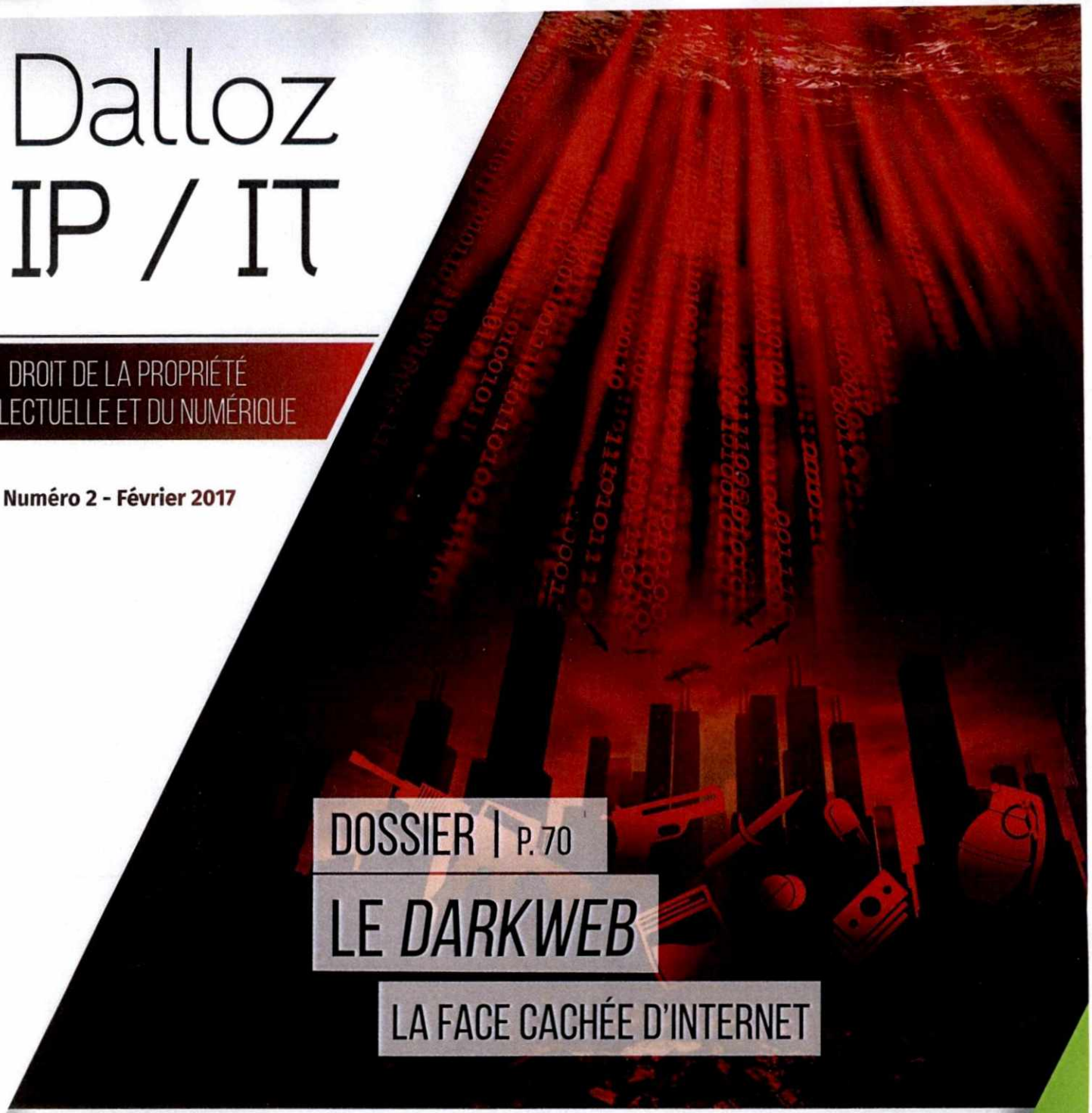
Dalloz IP / IT

DROIT DE LA PROPRIÉTÉ INTELLECTUELLE ET DU NUMÉRIQUE

Numéro 2 - Février 2017

9 782997 517020



DOSSIER | P. 70

LE *DARKWEB*

LA FACE CACHÉE D'INTERNET

PRATIQUE

La grande réforme du droit des marques en Europe : quel impact pour les praticiens ?

