FABRICE MATTATIA

Traitement des données personnelles

Le guide juridique

La loi Informatique et libertés et la CNIL
Jurisprudences

EYROLLES

 ISBN : 978-2-212-13594-7

Chapitre 8

Débats et perspectives

Bien que l'on dispose de plus de 30 ans de jurisprudence de la CNIL et des tribunaux, de nombreux points constituent toujours des sujets de débat, et représentent une incertitude pour les responsables de traitement. Par exemple, le statut de l'adresse IP relativement à la loi Informatique et Libertés a fait l'objet de jugements des tribunaux et de prises de position de la CNIL souvent opposés. Le responsable souhaitant traiter des adresses IP doit donc accorder à ce point une attention particulière.

Pour lever ces ambiguïtés et permettre une protection des données personnelles plus homogène au niveau européen, la Commission européenne a lancé en 2012 un chantier de refonte de la directive de 1995. Un projet de règlement remplaçant la directive a été soumis à discussion publique, en attendant un débat au Parlement européen. Les règles de protection des données personnelles sont donc appelées à évoluer dans les années qui viennent.

Le statut des adresses IP

L'adresse IP (*Internet Protocol*) est le numéro, unique au monde, sous lequel un ordinateur est relié à Internet. Ce numéro permet de le reconnaître sur la toile et de s'y connecter. L'adresse IP contient une indication de la zone géographique de l'ordinateur : la première partie de cette adresse désigne le réseau, la seconde repère le client sur ce réseau. Sauf dans les cas particuliers des adresses IP fixes paramétrées une fois pour toutes dans l'ordinateur ou réservées par le réseau pour des postes donnés, il n'y a pas obligatoirement un lien immuable entre un ordinateur, même fixe, et une adresse IP. Le réseau peut changer l'adresse IP qu'il attribue à un de ses clients. Inversement, un même ordinateur portable peut se connecter sur plusieurs réseaux avec ou sans fil, sous des adresses différentes.

Mais comme le fournisseur d'accès garde la mémoire des adresses qu'il attribue, il est toujours possible, connaissant une adresse utilisée à un instant donné, de remonter à l'ordinateur qui l'utilisait et à son titulaire.

Sur Internet, la trace la plus répandue de l'identité de l'internaute réside ainsi dans l'adresse IP de son ordinateur. La capacité de relier, *via* une adresse IP, un historique de navigation à l'identité d'une personne permet de dresser le profil de cette dernière et de retracer ses activités, mettant ainsi en danger sa vie privée. Toutefois, l'adresse IP est celle d'une machine, non d'une personne. De nombreux débats ont donc eu lieu pour déterminer si l'adresse IP est une donnée personnelle.

Enjeu du statut de l'adresse IP

Cette question représente notamment un enjeu dans la lutte contre le téléchargement illégal et dans la protection des droits d'auteur. Elle conditionne, pour les sociétés propriétaires de droits, la possibilité de surveiller les téléchargements des internautes en les identifiant par leur adresse IP. Si l'adresse IP est une donnée à caractère personnel, alors sa surveillance sans autorisation est illégale.

En 2006-2007, plusieurs décisions contradictoires ont été rendues concernant la protection à accorder à l'adresse IP d'un internaute, selon que cette donnée est considérée ou non comme personnelle. Le statut exact de l'adresse IP vis-à-vis de la loi Informatique et Libertés a fait l'objet d'interprétations divergentes selon les commentateurs et les juridictions.

Jurisprudences contre le statut de données personnelles

Dans le cadre de deux procédures visant des échanges illégaux de fichiers musicaux, la cour d'appel de Paris devait examiner la validité de procès-verbaux dressés par des agents assermentés des sociétés de gestion de droits d'auteurs à l'aide de traitements informatisés non déclarés préalablement à la CNIL. Ces agents avaient relevé les adresses IP des contrevenants et avaient ensuite obtenu leurs noms des fournisseurs d'accès à Internet.

L'enjeu de la question posée à la cour était le suivant :

- Si l'adresse IP est une donnée à caractère personnel, alors les procédures en cause, dressées de manière viciée, sont entachées de nullité.
- Si l'adresse IP n'est pas une donnée à caractère personnel, les procédures sont bien valides.

