

Adresses IP et données personnelles : et si on se trompait de débat ?

La question du caractère personnel ou pas de l'adresse IP est complexe et contradictions. Alors que l'Hadopi va se servir de ces numéros Internet pour démasquer les pirates du Net, le débat n'est toujours pas tranché et pourrait devenir secondaire. Question d'analyse.

Par Winston Maxwell à Paris (photo) et Wim Nauwelaerts à Bruxelles, avocats, Hogan Lovells



L'un des plus grands débats juridiques actuels en matière du droit de l'Internet est de savoir si une adresse IP – ou « Internet Protocol », numéro d'identification de chaque ordinateur, mobile, voire objet, connectés aux réseaux des réseaux – est une donnée

personnelle au sens de la directive européenne de 1995 sur la protection des données à caractère personnel (1) et de la loi française sur l'informatique et les libertés. Si l'adresse IP est une donnée personnelle, cette directive et cette loi française s'appliquent. A l'inverse, si une adresse IP n'est pas une donnée personnelle, une grande partie des opérations de communication sur Internet échapperait à tout contrôle en matière de protection de données personnelles.

Dernière l'IP, pas toujours d'individu

Le système actuel est une approche binaire qui dépend de la réponse à une seule – mais redoutablement complexe – question, à savoir : la nature d'une adresse IP par rapport à la législation sur la protection des données personnelles. L'actualité apporte presque chaque mois de nouvelles décisions de justice qui rendent le débat encore plus difficile. Pourquoi est-ce que la question du « statut » de l'adresse IP est si complexe ? Parce que les adresses IP ont une multitude d'utilisations dans les réseaux et peuvent seulement dans certains cas conduire à l'identité d'un individu utilisant le réseau. Si on comparait les réseaux IP aux rues de Paris, les adresses IP serviraient à identifier chaque carrefour, chaque feu rouge, chaque lampadaire, chaque panneau de signalisation et enfin chaque voiture qui circule sur les voies. De plus, certaines adresses IP sont éphémères. A un moment donné, elles identifient une voiture circulant entre un carrefour A et un carrefour B, et l'instant d'après la même adresse IP identifie un lampadaire. Sur les réseaux de demain où les objets eux-mêmes deviendront communicants, une adresse IP pourra aussi bien identifier un paquet de café dans un magasin qu'un compteur électrique.

Est-ce qu'une adresse IP peut conduire à un individu ? Parfois oui. Tout comme une fibre de coton tombée sur une scène de crime et analysée par les équipes d'« experts », une adresse IP peut mener à une machine qui elle-même peut, parfois, fournir des indices sur la personne qui a été à l'origine d'une communication. Tout dépend du contexte et des moyens mis en œuvre. L'adresse IP est un indice qui peut dans certains cas conduire à un individu, dans d'autres cas pas.

On compte trois catégories d'adresses IP :

- 1 • Les adresses IP qui ne peuvent jamais conduire directement ou indirectement à un individu, quels que soient les moyens mis en œuvre.
- 2 • Les adresses IP qui peuvent fournir des indices indirects conduisant vers un individu, si l'on y met beaucoup de moyens (la catégorie des « experts »).
- 3 • Les adresses IP qui conduisent assez facilement à un abonnement nominatif. Même dans cette dernière catégorie, l'adresse IP permet seulement d'identifier le titulaire de l'abonnement d'accès, mais ne permet pas d'identifier l'individu qui a réellement utilisé un ordinateur à un instant « T ».

Les autorités de protection des données personnelles sont unanimes pour dire que les adresses IP de la troisième catégorie sont des données personnelles. Les tribunaux sont, quant à eux, partagés sur la question. Quant aux adresses IP de la seconde catégorie, le groupe de travail européen surnommé « Article 29 » – réunissant la Commission nationale de l'informatique et des libertés (Cnil) et ses homologues des Vingt-sept (2) – considère que les adresses IP sont des données nominatives si elles peuvent conduire à un individu en utilisant des moyens raisonnables (3). Personne ne sait exactement ce que signifie des « moyens raisonnables », d'où une grande insécurité juridique pour cette catégorie d'adresses IP. Quant à la première catégorie des adresses IP, celles qui ne peuvent jamais aboutir à un individu, elles ne sont jamais des données personnelles. Et pour cause.

Cas de EMI contre Eircom

Une adresse IP peut être considérée comme une donnée personnelle entre les mains d'une personne « X », mais pas entre les mains d'une personne « Y ». Par exemple, une adresse IP entre les mains d'un fournisseur d'accès à Internet (FAI) – qui dispose de moyens pour établir le lien entre l'adresse IP et

Notes

(1) - Directive européenne 95/46/CE du 24 octobre 1995.

(2) - Data Protection Working Party (« G29 »).

(3) - Groupe de travail « Article 29 » sur la protection des données, Avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, WP 136. Le critère exact est "l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne".

