L' « Affaire SWIFT » :

Yves Poullet
Professeur ordinaire aux facultés de droit de Namur et de Liège
Directeur du CRID des FUNDP

Elise Degrave
Assistante à la Faculté de droit de Namur
Chercheuse au CRID des FUNDP

1. Le 27 septembre 2006[1], la Commission belge de protection de la vie privée publiait un avis « courageux » relatif à ce qu'il est maintenant convenu d'appeler l' « Affaire SWIFT ». Elle affirmait que SWIFT avait commis une « *violation cachée, systématique, massive et à long terme des principes européens fondamentaux en ce qui concerne la protection des données* ». Le 22 novembre 2006, le groupe de l'article 29 émettait son opinion[2], dans un style quelque peu différent[3]. On ajoute que, par une résolution du 6 juillet 2006[4], le Parlement européen lui-même s'était ému du comportement de cette société coopérative bien connue chez nous.

Notre propos se limite à deux types de réflexions : les premières portent sur le fond des critiques adressées à SWIFT ; les secondes émettent quelques doutes sur la procédure suivie par la Commission belge de protection de la vie privée dans l'affaire qui nous occupe.

La question de fond

2. SWIFT opère un service de messagerie financière dont les qualités de sécurité expliquent le succès croissant auprès de milliers d'institutions financières et bancaires réparties dans le monde. Elle transporte des plis soigneusement fermés dont elle ne connaît que les institutions financières émettrices et réceptrices. L'infrastructure qu'elle utilise est mondiale mais s'appuie sur deux centres serveurs, l'un situé en Europe et l'autre aux Etats-Unis. La dimension internationale de ce réseau, comme celui de la plupart des réseaux de communication d'envergure[5], explique cette double localisation nécessaire à la sécurité des transmissions.

L'après 11 septembre 2001 a vu, au pays de l'Oncle Sam - champion des libertés et des droits de l'homme- une multiplication de lois sécuritaires justifiées par la lutte anti-terroriste. Ainsi, notamment le Patriot Act permet l'interception des messages transitant sur le sol américain tant

[1] Avis n° 37/2006 du 27 septembre 2006, disponible sur le site de la Commission : http://www.privacycommission.be

[2] Opinion 10/2006 on the processing of personal data by SWIFT, WP 128 disponible sur le site : http://ec.europa.eu/justice.home/fsi/privacy/index.en.htm . A noter que dès le 26 septembre, le Groupe de l'article 29 publiait un communiqué de presse sur l'affaire SWIFT (Doc. 01608/06/FR)

[3] Nous reviendrons infra n° 8 in fine sur cette différence de style qui n'est pas sans portée.

[4] Résolution du parlement européen sur l'interception des données de transfert bancaires du système SWIFT par les services secrets américains (P6_TA-PROV(2006)0317). A noter également le hearing organisé le 4 octobre 2006 par les Comités « Libertés civiles » et « Affaires économiques et monétaires » et dont les échanges sont repris sur le site du Parlement européen à l'adresse suivante : http://www.europarl.europa.eu/news/expert/infopress_page/017-11292-275-10-40-902-200610021PR11291-02-10-2006-2006-false/default_en.htm

[5] Ainsi le réseau Internet repose sur treize « root servers », dont onze sont établis aux Etats-Unis. Que dire de nos réseaux à l'architecture maillée qui, pour acheminer un message à un destinataire même distant de quelques dizaine de kilomètres, emprunte bien souvent le détour outre-Atlantique du transport des messages

sur base de décisions judiciaires que sur décision des services secrets[6]. C'est dans le cadre d'une de ces législations que dès 2002, l'administration américaine enjoignait à SWIFT l'accès à certaines données transitant par les Etats-Unis. SWIFT affirme ne pas avoir caché cet état de fait aux autorités européennes. N'a-t-il pas crié assez fort ? Nous l'ignorons mais ce qui est certain c'est que son cri, en toute hypothèse, eût de toute façon été mal entendu dans la mesure où le malheur de nos alliés américains justifiait que nos pays leur emboitent alors le pas dans leur lutte sans merci contre le diable.