La cour a estimé dans son arrêt du 27 avril 2007[1] que « l'adresse IP ne permet pas d'identifier le ou les personnes qui ont utilisé cet ordinateur, puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur d'accès l'identité de l'utilisateur. » Elle a précisé dans un arrêt du 15 mai 2007 consacré à une affaire similaire[2] que « cette série de chiffres en effet ne constitue en rien une donnée indirectement nominative relative à la personne dans la mesure où

1. CA Paris, 13e chambre, section B, 27 avril 2007.

2. CA Paris 13e chambre, section A, 15 mai 2007.

elle ne se rapporte qu'à une machine, et non à l'individu qui utilise l'ordinateur pour se livrer à la contrefaçon. » La cour en conclut que l'adresse IP ne constitue pas une donnée à caractère personnel et qu'en conséquence son traitement ne relève pas de la loi Informatique et Libertés. Elle a donc validé les procédures en cause.

Cette position semble pourtant contraire à la définition même des données à caractère personnel qui figure dans l'article 2 de la loi Informatique et Libertés. S'il est vrai que l'adresse IP ne se rapporte qu'à un ordinateur, elle permet toutefois de remonter à son utilisateur et donc d'identifier *indirectement* ce dernier lorsque celui-ci est seul à avoir accès à la machine, et ce en mettant en œuvre « l'ensemble des moyens » dont dispose « toute autre personne », en l'occurrence la police ou la gendarmerie.

Jurisprudences pour le statut de données personnelles

Prises de position

La CNIL s'est inquiétée publiquement de ces deux arrêts dans un communiqué en août 2007[3], en soulignant que « l'ensemble des autorités de protection des données des États membres de l'Union européenne a récemment rappelé, dans un avis du 20 juin 2007 relatif au concept de données à caractère personnel, que l'adresse IP attribuée à un internaute lors de ses communications constituait une donnée à caractère personnel. » La CNIL a demandé au Garde des Sceaux d'examiner la possibilité d'intenter un pourvoi en cassation contre cette jurisprudence, afin d'obtenir de la cour une réponse claire sur le statut de l'adresse IP, et a obtenu une réponse favorable du ministre. Toutefois ce recours n'a pas eu lieu, compte tenu d'un autre pourvoi en cassation formulé par une société de gestion de droits d'auteur contre un arrêt de la cour d'appel de Rennes dans une affaire similaire. Ce recours devait permettre à la Cour de cassation d'exprimer sa position.

Dans le même sens, le Conseil d'État avait pour sa part considéré en 2007 que les adresses IP étaient des « données nominatives »[4].

3. *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes*, *www.cnil.fr*, 2 août 2007.

4. Conseil d'État, 10e et 9e sous-sections réunies, n° 288149, 23 mai 2007.

Jurisprudences

D'autres juridictions ont suivi la position de la CNIL. Ainsi, pour le tribunal de grande instance de Bobigny[5], « au regard de cette définition posée par la loi, l'adresse IP constitue une donnée à caractère personnel en ce qu'elle permet d'identifier une personne en indiquant sans doute possible un ordinateur précis. Le numéro IP établit la correspondance entre l'identifiant attribué lors de la connexion à l'internaute et l'identité de l'abonné. »

De même, dans son jugement du 6 septembre 2007, le tribunal de grande instance de Saint-Brieuc a estimé que « l'adresse IP est, au sens strict, l'identifiant d'une machine lorsque celle-ci se connecte sur l'Internet et non d'une personne. Mais, au même titre qu'un numéro de téléphone

5. TGI Bobigny, 15e chambre, 14 décembre 2006.

n'est, au sens strict, que celui d'une ligne déterminée mais pour laquelle un abonnement a été souscrit par une personne déterminée, un numéro IP associé à un fournisseur d'accès correspond nécessairement à la connexion d'un ordinateur pour lequel une personne déterminée a souscrit un abonnement auprès de ce fournisseur d'accès. L'adresse IP de la connexion associée au fournisseur d'accès constituent un ensemble de moyens permettant de connaître le nom de l'utilisateur. En l'espèce il n'est pas contestable que les informations recueillies [...] constituaient des données à caractère personnelle [sic] ayant indirectement permis l'identification de Monsieur J.P. » Cette décision a fait l'objet d'un appel devant la cour de Rennes. Cette cour, sur deux autres dossiers, s'est prononcée dans le même sens : « L'adresse IP de l'internaute constitue une donnée indirectement nominative car, si elle ne permet pas par elle-même, d'identifier le propriétaire du poste informatique, ni l'internaute ayant utilisé le poste et mis les fichiers à disposition, elle acquiert ce caractère nominatif par le simple rapprochement avec la base des abonnés, détenue par le fournisseur d'accès à Internet. »[6] Bref, pour cette cour, « c'est de façon pertinente que les premiers juges ont relevé que l'adresse IP d'un internaute constituait une donnée à caractère personnel. »[7]

