Cette association dénonce le fait que l'introduction d'un plugiciel, le bouton « j'aime » de Facebook, sur le site de Fashion ID entraîne automatiquement la transmission de données à caractère personnel du visiteur à Facebook Ireland. Cette transmission s'opère, par un simple lien externe, sans que le visiteur en soit conscient et indépendamment du fait qu'il soit membre du réseau social Facebook ou qu'il ait cliqué sur le bouton « j'aime » Facebook. Ainsi sont notamment transférées des informations sur son adresse IP. Il est toutefois établi que le gestionnaire du site Internet ne peut pas déterminer les données que le navigateur transmet, ni l'usage qu'en fait le réseau social, en particulier s'il décide de les stocker et de les exploiter. Selon l'association plaignante, ce dispositif serait contraire aux dispositions 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 (auj. RGPD). La transmission de données s'effectue sans le consentement des visiteurs de Fashion ID, en violation des obligations d'information prévues par la directive.

En première instance, le tribunal régional de Düsseldorf (Landgericht Düsseldorf) a jugé que Fashion ID était responsable du traitement. Le site a fait appel, considérant qu'il n'a aucune influence sur les données transmises par le navigateur du visiteur de son site Internet et qu'il ignore l'usage qu'en fera Facebook Ireland. Saisi en appel, le tribunal régional supérieur de Düsseldorf (Oberlandesgericht Düsseldorf) se demande notamment à qui

incombent les obligations d'obtention du consentement et d'information des personnes concernées par le traitement des données à caractère personnel dans une situation telle que celle qui lui est soumise. Dans le doute, il pose plusieurs demandes de décisions préjudicielles. S'agissant de la responsabilité de Fashion ID, elle demande à la CJUE si *« dans un cas comme celui de l'espèce, où quelqu'un insère dans son site un code programme permettant au navigateur de l'utilisateur de solliciter des contenus d'un tiers et de transmettre à cet effet au tiers des données à caractère personnel, celui qui fait l'insertion est-il "responsable du traitement", au sens de l'article 2, sous d), de la directive [95/46], lorsqu'il ne peut avoir lui-même aucune influence sur ce processus de traitement des données ? »*. Les autres questions portent sur le recueil du consentement et les obligations d'information qui s'inscrivent dans une pluralité d'acteurs.

Pour répondre à ces questions préjudicielles, la Cour rappelle que la directive définit le traitement de données à caractère personnel comme étant constitué par *« toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »*. Selon la directive, la notion de « responsable du traitement » vise l'organisme qui, « seul ou conjointement avec d'autres », détermine les finalités et les moyens du traitement de données à caractère personnel. Cette notion ne renvoie pas nécessairement à un organisme unique et peut concerner plusieurs acteurs participant à ce traitement,

chacun d'entre eux étant alors soumis aux dispositions applicables en matière de protection des données. Dans le cas d'espèce, la Cour tire de cette définition qu'un traitement de données à caractère personnel peut être constitué d'une ou de plusieurs opérations, chacune d'entre elles visant l'un des différents stades que peut contenir un traitement de données à caractère personnel. Lorsque plusieurs acteurs déterminent conjointement les finalités et les moyens d'un traitement de données à caractère personnel, ils participent, en tant que responsables, à ce traitement.

Fashion ID a installé un plugiciel qui permet, via le réseau social, de bénéficier d'un avantage commercial en favorisant la publicité pour ses produits. Facebook Ireland en tire un profit, compte tenu de la valeur des données à caractère personnel ainsi récoltées.

Fashion ID influe de manière déterminante sur la collecte et la transmission des données à caractère personnel des visiteurs de son site au profit de Facebook Ireland, qui ne pourrait s'opérer en l'absence du plugiciel. Les deux bénéficiaires doivent justifier chacun d'un intérêt légitime à la collecte des données. L'existence d'une responsabilité conjointe n'entraîne pas nécessairement une responsabilité équivalente des différents acteurs, pour un même traitement de données à caractère personnel. La CJUE exclut que Fashion ID détermine les finalités et les moyens des opérations de traitement de données à caractère personnel ultérieures, effectuées par Facebook Ireland après leur transmission à cette dernière, de sorte que Fashion ID ne saurait être considérée comme étant responsable de ces opérations. Le recueil du consentement et l'obligation d'information ne concernent que l'opération ou l'ensemble des opérations de traitement des données à caractère personnel dont Fashion ID détermine les finalités et les moyens.

Les entreprises qui intègrent un plugiciel « j'aime » ne peuvent plus abandonner la responsabilité du traitement de données à

Facebook. Cette pratique pourrait être freinée par la décision de la CJUE. Les sites Internet doivent demander le consentement de l'internaute si elles veulent maintenir le bouton « j'aime », véritable aspirateur de données à caractère personnel.

Cour de justice de l'Union européenne (affaire C-193/18), arrêt du 13 juin 2019, Google LLC/ Bundesrepublik Deutschland

Un service de messagerie électronique sur Internet ne comprenant pas un accès à Internet, tel que le service Gmail fourni par Google LLC, ne consiste pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et ne constitue donc pas un « service de communications électroniques ».

Un litige oppose Google LLC à la République fédérale d'Allemagne au sujet de la décision de l'Agence fédérale des réseaux pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer (BNetzA) constatant que le service de messagerie électronique Gmail de Google constitue un service de télécommunications et lui enjoignant en conséquence, sous peine d'astreinte, de se conformer à son obligation de déclaration.
Gmail est un service dit « hors offre du fournisseur d'accès à l'Internet », disponible sur Internet sans la participation d'un opérateur de communications traditionnel.
La demande de décision préjudicielle du tribunal administratif supérieur du Land de Rhénanie-du-Nord-Westphalie porte sur l'interprétation de 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 modifiée par la directive 2009/140/CE du Parlement européen et du Conseil, du 25 novembre 2009.

L'article 2 c) de la directive cadre définit ainsi le « service de communications électroniques » : *« service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'information tels que définis à l'article 1er de la directive 98/34 qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques »*.
Pour le tribunal administratif, le service Gmail ne modifie pas le contenu mais le fractionne en plusieurs paquets (commutation par paquets) transmis au destinataire au moyen des protocoles TCP-IP (*Transmission Control Protocol – Internet Protocol*) et *Simple Mail Transfer Protocol* (protocole de transfert de courrier simple SMTP).
Google achemine le courrier à son destinataire par le biais de serveurs de messagerie électronique qui envoient les paquets de données après avoir identifié le destinataire au moyen du DNS (*domain name system*), selon des itinéraires aléatoires en vertu du principe du *« best effort »*.
Le tribunal administratif supérieur du Land de Rhénanie-du-Nord-Westphalie pose à la CJUE la question préjudicielle suivante : la notion de *« services qui consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications*

électroniques » figurant à l'article 2, sous c), de la directive-cadre doit-elle être interprétée en ce sens qu'elle inclut ou peut inclure les services de messagerie électronique sur Internet qui sont mis à disposition à travers l'Internet ouvert sans pour autant comprendre un accès à Internet ?