Juliette Robin et Juliette Dhuyser

TEXTES ET DÉCISIONS

Pourquoi l'arrêt *Soulier et Doke* dépasse le cas ReLire : le contrôle par la CJUE des modalités de l'autorisation préalable de l'auteur
CJUE 16 novembre 2016

Valérie-Laure Benabou

TEXTES ET DÉCISIONS

Compétence judiciaire pour connaître d'actions en responsabilité dirigées contre l'INPI : la Cour de cassation fait bloc
Civ. 1re, 3 novembre 2016

Frédéric Pollaud-Dulian

Version numérique incluse

DALLOZ

DROIT DU NUMÉRIQUE / DONNÉES À CARACTÈRE PERSONNEL

L'adresse IP est bien une donnée à caractère personnel

Référence

CJUE 19 octobre 2016, aff. C-582/14
Civ. 1re, 3 novembre 2016, n° 15-22.595

Mots-clés

DONNÉES À CARACTÈRE PERSONNEL – Traitement de données à caractère personnel – Adresse IP

Fondement

Loi n° 78-17 du 6 janvier 1978, art. 2 et 22 ;
Directive 95/46/CE du 24 octobre 1995, art. 2, art. sous a) et 7, art. sous f)

Solution : La Cour de justice de l'Union européenne a décidé, dans un arrêt du 19 octobre 2016 :

1) « *[...] une adresse de protocole Internet dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel au sens de cette disposition, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à Internet de cette personne* ».

2) « *L'article 7, sous f), de la directive 95/46 doit être interprété en ce sens qu'il s'oppose à une réglementation d'un État membre en vertu de laquelle un fournisseur de services de médias en ligne ne peut collecter et utiliser des données à caractère personnel afférentes à un utilisateur de ces services, en l'absence du consentement de celui-ci, que dans la mesure où cette collecte et cette utilisation sont nécessaires pour permettre et facturer l'utilisation concrète desdits services par cet utilisateur, sans que l'objectif puisse justifier l'utilisation desdites données après une session de consultation de ceux-ci* ».

Peu de temps après, dans un arrêt du 3 novembre 2016, la Cour de cassation a suivi la Cour de justice et décidé que « *[...] les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la CNIL [...]* ».

Observations : Par deux décisions rendues le 19 octobre 2016 et le 3 novembre 2016, la Cour de justice de l'Union européenne et la Cour de cassation ont successivement qualifié l'adresse IP (*Internet Protocol*) de donnée à caractère personnel, mettant ainsi un terme à une incertitude juridique longtemps entretenue par ces deux juridictions.

Dans la première espèce, soumise à l'examen de la Cour de justice, un ressortissant allemand, M. Breyer, avait consulté des sites internet des services fédéraux allemands, lesquels sites enregistraient l'adresse IP des visiteurs et les conservaient aux termes des sessions de consultation afin de se prémunir contre des attaques informatiques. M. Breyer avait introduit devant les juridictions allemandes un recours visant à ce qu'il soit fait interdiction à l'Allemagne de conserver ou de faire conserver, au terme des sessions de consultation des sites internet des services fédéraux allemands, l'adresse IP du système hôte accédant. La Cour fédérale de justice allemande a saisi la Cour de justice de deux questions préjudicielles. À la première question portant sur l'interprétation de la notion de donnée à caractère personnel telle qu'elle ressort de l'article 2 de la directive 95/46/CE du 24 octobre 1995, la Cour de justice a affirmé qu'une adresse IP dynamique enregistrée par un fournisseur de services à l'occasion d'un accès à un site internet constituait pour celui-ci une donnée à caractère personnel même si c'est un tiers qui dispose des informations nécessaires pour identifier la personne concernée. À la seconde question, portant sur l'interprétation des conditions de licéité d'un traitement de données à caractère personnel telles que prévues par l'article 7 de cette directive, la Cour de justice a décidé que la collecte et l'utilisation, par un fournisseur de services de médias, des données à caractère personnel afférentes à l'utilisateur de ces services en l'absence de consentement de celui-ci pouvaient être justifiées par l'intérêt légitime du responsable de traitement dont l'objectif est de garantir la capacité générale de fonctionnement de ces services.

