PM/SGAE/SEC 11.07.2017

NOTE DE COMMISSION

COMMISSION DES LIBERTES CIVILES DE LA JUSTICE ET DES AFFAIRES INTÉRIEURES (LIBE)

Objet : Position des autorités françaises sur le projet de rapport relatif à la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »).
Réf. : 2017/0003(COD)
Rapporteur : Marju LAURISTIN (S&D, Estonie)

Les autorités françaises précisent que la présente note se concentre sur les amendements du projet de rapport relevant des aspects pénaux des enjeux de sécurité, sans préjudice de la position française sur les autres dispositions du projet de texte et de commentaires ultérieurs sur ces mêmes aspects pénaux.

- Sur l'amendement 2 :

Cet amendement prévoit de modifier le considérant 2 du texte en gommant la distinction opérée entre les données de contenu et les métadonnées s'agissant du régime de protection prévu. Les autorités françaises souhaitent rappeler que la distinction des régimes juridiques, au plan européen et au plan interne, entre les données de souscriptions, les métadonnées et les données de contenu correspond à une réelle différence dans les risques d'atteintes à la vie privée des personnes concernées. Les législations nationales en la matière se sont construites sur cette distinction. Une telle remise en cause de cette « hiérarchie » fragiliserait ces législations et brouillerait le message porté par le législateur en termes de protection des données personnelles.

Les autorités françaises émettent donc un **avis défavorable** à l'amendement 2.

- Sur l'amendement 6 :

Les autorités françaises émettent un **avis défavorable** à la suppression du considérant 7 qui ne faisait que rappeler la compétence partagée entre l'Union et les États membres sur ces questions et préciser l'articulation entre ces législations le cas échéant.

- Sur l'amendement 19 :

Les autorités françaises émettent un **avis défavorable** à la suppression de la phrase précisant dans quel cadre une interférence avec le contenu des communications électroniques peut être autorisée, celle-ci permettant de clarifier le texte.

- Sur l'amendement 27 :

L'amendement proposé au considérant 26 semble problématique en ce sens qu'il exclut du champ du projet de règlement les règles relatives aux conditions dans lesquelles le droit de l'Union ou le droit des États membres pourront restreindre certaines des obligations prévues. L'amendement restreint de manière très significative le champ de ces restrictions aux situations dans lesquelles une personne est déjà soupçonnée d'avoir commis une infraction pénale. Cette restriction pose difficulté à plusieurs égards : il peut être justifié et proportionné de prévoir un accès aux métadonnées dans d'autres cadres que la sphère pénale. De surcroît, ces métadonnées peuvent être indispensables

dans d'autres situations que celles évoquées par le projet de rapport, par exemple dans le cas d'une disparition inquiétante d'un mineur, sans qu'une personne soit nécessairement soupçonnée d'avoir commis une infraction pénale.

La solution pourrait être d'écrire que le règlement « pourra prévoir » cette possibilité, plutôt que la rédaction proposée par la Commission et de maintenir le reste du considérant inchangé.

- Sur l'amendement 73 :

Les autorités françaises ne voient aucune raison de supprimer à l'article 7 la possibilité pour les opérateurs de communication électroniques d'anonymiser les données. L'anonymisation présente toutes les garanties nécessaires en termes de protection des données et a toujours été considérée comme l'un des corollaires possibles du principe de confidentialité.

- Sur les amendements 101, 102 et 103 :

Les autorités françaises émettent un **avis défavorable** aux amendements 101, 102 et 103 proposés dans le projet de rapport et soutiennent, à ce stade de leurs réflexions sur la conservation des données, le texte présenté par la Commission.

D'une part, l'institution de régimes différents pour l'article 5 et pour les articles 6, 7 et 8 pose un problème de cohérence juridique. En effet, l'article 7 est le corollaire de l'article 5 et dès lors il n'est pas compréhensible de prévoir des règles distinctes et séparées les concernant.

D'autre part, ce texte est un règlement et sera donc d'applicabilité directe. La distinction proposée, en introduisant une nuance inutile, rend moins lisible et compréhensible le texte aux yeux de praticiens.

Enfin, le projet de rapport propose de limiter le champ des objectifs d'intérêt général permettant de justifier de telles dérogations en retirant de la liste les intérêts économiques et financiers de l'Union ou d'un État membre. Cette limitation pose difficulté à plusieurs égards. En premier lieu, et alors qu'il s'agit d'aligner le texte « e-privacy » sur le règlement général sur la protection des données, cette exclusion ne semble pas justifiée. En second lieu, cette restriction pourrait avoir pour conséquence de contraindre les autorités nationales compétentes à « judiciariser » toutes les fraudes constatées afin de pouvoir accéder à certaines données, au risque d'asphyxier les autorités judiciaires et alors qu'il existe dans plusieurs États membres des autorités administratives compétentes pour lutter contre certains comportements frauduleux.