La CJUE ne va pas reconnaître cette qualité à Gmail. Pour la juridiction, il est constant que le fournisseur d'un service de messagerie sur Internet, tel que Gmail, réalise une transmission de signaux. Pour autant, il ne saurait en être conclu que les opérations réalisées par Google pour assurer le fonctionnement de son service de messagerie sur Internet constituent un « service de communications électroniques », au sens de l'article 2, sous c), de la directive-cadre, dès lors que ce service ne consiste pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques.

Ce sont, d'une part, les FAI des expéditeurs et des destinataires de courriers ainsi que, le cas échéant, des prestataires de services de messagerie sur Internet et, d'autre part, les gestionnaires des différents réseaux constituant l'Internet ouvert qui assurent, pour l'essentiel, la transmission des signaux nécessaires au fonctionnement de tout service de messagerie sur Internet et qui en assument la responsabilité. *« Le fait que le fournisseur d'un service de messagerie sur Internet intervienne activement dans les opérations d'envoi et de réception des messages, que ce soit en attribuant les adresses IP des équipements terminaux correspondant aux adresses de courrier électronique ou en procédant au découpage desdits messages en paquets de données et à leur introduction dans l'Internet ouvert, ou à leur réception de l'Internet ouvert, en vue de leur acheminement vers leurs destinataires, n'apparaît pas suffisant pour que ledit service puisse, sur le plan technique, être considéré comme consistant "entièrement ou*

principalement en la transmission de signaux sur des réseaux de communications électroniques", au sens de l'article 2, sous c), de la directive-cadre ».

L'arrêt de la CJUE conclut : *« L'article 2, sous c), de la directive 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 »), telle que modifiée par la directive 2009/140/CE du Parlement européen et du Conseil, du 25 novembre 2009, doit être interprété en ce sens qu'un service de messagerie électronique sur Internet ne comprenant pas un accès à Internet, tel que le service Gmail fourni par Google LLC, ne consiste pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et ne constitue donc pas un "service de communications électroniques" au sens de cette disposition »*.

Par le lieutenant Océane GERRIET

La responsabilité est le prix à payer pour le succès de ses commentaires Facebook !

TGI de Paris, 17ème Ch. ordonnance du juge de la mise en état du 19 juin 2019

Comme le rappelait Winston Churchill, la responsabilité s'accompagne de son lot de sacerdoces. À l'heure d'Internet et des médias sociaux, les élus de République ont également investi le cyberespace dans un souci de proximité et de transparence. Toutefois, par ce biais, ils exposent la responsabilité de la personne publique qu'ils incarnent, tout comme la leur. Le tribunal de grande instance (TGI) de Paris a rappelé cette subtile distinction dans le cadre de propos tenus sur Facebook. Il conclut que, s'ils sont tenus à partir d'un compte propre et personnel, les propos « ne relèvent pas [des] fonctions d'élue » et engagent donc la responsabilité personnelle de l'utilisateur, et *de jure*, la compétence du juge judiciaire.

« L'animal politique » jouit pourtant d'une liberté d'expression renforcée. Garantie par les dispositions de l'article 10 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, la liberté d'expression est considérée comme un pilier de la société démocratique par la Cour européenne des droits de l'Homme (CEDH). Elle vaut *« non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais* ***aussi pour celles qui heurtent, choquent ou inquiètent*** *»*[1]. Concernant la chose

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

politique, la CEDH va plus loin en affirmant que *« (…) la Convention ne laisse guère de place pour des restrictions à la liberté d'expression dans le domaine du discours politique ou de questions d'intérêt général »*, car *« il est fondamental (...) de défendre le libre jeu du débat politique », de sorte que les restrictions nécessitent des « raisons impérieuses »*[2/3]. La Cour de cassation a fait sienne cette interprétation en considérant que des propos, certes outrageants, mais exprimés sur *« un mode satirique*[4]*, dans un contexte polémique, au sujet des idées prêtées au responsable d'un parti politique ne dépassaient pas les limites admissibles de la liberté d'expression »*[5].

Néanmoins, toute liberté comporte ses exceptions, de surcroît lorsque l'élu outrepasse sa fonction ou revêt son habit d'homme ordinaire.

Dans la présente affaire, Mme Y, maire d'une commune, avait publié sur la page Facebook de sa mairie un commentaire où elle mettait en cause l'élue la précédant : *« Mme X. je connais un code pénal qui interdit aux anciens élus de voler des biens appartenant à la collectivité. Si vous voulez que nous rappelions sur cette page votre refus de restitution et notre menace de dépôt de plainte pour du matériel électronique appartenant à la collectivité après votre défaite, on peut »*. Ce commentaire avait été posté de son compte

2. CEDH, *Féret c. Belgique*, 10 décembre 2009, n° 15615/07.

3. Pour exemple, tenir des propos visant à porter atteinte, affaiblir ou détruire les idéaux et valeurs démocratiques (CEDH, *Parti de la prospérité et autres c. Turquie*, 13 février 2003, n° 41340/98, 41342/98, 41343/98, 41344/98 ou encore CEDH, *Orban et autres c. France*, 15 janvier 2009, n° 20985/08).

4. Sur la notion de satire, qui doit s'entendre comme « toute forme d'exagération et de déformation de la réalité visant à provoquer ou agiter », cf. CEDH, *Féret c. Belgique*, *op.cit.* note 2.

5. Crim., 20 septembre 2016, n° 15-82.942.

personnel. L'élue visée a assigné l'intéressée pour diffamation devant le TGI de Paris. En application du principe de séparation des autorités administratives et judiciaires, issu de la loi des 16 et 24 août 1790 et du décret du 16 fructidor an III, les avocats de la défense ont plaidé la nullité de l'assignation en raison de l'incompétence du juge judiciaire pour apprécier *« les conséquences dommageables d'une faute d'un agent public qui ne revêt pas le caractère d'une faute personnelle et détachable de la fonction »*. Ils estimaient que les propos tenus par la mairesse l'étaient en sa qualité de maire et engageaient par conséquent la responsabilité de la personne publique. Pour les juges, cette allégation ne saurait prospérer.