6. CA Rennes, 3e chambre, 22 mai 2008.

7. CA Rennes, 3e chambre, 23 juin 2008, dossier 07/01495, arrêt 08/868.

Dans l'attente d'une solution définitive

Pistes nationales

Un des arrêts rendus par la cour d'appel de Rennes a été cassé par la Cour de cassation en 2009[8]. Une décision sur le statut de l'adresse IP était attendue à cette occasion. Mais en l'espèce le litige concernait des relevés d'adresses IP effectués manuellement. La Cour a rappelé que la loi Informatique et Libertés « s'applique aux traitements *automatisés* de données à caractère personnel », pour décider qu'elle ne s'appliquait donc pas à la cause, puisque le traitement objet du litige était *manuel*. La Cour de cassation n'a ainsi pas utilisé cette occasion de préciser le statut de l'adresse IP, qui continue de faire l'objet d'appréciations divergentes de la part des tribunaux.

8. Cass. Crim., 13 janvier 2009, *www.legalis.net*, cassant l'arrêt CA Rennes du 22 mai 2008.

Une solution pourrait également intervenir par voie législative. Le débat parlementaire du printemps 2009 sur la loi Création et Internet (HADOPI), qui abordait le problème de la collecte des adresses IP, aurait pu constituer l'occasion de clarifier le statut de l'adresse IP et de mettre fin aux divergences entre juridictions, mais ce point n'a pas été abordé. Cette question a de nouveau été examinée en mars 2010, à l'occasion de la discussion en première lecture au Sénat de la proposition de loi des sénateurs Détraigne et Escoffier « visant à mieux garantir le droit à la vie privée à l'heure du numérique », mais le texte n'a finalement pas été adopté par l'Assemblée nationale. La question n'est donc pas tranchée.

Pistes européennes

Afin d'assurer de manière incontestable une protection de l'adresse IP en tant que donnée personnelle, certaines autorités ont souhaité obtenir une décision européenne sur ce sujet. Mais, comme le souligne le Contrôleur européen de la protection des données, une telle décision n'est pas nécessairement souhaitable. En effet, comme pour toute donnée, le caractère personnel ou non de l'adresse IP doit être évalué au cas par cas dans le cadre des définitions de la directive de 1995. Par ailleurs, créer un cadre juridique distinct pour ce type de donnée risquerait de faire perdre au droit son caractère d'universalité et de neutralité technologique[9].

Importance des circonstances

L'adresse IP doit-elle d'ailleurs bénéficier du même statut quelles que soient les circonstances ? Pour les imprimantes ou les proxys par exemple, qui disposent d'une adresse IP pour se connecter au réseau, le caractère « personnel » de cette adresse n'est pas envisageable. Il convient également de prendre en compte le fait que l'identification d'un utilisateur à partir d'une adresse IP n'est pas aussi automatique qu'on pourrait le croire, notamment en cas d'utilisateurs multiples comme dans le cas des cybercafés ou des ordinateurs en accès libre. Le même raisonnement pourrait s'appliquer à l'adresse IP : dans l'absolu, il est possible de considérer qu'une adresse IP n'est pas une donnée personnelle. Pour qu'elle le soit, il faut pouvoir démontrer que seule une personne donnée a pu utiliser l'ordinateur en question pour la connexion mettant en cause cette adresse IP. Soit cette personne est la seule à pouvoir utiliser l'ordinateur, soit celui-ci est partagé et dans ce cas un système sécurisé de comptes nominatifs permet de conserver en mémoire qui a fait quoi. Dans le cas contraire, faute de pouvoir assigner l'usage de l'ordinateur et donc de l'adresse IP à une personne déterminée, il peut sembler contestable d'assimiler l'adresse IP à une donnée personnelle.