Dans la seconde espèce, soumise à l'examen de la Haute juridiction française, trois sociétés d'un même groupe ayant constaté des connexions frauduleuses sur leur réseau informatique interne ont formé une requête sur le fondement de l'article 145 du code de procédure civile de façon à obtenir de plusieurs fournisseurs d'accès à internet la communication de l'identité des titulaires des adresses IP utilisées pour les connexions litigieuses. Une personne morale, identifiée par le biais de cette mesure d'instruction et ayant formé une demande de rétractation de l'ordonnance rendue, a invoqué l'illicéité de la mesure en arguant du fait que la conservation sous forme de fichier de ces adresses IP aurait dû faire l'objet d'une déclaration auprès de la CNIL. La Cour de cassation, interrogée sur la nécessité ou non de déclarer un tel fichier devait au préalable qualifier l'adresse IP, ce qu'elle a fait en décidant que ces adresses en tant qu'elles permettent d'identifier indirectement une personne physique sont des données à caractère personnel, de sorte que leur traitement devait faire l'objet d'une déclaration auprès de la CNIL.

À quelques semaines d'intervalle, la Cour de justice de l'Union européenne et la Cour de cassation adoptent donc la même approche en qualifiant l'adresse IP de donnée à caractère personnel (I), ce qui est lourd de conséquence car cela induit l'application à l'adresse IP du régime de protection propre aux données à caractère personnel (II).

I - L'ADRESSE IP QUALIFIÉE DE DONNÉE À CARACTÈRE PERSONNEL

La Cour de cassation et la Cour de justice s'accordent pour considérer que l'adresse IP ne permet pas en elle-même d'identifier une personne, mais, qu'en revanche, elle constitue un moyen d'identification indirecte en ce qu'elle permet d'obtenir d'un tiers, le fournisseur d'accès à Internet, des informations complémentaires (A). Ces solutions concordantes participent d'une acception large de la notion de donnée à caractère personnel (B).

A - L'adresse IP comme moyen d'identification indirecte de la personne

Il ne fait pas de doute que l'adresse IP, en tant qu'elle est constituée d'une suite de chiffres ne permet pas d'identifier directement la personne concernée. Pour ce faire, il convient d'obtenir des données supplémentaires. Les informations permettant d'identifier la personne se cachant derrière une adresse IP n'étaient, dans aucun des deux cas d'espèce, détenues par la personne qui avait connaissance de l'adresse IP, mais par un fournisseur d'accès à Internet. Il fallait donc croiser plusieurs informations détenues par deux personnes différentes, de manière à identifier la personne concernée, titulaire de l'adresse IP.

La loi du 6 janvier 1978, dans sa version initiale, considérait déjà qu'étaient « réputées nominatives [...] les informations permettant [...] directement ou non, l'identification des personnes physiques ». La version actuelle de la loi, issue de la transposition de la directive de 1995 par la loi n° 2004-575 du 21 juin 2004, prévoit que « [c]onstitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».

La Cour de justice l'a encore précisé dans sa décision : « l'utilisation par le législateur de l'Union du terme « indirectement » tend à indiquer que, afin de qualifier une information de donnée à caractère personnel, il n'est pas nécessaire que cette information permette, à elle seule d'identifier la personne concernée » (§ 41).

Qualifier l'adresse IP de donnée à caractère personnel en tant qu'elle permet indirectement, par le biais du fournisseur d'accès à Internet, d'identifier une personne est donc parfaitement conforme au texte de la Directive de 1995 et de la loi de 1978.