D'une part, les juges rappellent que *« la circonstance que les propos aient été publiés sur la page Facebook de la commune est indifférente, dans la mesure où,* ***pour apprécier la nature du comportement reproché, il convient d'examiner le compte Facebook, à partir duquel ont été publiés les passages litigieux*** *»*. Or, les constats d'huissiers révèlent qu'*« il n'est pas contesté que le compte utilisé pour la publication* ***est le compte Facebook personnel [de Mme Y]****, et non un compte consacré à ses activités de maire ou à la commune »*. D'autre part, le TGI de Paris estime ici qu'il n'y a pas besoin *« d'examiner le caractère personnel et détachable des fonctions de la faute reprochée »*, car *«* ***la publication litigieuse (…) ne relève pas de ses fonctions d'élus (…), ni ne ressort d'une activité d'un agent public*** *»*. Ils rejettent ainsi l'exception d'incompétence. Dès lors, sans qu'il soit besoin d'analyser la nature des propos, et donc le caractère détachable des fonctions, le caractère personnel du compte du réseau social suffit à caractériser la faute personnelle de l'agent.

Cette lecture est conforme à la position de la Cour de cassation qui a déjà eu l'occasion d'apprécier les propos tenus sur un autre réseau social : Twitter[6]. Dans ce cas d'espèce, un maire avait diffusé un extrait d'un projet de film porté par un élu de l'opposition lors d'un conseil municipal. Le tout était retranscrit en direct sur le site de la mairie. Ce film comportait des scènes où figuraient *« des jeunes femmes presque totalement dénudées dans des positions lascives »* et avait été tourné notamment dans les locaux de la mairie. Le maire, offusqué, déclara : *« l'image de la ville est terriblement ternie par cet acte »* et relaya sur son compte Twitter personnel des articles de presse évoquant *« le tournage d'un film pornographique »* dans la mairie. L'élu de l'opposition assigna le maire en diffamation devant le juge judiciaire. Le maire souleva l'exception d'incompétence au profit du juge administratif, estimant que ses propos étaient tenus *es qualité*. La Cour de cassation distingue ceux tenus lors du conseil municipal de ceux tenus sur Twitter. S'agissant de ces derniers, ils ont été tenus sur **un compte personnel *« libellé au nom de l'intéressé, sans autre précision »***, de sorte que rien ne pouvait prétendre qu'il s'agissait de celui du maire, ainsi il engage sa responsabilité personnelle. Les propos tenus lors du conseil municipal l'ont, quant à eux, été dans le cadre de l'exercice de ses fonctions d'élu, il appartenait donc aux juges d'analyser leur nature. La Cour de cassation confirme l'appréciation portée par les juges du fond qui soulignent que le maire a fait preuve *« d'une animosité personnelle »* à l'égard du plaignant en donnant une *« présentation trompeuse des séances réellement tournées dans les locaux de la mairie, faisant croire au public »* que toutes les scènes, dont les scènes litigieuses, y avaient été tournées. Ses propos étaient donc constitutifs d'une faute

6. Crim., 11 décembre 2018, n° 17-85159.

détachable du service engageant sa responsabilité personnelle. Dès lors, l'exception d'incompétence doit être rejetée.

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

OCTOBRE 2019

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

La Cour de justice de l'Union européenne (CJUE) a été saisie de trois renvois préjudiciels. Deux portent sur le « droit à l'oubli » et précisent l'arrêt CJUE du 13 mai 2014, Google Spain et Google (C-131/12). Le troisième explicite les obligations pesant sur un hébergeur au regard des contenus illicites. Simple rappel, le renvoi préjudiciel permet aux juridictions des États membres, saisies d'un litige, d'interroger la CJUE sur l'interprétation du droit de l'Union ou sur la validité d'un acte de l'Union. La Cour ne tranche pas le litige, mission qui relève de la juridiction nationale qui doit alors statuer en tenant compte de la décision de la Cour. Les dispositions de l'arrêt s'imposent aux autres juridictions des États membres ayant à statuer sur une question de droit similaire.

CJUE (Grande chambre), arrêt du 24 septembre 2019, C-507/17, Google LLC/ CNIL

L'exploitant d'un moteur de recherche qui fait droit à une demande de déréférencement est tenu d'opérer ce déréférencement non sur l'ensemble des versions de son moteur, mais sur les seules versions de celui-ci correspondant à l'ensemble des États membres. Il doit, si nécessaire, permettre d'empêcher ou de sérieusement décourager les internautes d'avoir accès aux liens qui font l'objet de cette demande, lorsqu'ils effectuent une recherche sur la base du nom de la personne concernée, depuis l'un des États membres (technique du « géo-blocage »).

La Cour a été saisie par le Conseil d'État dans le cadre d'un litige opposant Google LLC à la Commission nationale de l'informatique

et des libertés (CNIL) au sujet d'une sanction de 100 000 euros prononcée par celle-ci à l'encontre de Google en raison de son refus d'appliquer le droit au déréférencement à l'ensemble des extensions de nom de domaine de son moteur de recherche. Le droit au déréférencement – ou « droit à l'oubli » – est une des conséquences de l'arrêt CJUE du 13 mai 2014, Google Spain et Google (C-131/12). S'il ne supprime pas 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. Ce droit connaît quelques tempéraments, notamment lorsque la personne concernée est une personne publique. En effet, le déréférencement ne s'applique pas s'il apparaît, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant du public à avoir accès à l'information en question. 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 litige

À la suite de l'arrêt précité, Google a fait l'objet de nombreuses demandes. Mais le moteur de recherche a refusé de procéder au déréférencement sur les extensions autres que celles correspondant à des pays de l'Union européenne. Une personne physique s'est adressée à la CNIL pour faire droit à une demande de suppression de documents référencés par Google et la concernant. Par décision du 21 mai 2015, la présidente de la Commission nationale de l'informatique et des libertés (CNIL) a mis la société Google LLC en demeure de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom de la

personne, les liens menant vers des pages web et d'appliquer cette suppression sur toutes les extensions de nom de domaine de son moteur de recherche.

Mais Google n'a pas donné suite à cette mise en demeure, en limitant son action à une suppression partielle des liens : seuls ont été pris en compte les résultats affichés en réponse à des recherches effectuées sur les déclinaisons de son moteur dont le nom de domaine correspond à un État membre de l'Union (.fr,.eu,.de, etc.). N'ont pas ainsi été concernées les recherches via .com ou .org. Le moteur de recherche exploité par Google explore différents noms de domaine par des extensions géographiques. Grâce à l'identification de l'adresse IP de l'internaute, lorsque la recherche est effectuée depuis « google.com », Google procède, en principe, à une redirection automatique de cette recherche vers le nom de domaine correspondant au pays à partir duquel cette recherche est réputée être effectuée. L'internaute peut cependant, sans considération de sa localisation, effectuer ses recherches sur les autres noms de domaine du moteur de recherche. Par ailleurs, si les résultats peuvent différer selon le nom de domaine à partir duquel la recherche est effectuée sur le moteur, les liens affichés en réponse à une recherche proviennent de bases de données et d'un travail d'indexation communs.