Cette solution présente l'inconvénient d'être *a posteriori* : il faut avoir collecté l'adresse IP et enquêté sur l'ordinateur concerné pour savoir s'il y a ou non un utilisateur identifiable. On prend ainsi le risque de s'apercevoir après coup que l'on n'avait pas le droit de collecter cette adresse ! En pratique, comme on ne peut savoir *a priori* si une adresse IP est personnelle ou pas, l'application du principe de précaution oblige à la protéger dans tous les cas comme si elle était personnelle. Ce principe conduit à interdire tous traitement ou collecte de l'adresse IP non autorisés et réalisés sans le consentement des personnes concernées, position adoptée par le G29. Il considère que si l'adresse IP, même dynamique, d'un abonné *identifié* constitue « sans l'ombre d'un doute » une donnée personnelle, il n'en est pas toujours ainsi. « À noter toutefois le cas particulier de certains types d'adresses IP qui, dans certaines circonstances, ne permettent en fait pas

9. European Data Protection Supervisor, *EDPS Comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal service) & Directive 2002/58/EC (ePrivacy)*, 2 septembre 2008, § 3-16.

l'identification de l'utilisateur, et ce pour diverses raisons d'ordre technique et organisationnel. L'exemple des adresses IP attribuées à un ordinateur dans un café Internet illustre cette situation, puisque dans ce cas aucune identification des clients n'est requise. On pourrait faire valoir que les données collectées sur l'utilisation d'un ordinateur X pendant un certain laps de temps ne permettent pas l'identification de l'utilisateur à l'aide de moyens raisonnables et que celles-ci ne sont donc pas des données à caractère personnel. Toutefois, il convient de relever qu'il est très probable que les fournisseurs d'accès Internet ignorent si l'adresse IP en question permet ou non l'identification, et qu'ils traitent les données associées à cette IP de la même manière qu'ils traitent les informations associées aux adresses IP d'utilisateurs dûment enregistrés et identifiables. Ainsi, à moins que les fournisseurs d'accès internet soient en mesure de déterminer avec une certitude absolue que les données correspondent à des utilisateurs non identifiables, par mesure de sécurité, ils devront traiter toutes les informations IP comme des données à caractère personnel. »[10]

La passion suscitée par un tel débat technique, aussi bien chez les parlementaires que dans les médias, prouve que désormais sont largement appréhendés les enjeux de la protection des données personnelles face aux possibilités offertes par les nouvelles technologies. Le législateur, le gouvernement, la CNIL, les acteurs du numérique, ainsi que les utilisateurs se rejoignent dans une prise de conscience de la nécessité d'agir pour mieux protéger la vie privée et pour permettre une mise en œuvre satisfaisante des principes « Informatique et Libertés ».

10. Groupe de travail « Article 29 » sur la protection des données, *Avis 4/2007 sur le concept de données à caractère personnel*, 01248/07/FR, WP 136, 20 juin 2007, p. 18-19. Voir aussi Groupe de travail « Article 29 » sur la protection des données, *Le respect de la vie privée sur Internet - Une approche européenne intégrée sur la protection des données en ligne*, WP 37, 21 novembre 2000.

Le nouveau projet de règlement européen

La Commission européenne a constaté que la directive de 1995 a engendré, par transposition, 27 droits nationaux des données personnelles, dont la prise en compte constitue une charge pour les entreprises transeuropéennes qui doivent par exemple gérer 27 régimes de formalités différents. Elle souhaite donc remplacer cette directive (et celles qui l'ont complétée) par un règlement permettant une homogénéisation de la protection des données personnelles dans toute l'Union européenne. En effet, le règlement est directement applicable dans tous les États membres, sans nécessiter de transposition. Bien entendu, les tribunaux et les autorités de contrôle de chaque État pourront avoir chacun leur interprétation du règlement, mais le niveau de disparité devrait diminuer.

Nous présentons ci-dessous les grandes lignes du projet présenté en 2012 par la Commission. Des modifications importantes sont toutefois susceptibles d'affecter ce projet au cours de son processus d'adoption.

Renforcement des règles existantes

Le projet de règlement renforce l'exigence de consentement en demandant désormais un « consentement explicite », la charge de la preuve incombant au responsable de traitement.

Il étend l'obligation de notification des violations de sécurité, actuellement limitée aux seuls fournisseurs de services de communications électroniques, à tous les responsables de traitement. En cas de violation des données personnelles, l'autorité de contrôle et éventuellement les personnes concernées devront être averties sous 24 heures.