3. SWIFT livré à lui-même négocie alors avec l'administration américaine quelques garanties pour empêcher des atteintes trop flagrantes à ce que l'Europe consacre, depuis l'adoption de la Charte européenne des droits de l'Homme en même temps que le Traité de Nice en 2000, comme un droit de l'homme à part entière : la protection des données à caractère personnel. Jugera-t-on ces garanties insuffisantes ? C'est en tout cas ce qu'estime notre « courageuse » Commission. Sans doute, m'est-il permis d'en douter au moment où s'achève le second round de négociations entre les Etats-Unis et l'Europe à propos de l'obligation des compagnies aériennes de transférer pas moins de trente données relatives aux passagers transportés et ce pour une durée excessive et des destinataires mal précisés[7] ? Triste résultat unanimement dénoncé par le Parlement européen mais qui traduit bien la faiblesse dans la réalité de notre proclamation solennelle et quasi constitutionnelle en faveur de la protection des données à caractère personnel lorsque sont avancés par le grand frère américain les impératifs de sécurité. La conviction d'un écart entre discours et réalité s'accroît quand on rappelle que rien n'a été fait depuis que le 5 septembre 2001, le Parlement européen votait à une large majorité une résolution enjoignant aux autorités européennes de mettre fin aux pratiques d'espionnage et d'écoute des communications satellites opérées conjointement par les services secrets notamment des Etats-Unis et du Royaume-Uni dans le cadre du fameux réseau ECHELON[8]. Le cauchemar du 11 septembre, six jours après, suffit-il à expliquer l'amnésie depuis persistante de la part de nos autorités européennes[9] ?

---

[6] 107th Congress, 24th October 2001. Sur cette mesure et d'autres, lire O. KERR "Internet Surveillance Law After the USA PATRIOT Act: the Big Brother that isn't", The George Washington University Law School, Public Law and Legal Theory Working Paper No. 043, available at: http://ssrn.com/abstract=317501).
On ajoute que dans le cadre de certaines de ces législations, les Etats-Unis n'ont pas hésité à imposer des obligations à des entreprises localisés en dehors de leur territoire : la saga des transferts des données passagers par les compagnies américaines désirant atterrir aux Etats-Unis aux douanes américaines en est un autre exemple récent.

[7] Sur la décision 2006/729/PESC/JAI du Conseil du 16 octobre 2006 relative à la signature d'un accord entre l'Union européenne et els Etats-Unis d'Amérique sur le traitement et le transfert de données contenues dans les dossiers des passagers (« données PNR ») par des transporteurs aériens au ministère américain de la sécurité intérieure (J.O.C.E., 27.10.06, L298/27), lire l'opinion très critique du groupe de l'article 29 : « Opinion 9/2006 on the implementation of Directive 2004/82/EC of the Council on the obligation of carriers to communicate advance passenger data », WP 127 disponible sur le site du Groupe de l'article 29, cité supra, note 3

[8] Résolution du Parlement européen, 5 septembre 2001. Cette résolution a été prise sur base du rapport du député SCHMID en date du 18 mai 2005 (Report *on the existence of a global system for the interception of private and commercial communications (Echelon interception system), rapport presenté au Comité temporaire sur les ystème d'interception Echelon, comité mis en palce par le Parlement européen.*. Sur le système de surveillance Echelon, lire D.YERNAULT, "De la fiction à la réalité: le programme d'espionnage électronique global "Echelon" et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'Homme", *Rev. b. dr. Intern.,* 2000, p. 134 et s...