À l'issue du délai de mise en demeure, Google a proposé une solution de « géo-blocage », consistant à supprimer la possibilité d'accéder, depuis une adresse IP réputée localisée dans l'État de résidence de la personne concernée, aux résultats litigieux obtenus à la suite d'une recherche effectuée à partir de son nom, quelle que soit la déclinaison du moteur de recherche sollicitée par l'internaute. Cette proposition a été jugée insuffisante par la CNIL qui, par délibération du 10 mars 2016, a prononcé à l'égard de Google une sanction, rendue publique, de 100 000 euros.

Google a alors saisi le Conseil d'État d'un recours relatif à cette sanction. Devant la juridiction administrative, Google a avancé que le « doit à l'oubli » n'implique pas nécessairement que les liens litigieux soient supprimés, sans limitation géographique, sur l'ensemble des noms de domaine de son moteur.

Les questions préjudicielles

Le Conseil d'État a sursis à statuer en posant à la CJUE plusieurs questions préjudicielles :
« - Le « droit au déréférencement », tel qu'il a été consacré par la CJUE dans son arrêt Google Spain et Google sur le fondement des dispositions de l'article 12, sous b), et l'article 14, sous a), de la directive 95/46, doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche est tenu, lorsqu'il fait droit à une demande de déréférencement, d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur de telle sorte que les liens litigieux n'apparaissent plus, quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée, y compris hors du champ d'application territorial de la directive ?

- En cas de réponse négative à cette première question, le « droit au déréférencement », tel que consacré dans l'arrêt précité, doit-il 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 ?
- En outre, en complément de l'obligation évoquée à la deuxième question, le « droit au déréférencement » doit-il être interprété en ce sens que l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est tenu de supprimer, par la technique dite du « géo-blocage », depuis une adresse IP réputée localisée dans l'État de résidence du bénéficiaire du « droit au déréférencement », les résultats litigieux des recherches effectuées à partir de son nom, ou même, plus généralement, depuis une adresse IP réputée localisée dans l'un des États membres soumis à la directive 95/46, ce, indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche ? ».

La solution de la CJUE

La position du G29 lors des débats rejoint celle de la CNIL lorsqu'elle considère *« [qu']afin de donner pleinement effet aux droits des personnes concernées définis dans l'arrêt de la Cour, les décisions de déréférencement doivent être exécutées de manière à garantir la protection efficace et complète des droits des personnes concernées et à ce que la législation européenne ne puisse pas être contournée. En ce sens, la limitation du déréférencement aux domaines de l'Union européenne au motif que les utilisateurs ont tendance à accéder aux moteurs de recherche par l'intermédiaire de leurs domaines nationaux ne peut donc pas être envisagée comme moyen suffisant pour garantir de manière satisfaisante les droits des personnes concernées conformément à l'arrêt de la Cour. En pratique, cela signifie que tout déréférencement devrait également être appliqué à tous les domaines concernés, y compris les domaines.com ».*
La position de la CNIL ne fait pas cependant l'unanimité. La

Commission et plusieurs États membres soutiennent que l'instauration d'un droit de déréférencement mondial sur le fondement du droit de l'Union ne serait compatible ni avec celui-ci, ni avec le droit international public et constituerait un précédent dangereux invitant des régimes autoritaires à exiger également la mise en œuvre à l'échelle mondiale de leurs décisions de censure. L'idée d'un déréférencement mondial peut paraître séduisante par sa radicalité, sa clarté, sa simplicité et son efficacité.
Google fait valoir que le droit au déréférencement n'implique pas nécessairement que les liens litigieux soient supprimés, sans limitation géographique, sur l'ensemble des noms de domaine de son moteur. En outre, en retenant une telle interprétation, la CNIL aurait méconnu les principes de courtoisie et de non-ingérence reconnus par le droit international public et porté une atteinte disproportionnée aux libertés d'expression, d'information, de communication et de la presse garanties, notamment, par l'article 11 de la Charte.
La CJUE rappelle qu'Internet est un réseau mondial sans frontières. Les moteurs de recherche confèrent un caractère ubiquitaire aux informations et aux liens contenus dans une liste de résultats affichée à la suite d'une recherche effectuée à partir du nom d'une personne physique. Dans ce contexte, l'accès des internautes, notamment de ceux qui se trouvent en dehors de l'Union, au référencement d'un lien renvoyant à des informations sur une personne dont le centre d'intérêts se situe dans l'Union, est susceptible de produire sur celle-ci des effets immédiats et substantiels au sein même de l'Union. Ce constat suffirait à justifier l'existence d'une compétence du législateur de l'Union pour prévoir l'obligation, pour l'exploitant d'un moteur de recherche, de procéder, lorsqu'il fait droit à une demande de déréférencement

formulée par une telle personne, à un déréférencement sur l'ensemble des versions de son moteur. Mais de nombreux États tiers ne connaissent pas le droit au déréférencement ou adoptent une approche différente de ce droit. La liberté d'information des internautes est susceptible de varier de manière importante à travers le monde. Ni la directive 95/46 ou l'article 17 du règlement 2016/679 n'indiquent que le législateur de l'Union a fait le choix de conférer aux droits consacrés à ces dispositions une portée qui dépasserait le territoire des États membres et qu'il aurait entendu imposer à un opérateur, tel Google, une obligation de déréférencement portant également sur les versions nationales de son moteur de recherche qui ne correspondent pas aux États membres. Il n'existe donc pas d'obligation découlant du droit de l'Union de procéder à un tel déréférencement sur l'ensemble des versions de son moteur.

Ainsi, pour la CJUE, *« 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 ».*

CJUE (Grande chambre), arrêt du 24 septembre 2019, C-136/17, GC, AF, BH, ED/ Commission nationale de l'informatique et des libertés (CNIL)

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 exemple, l'acquittement doit apparaître avant les poursuites).

Le litige

Le litige oppose quatre personnes à la Commission nationale de l'informatique et des libertés (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, qui est 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 de la CNIL. Les motifs des

quatre plaignants sont 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 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 ont saisi le Conseil d'État pour contester la décision de la CNIL. Dans tous les cas – ce qui explique leur jonction – la question des données dites « sensibles » est posée.

Les questions préjudicielles

Le Conseil d'État va surseoir à statuer et adresser une demande de décision préjudicielle à la CJUE qui porte 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).
Une première question porte sur l'opposabilité aux moteurs de recherche de l'interdiction, sous réserve des exceptions prévues, du traitement des données relevant de l'article 8 paragraphes 1 et 5 de la directive de 1995. Le paragraphe 1 (auj. art. 9 du RGPD) interdit aux États membres les traitements de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la santé ou la vie sexuelle. Le paragraphe 5, quant à lui (auj. art. 10 du RGPD), exige le contrôle de l'autorité publique sur les traitements relatifs aux infractions et condamnations pénales.

La seconde question porte sur les exceptions prévues par le paragraphe 2 de l'article 8 et l'article 9 et leur application par un moteur de recherche. Les interdictions prévues au paragraphe 2 ne s'appliquent pas, selon la directive, lorsque la personne concernée a donné son consentement explicite ou lorsqu'elle a manifestement rendu publiques les données considérées. L'article 9 offre des dérogations aux fins de journalisme et d'expression artistique, dans la mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression.