La Cour de justice dans une décision du 29 janvier 2008 (*Promusicae*, aff. C-275/06, D. 2008. 480, obs. J. Daleau ; RTD com. 2008. 302, obs. F. Pollaud-Dulian ; RTD eur. 2008. 405, chron. J. Schmidt-Szalewski) avait déjà implicitement qualifié l'adresse IP de donnée à caractère personnel dans le cadre d'une contrefaçon de droit d'auteur. Plus récemment, dans un arrêt du 24 novembre 2011 (*Scarlet Extended*, aff. C-70/10, D. 2011. 2925, obs. C. Manara ; *ibid.* 2012. 2343, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *ibid.* 2836, obs. P. Sirinelli ; RSC 2012. 163, obs. J. Francillon ; RTD eur. 2012. 404, obs. F. Benoît-Rohmer ; *ibid.* 957, obs. E. Treppoz) et cité dans la décision commentée, la Cour de justice avait considéré de manière plus explicite que les adresses IP des utilisateurs d'Internet étaient des données à caractère personnel.

En revanche, la jurisprudence française, par deux arrêts de la Cour d'appel de Paris du 27 avril et du 15 mai 2007 rejetait la qualification de données à caractère personnel pour les adresses IP dans le contexte d'actes de contrefaçon en ligne. Par un arrêt du 28 mai 2008, la Cour d'appel de Paris confirmait ultérieurement cette position (sur cette jurisprudence, V. M. Teller, Les difficultés de l'identité numérique : quelle qualification juridique pour l'adresse IP ?, D. 2009. 1988). Pourtant, dans un avis du 20 juin 2007 relatif à la notion de données à caractère personnel, le groupe des CNIL européennes, dit « G29 », a clairement affirmé que l'adresse IP attribuée à un internaute lors de ses communications constituait une donnée à caractère personnel (« Avis 4/2007 sur le concept de données à caractère personnel » – Groupe de travail « article 29 » sur la protection des données, 01248/07/FR WP136).

Alors que la Cour de justice a précisé que les adresses IP dynamiques, qui varient à chaque connexion de l'internaute, étaient des données à caractère personnel. En revanche, elle ne se prononce pas sur les adresses IP statiques, qui sont quant à elles, attribuées par le fournisseur d'accès à un internaute de manière fixe. À la différence de la Cour de justice, la Cour de cassation n'indique pas la nature des adresses IP en litige et semble ainsi qualifier indifféremment toutes les adresses IP de donnée à caractère personnel. De toute évidence, l'identification d'une personne par le biais d'une adresse statique apparaît plus aisée que par le biais d'une adresse IP dynamique, qui suppose pour cette dernière de connaître l'heure précise de connexion aux fins d'identification de l'internaute titulaire de l'adresse IP litigieuse au moment de faits. *A fortiori*, si l'adresse IP dynamique est qualifiée de donnée à caractère personnel, il

ne peut donc qu'en être de même s'agissant de l'adresse IP statique.

B - Une acception large de la notion de donnée à caractère personnel

En pratique, la possibilité d'identifier indirectement une personne par le biais d'une adresse IP appelle certaines réserves.

Les deux décisions commentées s'appuient sur un présupposé qui est le suivant : un tiers, ici le fournisseur d'accès à internet, détient les coordonnées de la personne titulaire d'une adresse IP, grâce auxquelles il est possible de l'identifier.

Or, la réalité est autrement plus complexe. Pour le comprendre, il suffit de songer, dans le contexte de la cybercriminalité, aux difficultés rencontrées par les services de police pour identifier les auteurs d'attaques en déni de services (autrement appelées « DDOS » pour *Distributed Denial of Service*). Ces attaques, qui consistent en l'envoi d'une multitude de requêtes informatiques correspondant à des connexions à un site internet, ou à un serveur de manière plus générale, de façon à entraver son bon fonctionnement, restent souvent impunies. Le point de départ des investigations policières repose sur l'identification des adresses IP ayant accédé à de multiples reprises au site internet en question. Non seulement l'analyse porte sur un très grand nombre d'adresses IP, mais surtout, l'identification de la ou des personnes qui se dissimulent derrière ces adresses est ardue, voire en certains cas, impossible.