[9] Cf. toutefois les positions répétées du groupe de l'article 29 et plus récemment du Contrôleur européen à la protection des données. Ainsi dans son avis 10/2001 du 14 décembre 2001 sur une approche équilibrée dans la lutte contre le terrorisme, le groupe de travail de l'article 29 écrit à propos des mesures de lutte contre le terrorisme : « *Le groupe souligne également l'obligation de respecter le principe de proportionnalité concernant toute mesure restreignant le droit fondamental au respect de la vie privée selon l'article 8 de la Convention européenne des droits de l'homme et la jurisprudence s'y rapportant. Cela implique, entre autres, l'obligation de démontrer que toute mesure prise correspond à un "besoin social impératif". Les mesures qui sont simplement "utiles" ou "souhaitées" peuvent ne pas restreindre les libertés et droits fondamentaux. Le groupe de travail souligne donc la nécessité d'organiser un débat approfondi sur les actions de lutte contre le*

4. Notre propos n'est pas d'excuser une entreprise qui a laissé s'envoler ce que d'aucuns considéreront comme le bien le plus précieux : nos secrets de correspondance financière mais de mettre en garde contre cette attitude facile de certaines personnes apparemment vertueuses et chantres de la Privacy, qui les amène à crier « Haro sur le baudet ». L' « Affaire SWIFT » invite à dresser un procès plus essentiel que celui d'une entreprise, eût-elle la puissance de cette multinationale. Ce débat, c'est celui des limites que les droits de l'homme devraient assigner à l'action de l'Etat qui fut le premier à les reconnaître : les Etats-Unis. La question n'est pas de savoir si SWIFT avait ou non raison d'agir comme elle l'a fait. Il s'agit de déterminer s'il est normal et légitime que les services secrets américains, les juridictions américaines puissent aussi facilement lever le secret des correspondances et ce au nom de la lutte contre Al Qaida et autres suppôts de Satan[10].

La Commission belge élude ce débat. Nous estimons que ce débat était essentiel à l'heure où il faut bien constater que l'Europe ne s'est dotée d'aucune réglementation de protection des données dans les questions qui sont à l'origine même de l' « Affaire SWIFT », à savoir les questions d'investigations policières ou judiciaires dans les affaires pénales et celles mettant en jeu les services secrets et de sécurité nationale, questions relavant des « deuxième » et « troisième » piliers[11]. Sans doute, voit-on poindre une première tentative de réglementer la protection des données également dans ces secteurs avec le projet de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Toutefois, le parcours est encore long et le texte minimaliste actuel reste contesté par certains pays conquis par la logique sécuritaire[12] !

5. Faut-il reprocher à une entreprise de ne pas avoir pris des mesures là où l'Europe s'est jusqu'à présent tue et de n'avoir pas résisté aux ordonnances américaines qui s'appliquaient à elle ? La dimension internationale de nos réseaux, que nulle frontière n'arrête, ne laisse plus de choix à nos pays européens. Elle exige que l'Europe se dote d'un pouvoir d'agir politiquement et juridiquement vis-à-vis de pays tiers moins respectueux de la protection des données à caractère personnel. L'enjeu du débat est assurément politique. Au-delà, ce qui est en jeu au travers du

---

terrorisme, en analysant toutes leurs conséquences sur les libertés et droits fondamentaux des personnes et en refusant notamment l'amalgame entre la lutte contre le terrorisme réel et la lutte contre la criminalité en général, et en limitant également les mesures procédurales empiétant sur la vie privée à celles qui sont absolument nécessaires.
De plus, le groupe de travail rappelle que les mesures législatives limitant le droit des personnes au respect de la vie privée doivent être accessibles et prévisibles quant à leurs implications pour les personnes concernées. Cette exigence implique une législation suffisamment claire dans ses définitions des circonstances, de l'étendue et des modalités d'exercice des mesures d'intrusion. Les dispositions doivent être claires et détailler les circonstances dans lesquelles les pouvoirs publics sont autorisés à prendre des mesures limitant les droits fondamentaux. Elles devraient notamment spécifier où ces mesures peuvent être utilisées et devraient exclure toute surveillance générale ou préliminaire et offrir une protection contre les attaques arbitraires des pouvoirs publics. ».

[10] La Résolution du Parlement européen citée supra en note 4 est intéressante à cet égard dans la mesure où, au-delà du cas SWIFT, elle se dit gravement préoccupée par la création d'un climat marqué par une détérioration du respect de la vie privée et de la protection des données due à la récente législation américaine.

[11] Sur ce point, lire : F. DUMORTIER et Y. POULLET, « La protection des données à caractère personnel dans le cadre de la construction en piliers de l'Union Européenne », Actes du 1er colloque international organisé par l'APCAD, Barcelone, Novembre 2006, à paraître.