Une troisième question est plus orientée vers les obligations d'un moteur de recherche à l'égard des données devenues incomplètes ou inexactes, singulièrement s'agissant de procédure ou de condamnation pénale. Les dispositions de l'article 8, paragraphe 5, de la directive 95/46 doivent-elles être interprétées en ce sens que les informations relatives à la mise en examen d'un individu ou relatant un procès, et la condamnation qui en découle, constituent des données relatives aux infractions et aux condamnations pénales ? De manière générale, lorsqu'une page web comporte des données faisant état des condamnations ou des procédures judiciaires dont une personne physique a été l'objet, entre-t-elle dans le champ de ces dispositions ?

La décision de la CJUE

La CJUE rappelle les dispositions de son arrêt du 13 mai 2014 (Google Spain/Google, C-131/12) selon lesquelles l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de

préférence donné, doit être qualifiée de *« traitement de données à caractère personnel »*. L'exploitant de ce moteur de recherche doit être considéré comme le « responsable » dudit traitement. Il doit donc vérifier, dans le cadre de ses responsabilités, de ses compétences et de ses possibilités, que son activité respecte les exigences de la directive 95/46, notamment en ce qui concerne le droit à la vie privée.

Les dispositions de l'article 8, paragraphes 1 et 5, de la directive 95/46 (auj. art. 9 du RGPD) doivent être interprétées en ce sens que l'interdiction ou les restrictions relatives au traitement des catégories particulières de données à caractère personnel, visées par ces dispositions, *« s'appliquent, sous réserve des exceptions prévues par cette directive, également à l'exploitant d'un moteur de recherche dans le cadre de ses responsabilités, de ses compétences et de ses possibilités en tant que responsable du traitement effectué lors de l'activité de ce moteur, à l'occasion d'une vérification opérée par cet exploitant, sous le contrôle des autorités nationales compétentes, à la suite d'une demande introduite par la personne concernée »*. L'exploitant d'un moteur de recherche n'est pas responsable des données figurant sur la page web consultée mais du référencement de cette page. Le traitement effectué se distingue et s'ajoute à celui opéré par les éditeurs du web. Les exceptions prévues ne s'appliquent au moteur de recherche qu'en raison du référencement auquel il procède.
Sous réserve des exceptions prévues par la directive, l'exploitant d'un moteur de recherche a en principe l'obligation de faire droit aux demandes de déréférencement portant sur des liens menant vers des pages web sur lesquelles figurent des données à caractère personnel qui relèvent des catégories dites « sensibles ». Il est obligé de supprimer de la liste de résultats, affichée à la suite d'une

recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne. Cette obligation s'impose également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite. Mais le droit à la protection des données à caractère personnel n'est pas un droit absolu au regard de la fonction exercée par la personne dans la société, en particulier pour protéger la liberté d'information des internautes. L'exploitant peut refuser de déréférencer dès lors que le traitement est couvert par les exceptions prévues par la directive, aujourd'hui par le Règlement, sauf si le demandeur avance des raisons prépondérantes et légitimes tenant à sa situation personnelle.

Les informations relatives à une procédure judiciaire constituent des données relatives aux infractions et aux condamnations au sens de l'article 8 de la directive, indépendamment du fait que, au cours de la procédure judiciaire, la commission de l'infraction a été ou non établie.

Les données doivent être déréférencées si elles ne correspondent plus à la situation actuelle, dès lors qu'il est constaté que les droits de la personne prévalent sur ceux de l'internaute. Toutefois, en cas de maintien justifié par la liberté d'information des internautes, le moteur de recherche doit aménager la liste des résultats *« de telle sorte que l'image globale qui en résulte pour l'internaute reflète la situation judiciaire actuelle »*, ce qui conduit à changer l'ordre des résultats. Une page relative à l'acquittement ou au non-lieu doit figurer avant celles évoquant les poursuites.

CJUE (troisième chambre), arrêt du 3 octobre 2019, C-18/18, Eva Glawischnig-Piesczek/Facebook Ireland Limited

Le droit de l'Union ne s'oppose pas à ce qu'un hébergeur soit enjoint de supprimer des commentaires identiques et, sous certaines conditions, équivalents à un commentaire précédemment déclaré illicite. Il ne s'oppose pas non plus à ce qu'une telle injonction produise des effets à l'échelle mondiale, dans le cadre du droit international pertinent.

Le litige

Un litige oppose Mme Glawischnig-Piesczek, alors députée au Nationalrat (Conseil national en Autriche), présidente du groupe parlementaire « Die Grünen » (Les Verts) et porte-parole fédérale du parti, au réseau social Facebook Ireland qui exploite une plateforme pour les utilisateurs situés en dehors des États-Unis d'Amérique et du Canada.

Un utilisateur de Facebook Service a partagé, sur sa page personnelle, un article du magazine d'information autrichien en ligne *oe24.at* intitulé « Les Verts : en faveur du maintien d'un revenu minimum pour les réfugiés », ce qui a eu pour effet de générer sur cette page un « aperçu vignette » du site d'origine, comportant le titre de cet article, un bref résumé de ce dernier ainsi qu'une photographie de Mme Glawischnig-Piesczek. Cet utilisateur a, en outre, publié, au sujet de cet article, un commentaire rédigé dans des termes dont la juridiction de renvoi a constaté qu'ils étaient de nature à porter atteinte à l'honneur de la requérante, à l'injurier et à la diffamer. Cette contribution pouvait être consultée par chaque utilisateur de Facebook Service. La plaignante a

demandé sans succès à Facebook d'effacer le commentaire. La procédure a abouti devant l'Oberster Gerichtshof, la Cour suprême d'Autriche. Devant statuer sur la question de savoir si l'injonction de cessation, délivrée à un hébergeur qui exploite un réseau social comptant de nombreux utilisateurs, peut aussi être étendue aux déclarations textuellement identiques et/ou de contenu équivalent dont celui-ci n'a pas connaissance, elle indique que, selon sa propre jurisprudence, une telle obligation doit être considérée comme étant proportionnée, lorsque l'hébergeur a déjà pris connaissance d'au moins une atteinte aux intérêts de la personne concernée causée par la contribution d'un utilisateur et que le risque de voir d'autres violations être commises est ainsi avéré. L'Oberster Gerischstof pose néanmoins des questions préjudicielles.

Les questions préjudicielles

La demande de décision préjudicielle porte sur l'interprétation de l'article 15, paragraphe 1, de la directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique », transposée dans le droit français par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique).

Cette directive définit les responsabilités qui pèsent sur les hébergeurs, les éditeurs et moteurs de recherche. Son article 14, intitulé « Hébergement », dispose que les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service.