De nombreux obstacles techniques peuvent en effet entraver les recherches menées par les services de police. L'utilisation d'un proxy ou d'un VPN (*Virtual Private Network*) en fait partie. Ces programmes introduisent un intermédiaire dans la communication entre ordinateurs de manière à substituer l'adresse IP du programme à celle de l'internaute qui accède à Internet. Sa véritable adresse IP reste alors dissimulée de sorte qu'il ne peut être identifié. Les sites internet utilisent aujourd'hui des outils permettant d'identifier les adresses IP de proxy ou de VPN et de les bloquer, de manière à empêcher les attaques. Afin de contourner ces outils, les auteurs de cyberattaques privilégient les *botnets*, un réseau d'ordinateurs utilisés à l'insu de leur propriétaire, en vue de lancer des attaques. Ici encore, l'adresse IP qui pourrait être collectée par le site internet objet d'une telle menace ne permettra pas d'identifier la personne qui est réellement à l'origine de l'attaque.

Pour autant, la position adoptée par la Cour de justice de l'Union européenne et par la Cour de cassation ne doit pas surprendre. Elle correspond à une tendance aujourd'hui connue, qui consiste à interpréter largement la notion de donnée à caractère personnel, dans un souci de protection plus grand de la personne (en ce sens, V. not. Numérique et libertés : un nouvel âge démocratique, Rapport n° 3119, AN 9 oct. 2015, présenté par M. Christian Paul et M^me^ Christiane Féral-Schul, coprésidents).

II - LE RÉGIME DE LA DONNÉE À CARACTÈRE PERSONNEL APPLIQUÉ À L'ADRESSE IP

Qualifier l'adresse IP de donnée à caractère personnel a pour conséquence directe l'application du régime des données à caractère personnel à cette donnée. Ainsi la constitution d'un fichier comportant des adresses IP pourra être qualifié de traitement de donnée à caractère personnel et le responsable de traitement sera assujetti à toutes les obligations décrites dans la directive de 1995 et retranscrites dans la loi de 1978. La Cour de cassation, dans l'arrêt commenté a ainsi indiqué que le traitement de ces données devait faire l'objet d'une déclaration préalable auprès de la CNIL (A), tandis que la Cour de justice a pu préciser les conditions de licéité du traitement des adresses IP (B).

A - Le nécessaire respect des obligations déclaratives

Après avoir qualifié l'adresse IP de donnée à caractère personnel, la Cour de cassation dans l'arrêt commenté en a très logiquement inféré qu'un fichier d'adresses IP devait faire l'objet des formalités prévues à l'article 22 de la loi Informatique et Libertés et plus précisément, d'une déclaration auprès de la CNIL. En l'espèce, la rétractation de l'ordonnance prise sur le fondement de l'article 145 du code de procédure civile était en jeu puisqu'une personne identifiée par le biais de son adresse IP invoquait l'absence de déclaration auprès de la CNIL du fichier d'adresses IP et partant, soulevait l'illicéité de la mesure d'instruction obtenue sur ce fondement. La Cour de cassation qui admet implicitement l'illicéité du traitement de données en reconnaissant une obligation de déclaration de traitement, en l'occurrence inexécutée, a logiquement cassé l'arrêt d'appel qui avait rejeté la demande de rétractation.

À l'aune de cette décision, il convient de s'assurer, lorsque l'on forme une requête ayant pour objet de solliciter d'un fournisseur d'accès à internet l'identification d'une personne par le biais d'une adresse IP, que les principes de la loi de 1978 au regard de la collecte et du traitement de ces données ont été respectés et en particulier, les obligations déclaratives.