[12] Proposition de décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, disponible à http://www.libertysecurity.org/IMG/pdf/COM_2005_475_final.pdf

dialogue US-EU, c'est d'offrir une réponse à l'appel lancé par le récent sommet de Tunis sur la Société de l'Information, en novembre 2005[13] :

« *Nous exhortons toutes les parties prenantes à garantir le respect de la vie privée et la protection des informations et données à caractère personnel, et ce par différents moyens : adoption de législations, mise en œuvre de cadres de coopération, élaboration de bonnes pratiques et mise au point de mesures techniques et d'autoréglementation par les entreprises et les utilisateurs. Nous encourageons toutes les parties prenantes, en particulier les Etats, à réaffirmer le droit des personnes à accéder à l'information conformément à la Déclaration de principes de Genève et à d'autres instruments internationaux arrêtés d'un commun accord, ainsi qu'à coordonner leur action au niveau international en tant que de besoin* ».

Les questions de procédure

6. Au-delà du débat qu'il suscite sur le fond, l'avis de la Commission soulève des questions de compétence et de procédure.

Face à une situation où le respect des principes fondamentaux de la vie privée semble menacé, la loi sur la protection de la vie privée offre à la Commission plusieurs possibilités d'intervention. Parmi celles-ci figure le pouvoir de rendre un avis, conformément à l'article 29 ou à l'article 31 de la loi.

Les procédures prévues par ces deux dispositions ne se confondent point. Pourtant, il n'apparaît pas clairement à la lecture de l'avis du 27 septembre 2006 (ci-après, l'avis « Swift »), que celui-ci procède de l'une ou de l'autre procédure, ni que l'avis respecte toutes les exigences prescrites par l'une de ces procédures.

7. *L'article 29* autorise la Commission à prononcer un avis « *sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi (…)* »[14]. Elle peut le faire d'initiative ou à la demande des autorités législatives ou exécutives fédérales, communautaires et régionales ainsi qu'à la demande de la COCOM ou d'un comité de surveillance.

En l'espèce, la Commission se réfère à l'article 29 de la loi sur la protection de la vie privée et précise qu'elle a reçu une demande d'avis du Collège du renseignement et de la sécurité. Pourtant, cet organe est une autorité administrative qui n'est pas visée par la liste limitative de l'article 29. Sa demande ne permettait donc pas à la Commission d'enclencher une telle procédure.

Il reste que la Commission pouvait, légalement, agir d'initiative. Mais, dans cette hypothèse, la formulation de l'avis pose question au regard du but assigné à cette compétence. En effet, les avis doivent trouver leur raison d'être dans l'éclairage qu'ils apportent aux questions concernant la protection de la vie privée. Il s'agit donc, pour la Commission, d'intervenir dans le but d'aider à la compréhension de la loi et non de démontrer la responsabilité d'une entreprise, ou, plus largement, d'un responsable de traitement particulier. En d'autres termes, son rôle doit s'apparenter à celui d'un organe consultatif, et non à celui d'une juridiction. A cet égard, l'avis en

[13] Le Sommet Mondial de la Société de l'Information (SMSI) s'est tenu en deux phases : la première à Genève du 10 au 12 décembre 2003 ; la seconde, à Tunis, du 16 au 18 novembre 2005. Sur ces deux sommets et les documents auxquels ils ont abouti, en particulier l'agenda de Tunis, voir le site de l' Union Internationale des Télécommunications: http://www.itu.int/wsis

[14] Article 29, §1, de la loi.

question ne répond pas aux caractéristiques d'une opinion émise par une autorité aux compétences consultatives.