Deux conditions sont toutefois émises :

- le prestataire n'a pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'a pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ;
- le prestataire, dès le moment où il a de telles connaissances, doit agir promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

L'article 15, paragraphe 1, de cette directive, au cœur du renvoi, dispose que les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services par un hébergeur, une obligation générale de surveiller les informations qu'il transmet ou stocke, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites. La responsabilité de l'hébergeur est donc limitée.

Les questions préjudicielles sont ainsi rédigées :

1) *« Lorsqu'un hébergeur n'a pas promptement retiré certaines informations illicites, l'article 15, paragraphe 1, de la directive 2000/31 s'oppose-t-il, d'une manière générale, à ce que soit imposée une des obligations suivantes :*

- *retirer ces informations illicites elles-mêmes, au sens de l'article 14 de la directive ;*
- *retirer également d'autres informations identiques :*

- au niveau mondial,

- dans l'État membre concerné,

- du destinataire concerné du service au niveau mondial,

- du destinataire concerné du service dans l'État membre concerné ? »

2) En cas de réponse négative à la première question : *« en va-*

t-il de même concernant les informations de contenu équivalent ?
3) En va-t-il de même concernant les informations de contenu équivalent, dès le moment où l'exploitant a connaissance de cette circonstance ? »

La décision de la CJUE

La Cour rappelle que l'interdiction d'imposer une obligation de surveillance générale des contenus n'exclut pas une surveillance *« applicable à un cas spécifique »*. Un tel cas spécifique peut notamment trouver son origine dans une information précise, stockée par l'hébergeur, dont le contenu a été analysé et déclaré illicite par une juridiction compétente de l'État membre. En l'espèce, il s'agit de propos qualifiés de diffamatoires.
L'injonction adressée doit pouvoir s'étendre aux informations dont la formulation peut être légèrement différente, tout en véhiculant le même message afin d'éviter une multiplication des instances, chaque fois qu'un mot est changé ou que la tournure de la phrase est modifiée. Le sens du contenu l'emporte sur sa forme dès lors qu'il aboutit au même résultat.
Pour la CJUE, Facebook Ireland avait connaissance de l'information illicite en cause et n'a pas agi promptement aux fins de la retirer ou de rendre l'accès à celle-ci impossible, comme le prévoit l'article 14 de la directive 2000/31.
Eu égard à la dimension mondiale d'Internet, le législateur de l'Union a considéré qu'il était nécessaire d'assurer la cohérence des règles de l'Union dans ce domaine avec les règles applicables au niveau international. La directive 2000/31 ne s'oppose donc pas à ce que lesdites mesures d'injonction produisent des effets à l'échelle mondiale.
Dans ces conditions, une juridiction d'un État membre peut :

- enjoindre à un hébergeur de supprimer les informations qu'il stocke et dont le contenu est identique à celui d'une information déclarée illicite précédemment ou de bloquer l'accès à celles-ci, quel que soit l'auteur de la demande de stockage de ces informations ;
- enjoindre à un hébergeur de supprimer les informations qu'il stocke et dont le contenu est équivalent à celui d'une information déclarée illicite précédemment ou de bloquer l'accès à celles-ci, pour autant que la surveillance et la recherche des informations concernées par une telle injonction sont limitées à des informations véhiculant un message dont le contenu demeure, en substance, inchangé par rapport à celui ayant donné lieu au constat d'illicéité et comportant les éléments spécifiés dans l'injonction et que les différences dans la formulation de ce contenu équivalent par rapport à celle caractérisant l'information déclarée illicite précédemment ne sont pas de nature à contraindre l'hébergeur à procéder à une appréciation autonome de ce contenu ;
- enjoindre à un hébergeur de supprimer les informations visées par l'injonction ou de bloquer l'accès à celles-ci au niveau mondial, dans le cadre du droit international pertinent.

Par le lieutenant Océane GERRIET

La preuve à l'ère numérique : la fin ne justifie pas les moyens !

TGI de Paris, ordonnance du juge des référés du 2 août 2019

Dans cette ordonnance rendue sous la forme du référé, le TGI de Paris rappelle le principe de licéité de la preuve, de surcroît lorsqu'il s'agit des données, protégées par le sacro-saint Règlement général sur la protection des données (RGPD)[1].

La société « Mile High Distribution », société canadienne de films, constate la présence de ses œuvres sur des plateformes en ligne auxquelles elle n'a accordé aucune autorisation. Déterminée, elle demande à une société allemande, « Media protector », de collecter les données liées au téléchargement de ses œuvres aux fins d'identifier les contrevenants. Armée d'une liste de 895 adresses IP, elle cite devant le juge des référés la société Orange et demande à obtenir la communication des données d'identification des adresses IP.

En effet, **l'article 145 du Code de procédure civile** permet à tout intéressé d'obtenir *« avant tout procès »* et en cas de *« motif légitime »*, les preuves dont *« pourrait dépendre la solution d'un litige »*. À cette fin, des *« mesures d'instruction légalement*

1. 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

admissibles, peuvent être ordonnées (…) sur requête ou en référé ». La société canadienne avait sans conteste un motif légitime à agir en ce qu'il s'agissait de préserver et de protéger ses droits d'auteur. Néanmoins, comme le soulève la société Orange, la légalité de la mesure d'instruction attendue suscite des doutes quant à la licéité de la collecte d'adresses IP. Elle estime que, s'agissant d'un traitement de données à caractère personnel, la société demanderesse n'a pas respecté la réglementation relative à la protection de ce type de données. Il est à noter que les faits litigieux se sont déroulés avant et après le 25 mai 2018, de sorte que le juge des référés a dû appliquer tantôt la loi du 6 janvier 1978, tantôt le RGPD.

En tout état de cause, il est de jurisprudence constante que les mesures sollicitées dans le cadre du référé-probatoire ne doivent pas porter *« atteinte à une liberté fondamentale »*[2]. **Or, la protection des données personnelles est un droit fondamental** mentionné à l'article 8 de la charte des droits fondamentaux de l'Union Européenne[3] (UE) et faisant partie intégrante du respect de la vie privée et familiale, droit fondamental garanti par l'article 8 de la Cour européenne des droits de l'Homme[4].