éventuellement un abonnement d'accès à Internet – serait considérée comme une donnée personnelle. Alors qu'une adresse IP entre les mains d'une tierce personne ne le serait pas, parce que cette tierce personne ne pourrait pas, en utilisant des moyens raisonnables, retrouver le lien entre l'adresse IP et un abonnement. Cette approche est illustrée par une décision du 16 avril dernier de la « High Court » d'Irlande (4), dans une affaire impliquant la maison de disques EMI et l'opérateur de télécommunications Eircom. Dans cette affaire, EMI a intenté une action contre Eircom en responsabilité parce qu'Eircom n'avait pas mis en œuvre les moyens raisonnables pour limiter les téléchargements illicites sur son réseau. L'affaire n'est pas allée jusqu'à son terme car les parties ont transigé : Eircom s'est engagé à mettre en place un système de réponse graduée sur une base contractuelle avec ses abonnés. Eircom va s'appuyer sur des adresses IP communiquées par EMI et d'autres labels de disques. L'autorité de protection des données personnelles d'Irlande a saisi la Haute cour pour décider si le protocole transactionnel entre Eircom et EMI violait les dispositions de la loi sur la protection des données personnelles en Irlande. Au départ, la cour devait décider si les adresses IP constituaient des données personnelles. Et là, la cour a décidé que ces mêmes adresses n'étaient pas des données personnelles entre les mains d'EMI mais qu'elles l'étaient entre les mains d'Eircom. Elle a estimé que EMI n'avait ni les moyens ni la motivation pour trouver l'identité de la personne correspondant à l'adresse IP en cause. Cette approche a été utilisée également par la Cour d'appel de Paris (5) qui a décidé, le 1^{er} février 2010, que les adresses IP collectées par la Sacem n'étaient pas des données personnelles. Les autorités de protection des données personnelles ne sont pas d'accord avec cette approche (6).

Google : « résultats insatisfaisants »

Le groupe « Article 29 » vient d'écrire à Google une lettre datée du 26 mai dernier et signée de son président Jacob Kohnstamm (7) pour se plaindre des pratiques du géant du Net en matière de rétention des données concernant les résultats de recherches. Google estime avoir rendu les données anonymes, conformément à la directive européenne de 1995 sur la protection des données à caractère personnel, en effaçant le dernier octet de chaque adresse IP. Selon le groupe des « Cnil » européennes, cette anonymisation est insuffisante, car il serait toujours possible dans certaines circonstances de retrouver l'identité d'une personne à travers ces adresses IP partielles. On est en plein dans la catégorie dite des « experts » ! Ces décisions démontrent à quel point le débat sur les adresses IP est complexe et semé de contradictions.

Et pourtant toute l'application de la directive européenne et de la loi française sur la protection des données personnelles dépend de cette analyse ! Cela conduit à des résultats insatisfaisants. Premièrement, il reste forcément une grande incertitude pour les acteurs économiques sur l'applicabilité ou non de la loi. Deuxièmement, la loi sur la protection des données personnelles s'appliquera à des cas qui ne posent aucun risque pour la vie privée des citoyens, et inversement ne s'appliquera pas à certains cas qui soulèvent un risque réel. Cette deuxième éventualité a notamment été soulevée dans un document du Contrôleur européen des données personnelles (8) sur les RFID (Radio Frequency Identification).

Le « Privacy by Design »

Les systèmes des RFID identifient des objets qui, dans certains cas, ne peuvent pas objectivement conduire à un individu. Donc, ce ne sont pas des données personnelles. Dans ce cas précis, le Contrôleur européen des données personnelles recommande de ne pas s'arrêter uniquement sur la question « *Est-ce une donnée nominative ?* » mais plutôt de regarder l'impact global du système mis en œuvre et de concevoir le système de manière à incorporer des garanties pour les citoyens. Il s'agit de l'approche « *Privacy by Design* » conseillé depuis longtemps par les autorités canadiennes. Le « Privacy by Design » comprend plusieurs étapes. D'abord, au moment de la conception d'un nouveau système, le concepteur du système effectuerait une étude d'impact qui identifierait les risques potentiels pour la vie privée et des mesures qui pourraient être prises pour réduire ces risques. Le concepteur du système mettrait en œuvre les mesures préconisées dans le rapport. Ensuite dans la mise en œuvre du système, des mesures de gouvernance pourraient être prises afin, là encore, de réduire les risques identifiés lors de l'étude d'impact. Par exemple, si les données utilisées pour identifier un utilisateur sont codées, la clé permettant de déchiffrer ce code serait détenue par une entité structurellement séparée de l'entité qui exploite les données codées. Enfin, avec l'évolution de la technologie et des menaces qui pèsent sur la sécurité, l'exploitant du système aurait le devoir de mettre à jour les mesures de protection.

La Commission européenne et le Contrôleur européen des données personnelles préconisent une approche de ce type à l'égard des systèmes de RFID, ainsi que pour les systèmes de transport intelligent. L'analyse se concentre en premier lieu sur les risques éventuels pour la vie privée et les mesures qui peuvent être prises pour réduire ce risque. La question de savoir si une adresse IP est ou non une donnée personnelle deviendrait secondaire. @

Notes

(4) - EMI Records v. EIRCOM, 2010 IEHC 108, 2008 1601 P, 16 avril 2010.

(5) - Cour d'appel de Paris, 12^e chambre, pôle 5, arrêt du 1^{er} février 2010, Cyrille S. / SACEM, Sdrm. Voir également Cour de Cassation, Chambre criminelle, arrêt du 13 janvier 2009, Sacem et autres / Cyrille S.

(6) - Voir notamment l'article de la CNIL du 2 août 2007 « *L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes* ».

(7) - Le président du « G29 » Jacob Kohnstamm a également adressé le 26 mai 2010 une lettre similaire à chacun des dirigeants de Microsoft et Yahoo.

(8) - Opinion du « European Data Protection Supervisor » sur la communication de la Commission européenne au Parlement et Conseil européens intitulée « *Radio Frequency Identification (RFID) in Europe* », COM(2007) 96, p.C101/3