- Sur l'amendement 116 :

L'amendement 116 prévoit que *« Les fournisseurs de services de communication électronique assurent une protection satisfaisante contre l'accès non autorisé aux données de communications électroniques ou l'altération de celles-ci, et veillent à ce que la confidentialité et la sécurité de la transmission soient également garanties par la nature des moyens de transmission utilisés ou par le recours aux techniques de pointe en matière de chiffrement de bout en bout de ces données .*

En outre, en cas de chiffrement des données de communications électroniques, le recours, au regard de ces communications, au déchiffrement, à la rétro-ingénierie ou à la surveillance est proscrit. Les États membres n'imposent aux fournisseurs de services de communication électronique aucune obligation qui aboutirait à un affaiblissement de la sécurité et du chiffrement de leurs réseaux ou services ».

Par cet amendement, le projet de rapport souhaite garantir un niveau élevé de confidentialité et d'intégrité des communications électroniques en proposant d'une part que les fournisseurs de services recourent aux techniques de pointe en matière de chiffrement de bout en bout, et en interdisant d'autre part le recours au déchiffrement, à la rétro-ingénierie ou à la surveillance. Les

États membres n'auraient désormais plus la possibilité de prévoir des obligations qui aboutiraient à un affaiblissement de la sécurité et du chiffrement des réseaux ou services.

Si les autorités françaises ont rappelé à de nombreuses reprises l'utilité des technologies de chiffrement, qui sont indispensables dans le domaine économique ou pour la sécurité des communications sensibles, elles ont également souligné la nécessité de prévoir une possibilité d'accès aux communications et aux métadonnées dans le cadre d'enquêtes pénales. En effet, de nombreuses affaires ont montré l'utilisation de moyens de communication cryptés par les personnes identifiées en tant que criminels, et notamment pour celles suspectées de faits de terrorisme. Ces applications, peu onéreuses et simples d'utilisation (*Telegram* en particulier) sont parfaitement maîtrisées par la mouvance djihadiste et participent directement à la structuration des groupes terroristes. Or, le chiffrement des communications électroniques rend inefficace les interceptions de données échangées entre suspects sur les réseaux de télécommunications.

Aussi, la proposition d'amendement 116 appelle les observations suivantes :

1) Les implications du recours à la technique de chiffrement de bout en bout

D'après le Commissariat français aux communications électroniques de défense, avec l'utilisation de la technique de chiffrement de bout en bout (chiffrement par les terminaux) qui devrait être la seule envisageable avec l'adoption de cet amendement, les suspects dont les communications électroniques seraient interceptées ne pourraient ignorer qu'ils sont sous surveillance.

En effet, le chiffrement de bout en bout (*end-to-end encryption*) implique pour le décryptage des données la mise en place systématique au sein des réseaux de la technique dite du *« Man in the Middle Attack »* ou *« de l'homme du milieu »* de façon à récupérer les clés et éléments associés. Cette technique induit que les clés ne sont pas échangées par les deux terminaux et sont modifiées par l'équipement *Man in the Middle Attack*. Pour s'en apercevoir, il suffit de comparer les clés de chiffrement du terminal d'une cible et de celui de son correspondant. Or, les réseaux de criminalité organisée ou certaines organisations terroristes ont les moyens de détecter ou former leurs membres à la détection des attaques dites *« Man In the Middle »*.

La proposition de règlement initiale, telle que présentée par la Commission européenne, ne comprend pas cette proposition de chiffrement de bout en bout[1] .

Cet amendement, s'il était adopté, conduirait à limiter les possibilités de recueillir des indices numériques pertinents pour les enquêtes dans la mesure où les suspects auraient connaissance du fait qu'ils sont placés sous surveillance. Or, il est fondamental de ne pas priver les services enquêteurs et les autorités judiciaires de cette possibilité d'accéder à des données utiles à la caractérisation d'infractions pénales.

2) Interdiction des mesures de surveillance et de déchiffrement y compris dans un cadre pénal

Le projet de rapport souhaite interdire toutes les méthodes permettant de contourner le chiffrement : le déchiffrement, la rétro-ingénierie ou la surveillance. Le projet de rapport souhaite également que les États membres ne puissent pas prévoir des obligations qui aboutiraient à un affaiblissement de la sécurité et du chiffrement des réseaux ou services.

Or, si l'article 11 du projet de règlement prévoit que les États membres peuvent édicter des règles nationales venant limiter les droits et obligations en matière de confidentialité des communications, de traitement des métadonnées et des données stockées sur les équipements terminaux, notamment à des fins de prévention et de détection d'infractions pénales graves, cet article ne vise pas l'article 17. Il n'y aurait donc pas d'exception prévue au principe du chiffrement des communications, quel que soit le motif.

[1] cf texte: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52017PC0010)

Conclusion:

En définitive, la combinaison de l'obligation de recours au chiffrement de bout en bout des communications électroniques et de l'impossibilité pour les autorités compétentes en matière pénale de pouvoir déroger à l'interdiction des méthodes de contournement aurait pour effet de paralyser les enquêtes pénales en interdisant l'accès à la preuve numérique.

En conséquence, il apparait pertinent de solliciter le rejet de cet amendement, et les autorités françaises émettent donc un **avis défavorable** à son sujet.

CONTACTS AUPRÈS DES AUTORITÉS FRANÇAISES

Secrétariat général des affaires européennes
M. Cyrille BAUMGARTNER, cyrille.baumgartner@sgae.gouv.fr

Représentation permanente de la France auprès de l'Union européenne
M. Jean MAFART, jean.mafart@diplomatie.gouv.fr