En l'espèce, en collectant massivement des adresses IP, la société demanderesse reconnaît que son opération doit être considérée comme un « traitement de données à caractère personnel » au sens de **l'article 2 de la loi du 6 janvier 1978**[5] (pour les faits antérieurs

2. Civ. 2ème, 8 février 2006, n° 05-14.198.
3. 2000/C 364/01 du 18 décembre 2000.
4. CEDH, *S. et Marper c. Royaume-Uni*, 4 décembre 2008, n° 30562/04 et 30566-04.
5. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

au 25 mai 2018) et **de l'article 4 du RGPD**. Pour rappel, ce dernier définit la *« donnée à caractère personnel »* comme *« toute information se rapportant à une personne physique identifiée ou* identifiable *(…) »* et précise qu'est réputée être *« 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 (…) ».* La Cour de justice de l'Union Européenne a déjà eu l'occasion d'affirmer que l'adresse IP était une donnée à caractère personnel, car elle permet *« l'identification précise [de l'utilisateur] »*[6], qu'elle soit fixe ou dynamique[7]. Cette position a été confirmée par la Cour de cassation en 2016 qui a rappelé que *« la collecte (…) d'adresses IP qui permettent l'identification des utilisateurs constitue un traitement automatisé de données à caractère personnel contenu dans un fichier lequel doit donner lieu à déclaration à la CNIL »*[8].

De jure, conformément à l'article 3 dudit RGPD, l'entreprise ne pouvait ignorer que le présent règlement s'appliquait, car même si elle est située en dehors de l'UE, il s'agit de données appartenant à des personnes se trouvant sur ce territoire et le traitement a pour objectif de suivre le comportement de ces personnes. Ainsi, elle doit respecter la réglementation susmentionnée, notamment : l'existence d'un registre du traitement mis en œuvre, la désignation d'un représentant du traitement au sein de l'UE, le respect des règles relatives à la sécurité et à la confidentialité des données et

6. CJUE C-70/10 du 24 novembre 2011.
7. CJUE C-582-14 du 19 octobre 2016.
8. Civ. 1ère, 3 novembre 2016, n° 15-22595.

l'encadrement de leur transfert, y compris en dehors de l'UE. Le juge des référés va même plus loin en estimant que cette collecte – s'inscrivant dans la lutte contre la contrefaçon sur Internet – doit être considérée comme une *« une collecte à grande échelle de données d'infraction au sens de* ***l'article 10 du RGPD*** *»* de sorte que, conformément à **l'article 37 du RGPD**, un tel traitement obligeait à désigner un *data protection officer*. Pour aller plus loin, en 2016, le juge des référés de Meaux[9] a été saisi d'un référé-probatoire dans des conditions sensiblement similaires à celles de l'espèce. Une société demanderesse avait collecté l'adresse IP d'un expéditeur de courriels qu'elle estimait frauduleux et en demandait l'identification. Malgré sa plainte, le juge des référés souligne que seules les autorités judiciaires sont habilitées à demander la communication de telles données et qu'une telle collecte consiste en un traitement de données à caractère personnel répondant aux exigences de la loi de 1978.

En tout état de cause, pour le cas d'espèce, il appert que la société demanderesse ne produit aucun élément permettant d'attester de la régularité de ce traitement et du respect des obligations citées *supra*. La simple *« déclaration de conformité auprès de la CNIL »* ne saurait suffire à démontrer la licéité du traitement, car elle n'est qu'une étape préalable visant à obtenir l'autorisation de mise en œuvre de celui-ci. Dès lors, malgré la protection de ses propres intérêts (droit de la propriété intellectuelle), l'absence de licéité du traitement constitue *« un empêchement légitime »* à l'application du référé-probatoire, car il représente *« une atteinte illégitime et disproportionnée aux droits et libertés fondamentales d'autrui, en*

9. Ordonnance du juge des référés du TGI de Meaux en date du 10 août 2016, *France sécurité c. NC Numéricable.*

l'espèce le droit à la protection des données à caractère personnel des individus dont les adresses IP ont été collectées ». Par conséquent, il ne pouvait être donné suite à la requête de la société « Mile High Distribution ».

La fin ne justifie donc pas les moyens. Une fois encore, la loi se rappelle au cyberespace et met fin peu à peu à la *« cyber-utopie libertaire »*[10].

10. *Electronic Frontier Fondation. A declaration of the independance of the cyberspace, by John Perry Barlow.* [Consulté le 16 octobre 2019]. Disponible sur : https://www.eff.org/cyberspace-independence.

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

NOVEMBRE 2019

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

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

JURISPRUDENCE ADMINISTRATIVE

Droit au déréférencement (« droit à l'oubli »)

Le Conseil d'État applique les principes définis par l'arrêt CJUE (Grande chambre) du 24 septembre 2019 (C-136/17, GC, AF, BH, ED/ Commission nationale de l'informatique et des libertés, voir *supra*, p. 129-135). 13 décisions, du 6 décembre 2019, fixent le cadre dans lequel un exploitant de moteur de recherche doit, sous le contrôle de la CNIL, appliquer le droit au déréférencement.

Rappel des faits

Le droit au déréférencement – ou « droit à l'oubli » – est une des conséquences de l'arrêt CJUE du 13 mai 2014, *Google Spain et Google* (C-131/12). S'il ne fait pas disparaître le document que le plaignant estime contraire à sa vie privée, il supprime les liens vers les pages web qu'offre le moteur de recherche. Conformément au règlement 2016/679 (art. 17 du Règlement général sur la protection des données – RGPD), ce droit au déréférencement est dénommé « droit à l'effacement » ou « droit à l'oubli ».
Un litige opposait quatre personnes à la Commission nationale de l'informatique et des libertés (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 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 Cour de justice de l'Union européenne (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 proportionnalité entre les droits du demandeur et ceux de l'internaute. Les données relatives aux procédure 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 exemple, 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[1], soit la 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

1. 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).

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 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.

Les 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 2019.

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'Église 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).

Les données pénales (relatives à une procédure judiciaire ou à une condamnation pénale)

Dans son arrêt du 24 septembre 2019 précité, la CJUE avait

considéré que les informations relatives à une procédure judiciaire constituent des données relatives aux infractions et aux condamnations au sens de l'article 8 de la directive de 1995, indépendamment du fait que, au cours de la procédure judiciaire, la commission de l'infraction a été ou non établie. Les données doivent être déréférencées si elles ne correspondent plus à la situation actuelle, dès lors qu'il est constaté que les droits de la personne prévalent sur ceux de l'internaute. Toutefois, en cas de maintien justifié par la liberté d'information des internautes, le moteur de recherche doit aménager la liste des résultats *« de telle sorte que l'image globale qui en résulte pour l'internaute reflète la situation judiciaire actuelle »*, ce qui conduit à changer l'ordre des résultats. Une page relative à l'acquittement ou au non-lieu doit figurer avant celles évoquant les poursuites.

Le Conseil d'État reprend ces règles : même lorsqu'il apparaît que le référencement de telles données non actualisées est légal, l'exploitant d'un moteur de recherche n'en est pas moins tenu d'aménager la liste des résultats de telle sorte que celle-ci fasse d'abord apparaître au moins un lien menant vers une page web comportant des informations à jour, afin que l'image en résultant soit fidèle à la situation judiciaire actuelle de la personne concernée. Dans tous les cas, le maintien des liens avec des informations pénales doit être strictement nécessaire à l'information du public.