8. En d'autres termes, on pouvait attendre de la Commission qu'elle adopte une attitude neutre dans cette affaire. Cela supposait qu'elle refuse de prendre parti « dans des affrontements qui se déroulent sur la place publique »[15]. C'est d'ailleurs ce que fait le Conseil d'Etat lorsqu'il est amené à exercer une compétence consultative à propos de questions administratives non litigieuses relatives à l'application de lois ou de règlements[16]. Cela supposait, également, qu'elle se prononce objectivement sur l'application de la loi et l'interprétation à lui donner dans les hypothèses soulevées par le cas d'espèce. Une telle attitude aurait d'ailleurs donné pleinement sens à l'article 29 en ce qu'il habilite cette autorité à se prononcer sur toute « question » relative à la protection de la vie privée. Ces questions, justement, ne manquaient pas. Lorsque le centre de traitement de l'entreprise se trouve aux Etats-Unis, la loi s'applique-t-elle ? Quels critères utiliser pour identifier le responsable du traitement et les sous-traitants de celui-ci? Ce sont là quelques interrogations parmi d'autres. Plutôt que d'y répondre, la Commission belge articule son raisonnement autour des faits reprochés à SWIFT afin de démontrer sa responsabilité. Finalement, il revient au citoyen de chercher les réponses aux questions soulevées en filigrane d'un verdict que la Commission n'était pas habilitée à donner.

On pouvait également attendre de la Commission qu'elle adopte une attitude constructive. Cela supposait qu'outre les reproches adressés au passé, elle offre des solutions pour l'avenir. C'est d'ailleurs ce qu'a fait le Groupe de l'article 29 dans son avis rendu en novembre 2006 au sujet de la même affaire[17]. Après avoir interprété la directive 95/46/CE de manière générale à l'occasion des problèmes soulevés par l' « affaire » Swift, il adresse plusieurs conseils à cette entreprise, à la Banque nationale et aux différentes institutions financières.

9. S'il semble dès lors que la Commission n'a pas respecté les limites imposées par l'article 29 de la loi, cette dernière a-t-elle respecté la procédure prévue par l'article 31 de la loi ?

L'article 31 subordonne l'émission d'un avis à l'existence d'une plainte ayant trait « à sa mission de protection de la vie privée à l'égard des traitements de données à caractère personnel ou à d'autres missions qui lui sont confiées par la loi »[18]. Cette plainte peut être introduite par toute personne témoignant d'un intérêt[19]. Si la plainte est jugée recevable, elle est portée à la connaissance du maître de fichier qui peut alors exercer un droit de défense[20]. Au vu des arguments avancés de part et d'autre, la Commission tente de concilier les parties. A défaut d'y être parvenue, elle émet un avis sur le caractère fondé de la plainte. Celui-ci peut être accompagné de recommandations à l'intention du responsable de traitement[21].

10. En l'espèce, la Commission fait référence à une plainte introduite par l'organisation « Privacy International » qui l'aurait incitée à intervenir. Pourtant, l'avis de la Commission ne se prononce pas sur la recevabilité de la plainte, ni sur son caractère fondé ou non. En outre, Swift n'a pu exercer son droit de défense. La Commission n'a pas non plus tenté de concilier Swift et le plaignant. Il semble donc que l'avis en question n'ait pas été rendu conformément à cette procédure.

---

15 M. LEROY, *Contentieux administratif,* Bruxelles, Bruylant, 3ème éd., 2004, p. 164.
16 *Ibidem,* pp. 163-165.
17 Avis du 22 novembre 2006 WP 128, disponible sur le site http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
18 Article 31, §1, de la loi.
19 Article 16 du Règlement d'ordre intérieur de la Commission de la protection de la vie privée ci-après « R.O.I. ».
20 Article 31, §2, de la loi ; article 21 et s. du R.O.I.
21 Article 31, §3, de la loi ; article 25 du R.O.I

11. Au vu de ces critiques, des recours seraient-ils possibles à l'encontre d'un tel avis? La réponse à cette question varie : soit l'avis est rendu par application de l'article 29, soit il est rendu par application de l'article 31 de la loi.

Dans l'hypothèse où l'avis est rendu sur la base de l'article 29 de la loi, un recours devant le Conseil d'Etat semble devoir être exclu. En effet, la Commission ne peut être considérée comme une autorité administrative, n'étant pas soumise à suffisance au contrôle du pouvoir exécutif[22]. Dès lors, les actes qu'elle adopte ne peuvent être considérés comme des actes administratifs susceptibles d'annulation par la Haute juridiction administrative.