Il renforce également la protection des données de santé et rend dans certains cas obligatoire la désignation d'un CIL (pour le secteur public et pour un certain nombre d'entreprises).

Le projet de règlement renforce aussi le rôle du G29 qui regroupe les autorités nationales de protection.

Le montant maximum des sanctions des autorités de protection est porté à un million d'euros ou, pour les entreprises, 2 % du chiffre d'affaires mondial (contre 150 000 € actuellement pour la CNIL).

Catégories spéciales

Le projet de règlement crée de nouveaux concepts, comme la protection des données concernant les enfants.

Il précise les règles applicables pour les journalistes, les professionnels de santé, les employeurs, les statisticiens, les personnes soumises au secret professionnel ainsi que pour les traitements d'intérêt public.

Nouvelles formalités

Les formalités actuelles (déclarations, autorisations…) sont allégées. En revanche, le projet de règlement instaure pour le responsable une obligation de créer et de tenir à jour en interne toute la documentation concernant ses traitements, afin de permettre un contrôle effectif par les autorités de protection.

Pour alléger les obligations pesant sur les entreprises transeuropéennes, le projet de règlement confie à la seule autorité de protection du pays où l'entreprise a localisé son « établissement principal » la compétence sur tous les traitements opérés par cette entreprise dans l'UE.

À noter

Cette proposition est critiquée par de nombreuses autorités nationales, dont la CNIL, qui dénoncent le manque de fondement juridique de la notion d'établissement principal et craignent un détournement de cette mesure par les entreprises qui pourront implanter leur établissement principal dans les pays où les autorités sont les moins sévères.

Pour les transferts hors de l'Union, le projet de règlement accorde plus d'importance aux BCR (*Binding Corporate Rules*), règles internes au sein de l'entreprise destinataire qui garantissent une protection adéquate des données.

Nouvelles obligations

Le projet de règlement impose que l'information donnée aux personnes concernées soit claire et compréhensible.

Le responsable du traitement doit fournir aux personnes concernées des moyens simples, y compris électroniques, d'exercer leurs droits. Il doit répondre aux demandes de ces dernières dans un délai défini et doit motiver ses refus éventuels.

Le responsable de traitement doit pouvoir rendre compte de toutes les mesures prises (*accountability*) pour respecter la loi.

Les responsables de traitements établis hors de l'Union européenne, mais dont les traitements concernent les citoyens de l'UE, doivent désigner un représentant dans l'UE.

Nouvelles interdictions

Le projet de règlement interdit au responsable de traitement de remettre les données aux autorités judiciaires ou administratives d'un État hors de l'Union, même sur réquisition de celles-ci, sans y être autorisé par un accord international ou par les autorités de protection européennes. Le règlement s'oppose ainsi au *Patriot Act* américain qui permet au gouvernement des États-Unis d'accéder à toute donnée traitée par une entreprise américaine, même en-dehors de leur territoire.

Nouveaux droits

Le projet de règlement crée pour les personnes concernées un « droit à l'oubli », qui consiste à pouvoir obtenir l'effacement des données, de leurs copies et des liens Internet qui y mènent.

Autre création, un « droit à la portabilité », qui consiste à pouvoir récupérer ses données sous un format permettant le transfert vers un autre traitement de son choix.

Le droit d'opposition est complété par un droit à ne pas faire l'objet d'un profilage.

Enfin, les associations de défense des consommateurs pourront porter plainte au nom des personnes concernées.

Débat à suivre

Le processus d'adoption du projet de règlement n'en est qu'à ses débuts. Toutes les parties intéressées, aussi bien les autorités nationales de protection des données comme la CNIL que les associations de défense des consommateurs et celles représentant les professionnels du secteur, sans oublier bien sûr les entreprises gérant des données personnelles, ont réagi au projet de la Commission et proposé des amendements. Le texte sera présenté au Parlement européen pour discussion, et des évolutions majeures auront sans doute lieu.

La protection des données personnelles constitue l'un des défis les plus importants lancés à la société par les technologies numériques. Le grand public et les décideurs se sont emparés de la question. Aussi, nul doute que les années à venir ne soient jalonnées de débats multiples sur les mesures à adopter, les règles à instaurer, les comportements à faire évoluer… Désormais, il appartient à chacun d'entre nous d'être acteur de sa propre protection.