Dans une des affaires jugées le 6 décembre 2019, le Conseil d'État a estimé qu'un particulier, condamné en 2010 à une peine de sept ans d'emprisonnement, peut demander le déréférencement des liens menant vers des chroniques judiciaires exactes faisant état de sa condamnation, alors même qu'il est toujours sous suivi socio-judiciaire. *« Le maintien de ces liens – relatifs à des faits anciens et concernant un individu sans notoriété – ne peut être regardé* comme

strictement nécessaire à l'information du public, ce d'autant plus que l'accès aux données relatives à des condamnations pénales (notamment au casier judiciaire) n'est en principe possible, en France, que dans des conditions strictement limitées » (arrêt n° 401258). En revanche, l'accès du public à des articles de presse relatant la condamnation d'un maire, pour apologie de crimes de guerres ou contre l'humanité, est strictement nécessaire à l'information du public. L'annulation de la condamnation en cassation ne suffit pas à rendre illégal le référencement des liens, compte tenu de la notoriété de l'intéressé et des conditions dans lesquelles les propos litigieux ont été tenus et repris. En outre, les pages vers lesquelles ils mènent comportent un *addendum* mentionnant cette décision de justice ultérieure (arrêt du 6 décembre n° 405464). Enfin, une actrice d'une série diffusée à la télévision ne peut exiger le déréférencement de liens menant vers des articles faisant état de sa condamnation, en 2018, pour des faits de violence conjugale. Ces articles reprennent des propos qu'elle a tenus, dans une interview récente donnée au sujet de sa condamnation, et sont donc strictement nécessaires à l'information du public (arrêt du 6 décembre n° 429154).

Les données touchant à la vie privée sans être sensibles

Le droit au déréférencement n'est pas absolu. La CNIL peut refuser de faire droit à la demande s'il existe un intérêt prépondérant du public à accéder à l'information en cause.
Le droit à la liberté de l'information l'emporte alors sur le droit au respect de la vie privée du demandeur.
Ainsi, un particulier est fondé à demander le déréférencement de liens menant vers des pages web relatives au brevet d'invention qu'il a déposé et mentionnant son adresse personnelle. Dans ce cas

en effet, l'intérêt du public à accéder à l'information n'est pas prépondérant. Le demandeur n'a déposé qu'un brevet, ancien et ayant expiré. Les moyens de le joindre peuvent être trouvés par d'autres voies (arrêt du 6 décembre n°405910). Mais l'intérêt du public à accéder à des informations relatives à l'activité et aux coordonnées professionnelles d'un médecin généraliste est prépondérant et justifie le refus de la CNIL de procéder au déréférencement des liens menant vers ces informations (arrêts du 6 décembre, n° 403868 et 403869).

JURISPRUDENCE JUDICIAIRE

Vie privée et outils informatiques professionnels

Cour de cassation, ch. sociale (n° 17-28448) arrêt du 23 octobre 2019, Mme P/ société I…N…

Sont couverts par le secret des correspondances les messages électroniques, échangés au moyen d'une messagerie instantanée, à partir d'un ordinateur professionnel, provenant d'une boîte aux lettres électronique personnelle, distincte de la messagerie professionnelle.

Madame P, secrétaire au sein de la société I…N…, a été licenciée pour faute grave. Son employeur a constaté en son absence que la boîte de messagerie personnelle instantanée MSN Messenger de son employée, accessible depuis son ordinateur professionnel, comprenait des échanges d'ordre privé avec une autre employée et mettait en évidence des transferts de documents confidentiels appartenant à l'entreprise auxquels elle ne pouvait avoir accès

compte tenu de ses fonctions. Outre l'envoi de mails comprenant des *« considérations personnelles ou des éléments personnels de sa vie privée, totalement étrangers au fonctionnement de l'entreprise »*, l'employeur lui reproche un vol de documents à des fins personnelles en vue de les divulguer à des employés.

La cour d'appel de Paris, dans un arrêt du 28 septembre 2017, a donné tort à l'employeur qui avait accédé à sa boîte personnelle. Elle a estimé que les messages instantanés ne constituaient pas des modes de preuve licites, au motif qu'*« à l'évidence un tel compte de messagerie est personnel et distinct de la messagerie professionnelle sans qu'il soit besoin d'ajouter une mention « personnel » ou encore « conversation personnelle »*.

La Cour de cassation a validé la position de la cour d'appel. Elle confirme ainsi sa jurisprudence posée par l'arrêt NIKON (Cass. Soc., n° 99-42942, 2 décembre 2001) et affirmant le droit du salarié au respect de sa vie privée sur son lieu de travail : les courriels adressés et reçus par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, en sorte que l'employeur est en droit de les ouvrir en dehors de la présence de l'intéressé, sauf si le salarié les identifie comme personnels (voir également Cass.soc., n° 12-11866, 16 mai 2013). La même position a été prise plus récemment (Cass.soc, n°14-27949, 7 avril 2016) à l'égard d'une cour d'appel qui n'avait pas vérifié si un message électronique litigieux était issu d'une boîte à lettre électronique personnelle, distincte de la messagerie professionnelle, couverte par le secret des correspondances.

L'usage « mixte » de moyens informatiques mis à la disposition d'un employé par son entreprise a fait l'objet d'une abondante jurisprudence.

S'agissant des fichiers, la Cour de cassation, chambre sociale, dans un arrêt du 21 octobre 2009 (n° 07-43.877), a jugé que les dossiers et fichiers, créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur, sont présumés avoir un caractère professionnel, sauf si le salarié les identifie comme étant personnels, de sorte que l'employeur peut y avoir accès hors sa présence. Cette ligne de partage s'applique aux documents contenus sur une clé USB (Cass.soc. n° 11-28649, 12 février 2013).
Seul le risque ou un événement particulier peut autoriser l'accès, hors de la présence du salarié, aux fichiers informatiques identifiés comme personnels. Cette position a été confirmée par l'arrêt du 4 juillet 2012 de la chambre sociale de la Cour de cassation (n° 11-12502). Elle a été validée par la Cour européenne des droits de l'Homme (5e section, arrêt du 22 février 2018) qui a jugé qu'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.
En ce qui concerne un téléphone portable mis à la disposition de l'employé, la Cour de cassation (Cass. com., n° 13-14779, 10 décembre 2015) a pris une position similaire : *« les messages écrits (« short message service » ou SMS) envoyés ou reçus par le salarié au moyen du téléphone mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, en sorte que l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels ; qu'il en résulte que la production en justice des messages n'ayant pas été identifiés comme étant personnels par le salarié ne constitue pas un procédé déloyal au sens des articles 9 du code civil et 6, paragraphe 1, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales rendant irrecevable ce mode de preuve »*.

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

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** **Lieutenant Océane GERRIET**
Équipe éditoriale :	**Odile NETZER**

Veille juridique /Droit de l'espace numérique - 2019