Par ailleurs, un recours devant une juridiction civile serait subordonné aux conditions de l'article 1382 du Code civil. Ainsi faudrait-il prouver que la Commission, en ne respectant pas les limites de sa compétence consultative, a commis une faute et qu'en outre, cette faute ait causé un dommage à la société Swift. Or, le dommage peut-il être trouvé dans l'atteinte à la réputation, la faute, dans le non respect des droits minimaux de la défense ? Nous ne sommes pas là pour trancher.

Dans l'hypothèse où l'avis est rendu sur la base de l'article 31 de la loi, on peut se demander s'il ne constitue pas un acte juridictionnel attaquable devant le Conseil d'Etat. La procédure instituée par l'article 31 révèle, en effet, différents indices en ce sens. Ainsi, l'avis se prononce sur un conflit entre un maître de fichier et une personne ayant porté plainte à son égard. La procédure à suivre, prévue par la loi et le règlement d'ordre intérieur de la Commission, prévoit certaines garanties telles que le respect des droits de la défense, la possibilité pour la Commission d'auditionner les parties ou d'ordonner des mesures d'instruction ainsi que l'obligation de motiver les avis rendus et les recommandations qui les accompagneraient[23].

Ces seuls indices peuvent-ils suffire à démontrer l'existence, en l'espèce, d'un acte juridictionnel ? L'avis, remarquera l'observateur attentif, ne revêt pas l'autorité de la chose jugée. Il n'a pas non plus de valeur exécutoire puisque le refus de se conformer à cet acte n'est assorti d'aucune sanction légale. Et la Commission peut-elle être qualifiée de juridiction administrative alors que les « juges » ne bénéficient pas de toutes les garanties d'indépendance ?

12. La transposition de la directive 95/46/CE qui a abouti à la loi du 8 décembre 1992 relative à la protection de la vie privée était l'occasion de préciser les compétences de la Commission. Il importait, en particulier, de distinguer la compétence consultative de la Commission, de sa compétence décisionnelle et de prévoir, dans ce dernier cas, des recours juridictionnels. En effet, la directive dispose qu'outre une compétence consultative, l'autorité de contrôle a le pouvoir d'ordonner un certain nombre de mesures telles que l'effacement ou la destruction de données, l'interdiction temporaire ou définitive d'un traitement, etc. Les décisions faisant grief peuvent faire l'objet d'un recours juridictionnel. Une telle possibilité est pourtant inexistante en droit belge si bien que les citoyens risquent de se trouver dépourvus de toute possibilité de contester les décisions de la Commission.

---

[22] E. DEGRAVE, « La Commission de la protection de la vie privée : un organisme invincible ? », *R.T.D.I.,* 2006, pp. 237-238.

[23] Pour de plus amples détails au sujet de ces indices, voy. M. LEROY, *op. cit.,* pp. 115-137 et 210-212 ; P. LEWALLE, *Contentieux administratif,* Bruxelles, Larcier, 2002, pp. 347-369.

Conclusions

13. Notre propos peut être perçu comme polémique à l'endroit des défenseurs de notre vie privée. Il n'en est rien. Que ceux ci veuillent bien lire, dans les lignes qui précèdent, notre volonté de rappeler les véritables enjeux de la protection des données dans un monde globalisé. Il est urgent que nos autorités européennes rappellent à la face du monde la manière dont elle entend assurer, sur base de la jurisprudence de l'article 8 de la Convention européenne des droits de l'homme, l'équilibre entre les impératifs de sécurité et cette protection des données, chaque jour plus fondamentale pour assurer nos libertés. L' « Affaire SWIFT » est l'occasion de ce rappel ; elle ne peut se transformer en un procès contre ce qui risque d'apparaître rapidement comme une victime de la propre incurie européenne. Par ailleurs, il est urgent que les compétences de notre Commission soient précisées, sous peine de transformer la Commission en un « juge » omnipotent sans que ne soient traduites les exigences d'un procès loyal mené en toute indépendance.