Cet arrêt n'est pas sans rappeler la décision prise par la chambre sociale de la Cour de cassation qui avait déclaré un licenciement sans cause réelle et sérieuse car la mesure avait été prise sur le fondement d'un système de surveillance de la messagerie électronique des salariés qui n'avait pas été déclaré à la CNIL (Soc. 8 oct. 2014, n° 13-14.991, D. 2014. 2055 ; *ibid.* 2015. 104, chron. E. Wurtz, F. Ducloz, S. Mariette, N. Sabotier et P. Flores ; *ibid.* 2016. 167, obs. J.-D. Bretzner et A. Aynès).

Le non-respect des principes de protection des données à caractère personnel peut donc engendrer la nullité de décisions fondées sur ces traitements. À travers cette décision, la Haute juridiction rappelle, s'il en était besoin, la nécessité de respecter les principes de la loi Informatique et Libertés.

À l'aune du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, qui entrera en vigueur le 25 mai 2018, il n'y aura plus de déclaration à faire auprès de la CNIL. Il conviendra néanmoins de respecter l'ensemble des autres principes de protection des données à caractère personnel et notamment celui du traitement licite des données, qui fait justement l'objet de précisions importantes dans l'arrêt de la Cour de justice.

B - Des précisions sur les conditions de licéité du traitement des adresses IP

L'application du régime des données à caractère personnel à une adresse IP engendre un certain nombre de questions. Les adresses IP collectées par un site internet le sont souvent dans un but précis, celui d'identifier les accès frauduleux et notamment d'empêcher les attaques en déni de service.

Dans ce contexte singulier de lutte contre la cybercriminalité, comment appliquer le principe de licéité dans la collecte et le traitement des données ? Peut-on notamment collecter les adresses IP sans le consentement de la personne concernée ?

La Cour de justice répond favorablement à cette question et considère que le traitement de telles données peut être licite sans le consentement de la personne intéressée, dès lors qu'« il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement [...] à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée [...] » (art. 7, f, de la dir. de 1995). Le recours à la notion d'intérêt légitime pour justifier un traitement de données suppose donc une pondération des intérêts en présence : d'une part, ceux du fournisseur de services en ligne et, d'autre part, ceux des utilisateurs de ces services.

En l'occurrence, l'intérêt légitime du responsable de traitement reposait sur la nécessité d'assurer la continuité du fonctionnement des sites et, partant, de prévenir les actes frauduleux. La décision de la Cour de justice qui fonde la licéité du traitement des adresses IP sur l'intérêt légitime du responsable de traitement est cohérente. Elle s'inscrit dans la droite ligne de la doctrine du G29 qui considère que le recours à la notion d'intérêt légitime est justifié dans un contexte de prévention de la fraude ou de sécurité des systèmes d'information (*Opinion 06/2014 on the notion of legitimate interest of the data controller under article 7 of Directive 95/46/EC adopted on 9 April 2014*, 844/14/EN WP 217, p. 25).

La qualification de données à caractère personnel appliquée à l'adresse IP emporte des effets conséquents. Si la Cour de cassation et la Cour de justice ont apporté des précisions à cet égard, il convient à présent, pour les responsables de traitement, de les mettre en œuvre afin d'éviter tout risque juridique.

| CONSEIL PRATIQUE

Dans l'attente de l'entrée en vigueur le 25 mai 2018 du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, qui supprime les formalités préalables, les traitements de données consistant en des adresses IP doivent faire l'objet d'une déclaration préalable auprès de la CNIL, sauf en cas de présence d'un Correspondant informatique et libertés (CIL), auquel cas le traitement devra simplement être ajouté à son registre.

Géraldine Péronne
Avocat à la Cour - Cabinet VIGO (le Cabinet VIGO est membre du réseau GESICA) - Docteur en droit

Emmanuel Daoud
Avocat à la Cour - Cabinet VIGO (le Cabinet VIGO est membre du réseau GESICA) - Membre du Conseil de l'Ordre