exigences posées par la méthode de couverture. Mais, signe de la nature objective de la responsabilité disciplinaire, la Commission a tout de même considéré que la régularisation était sans conséquence sur le grief[12].

Manquements afférents à la lutte contre le blanchiment. Les établissements de monnaie électronique sont, comme tous les prestataires de services de paiement et autres acteurs du domaine bancaire, tenus à des obligations imposées en vue de la LCB-FT[13]. À ce titre, ils doivent donc procéder à une classification des risques[14], identifier leurs clients[15] (ce que l'on nomme classiquement le KYC) et mettre en place un système de surveillance des opérations[16]. Les manquements aux obligations attachées à la LCB-FT comptent parmi les plus classiques dans le contentieux disciplinaire, mais les griefs retenus ici sont intéressants en ce qu'ils illustrent les attentes de l'ACPR en matière de monnaie électronique, notamment lorsqu'elle repose sur un réseau de distribution.

Ainsi, la société TSI a-t-elle été d'abord sanctionnée pour ne pas avoir mis en place une classification des risques couvrant l'activité de distribution de monnaie électronique par des réseaux de points de vente physiques, et pour avoir permis le règlement de montants pouvant atteindre des milliers d'euros de manière fractionnée, avec des cartes elles-mêmes limitées à 250 euros. Les procédures de surveillance qu'elle avait mises en place n'étaient pas suffisantes pour identifier les clients ayant procédé à des opérations importantes en termes de montants cumulés.

Pour les opérations de paiement à distance auxquelles elle permettait de procéder par simple utilisation de numéros de carte bancaire, TSI s'est vue ensuite reprocher de ne pas avoir identifié les clients lors de la collecte des fonds pour le compte de sites marchands alors même qu'elle n'était en relation qu'avec des intermédiaires (et non avec les sites eux-mêmes) et que les comptes bénéficiaires des règlements étaient principalement situés à Malte et dans les pays nordiques.

Plusieurs enseignements déterminants en pratique peuvent être déduits de cette décision. L'ACPR veille au respect du KYC par les distributeurs, pour lesquels l'émetteur peut être tenu responsable. Elle condamne la pratique des émissions fractionnées destinée à éviter l'assujettissement aux règles de KYC. Elle est très ferme sur l'obligation de vérifier l'identité des bénéficiaires finaux. Si le secteur des paiements s'est libéralisé, l'autorité française entend manifestement détecter tous les risques de fraude et mettre au pas, si nécessaire, les nouveaux acteurs. ■

12. En outre, le manquement avait été perpétué sur une longue période et était établi au moment du contrôle.
13. P. Storrer, *op. cit.*, n° 202, p. 177.
14. C. mon. fin., art. R. 561-38, I, 2°.
15. C. mon. fin., art. L. 561-5, I a. 1er et L. 561-6. Mais le législateur instaure toutefois une petite dérogation pour les opérations en monnaie électronique de petits montants (250 euros) dès que le montant total des opérations réalisées sur une année civile ne dépasse par un certain montant (2 500 euros).
16. Anciennement art. 11-7, 2.2 du règlement 97-02 (applicable au moment des faits) désormais arrêté du 3 novembre 2014.

Après l'arrêt Schrems, vers un *safe harbor 2.0* ?

Commentaire d'Emmanuel Jouffin

Le 6 octobre 2015, la CJUE[1] a rendu une importante décision en matière de protection des données personnelles. Dans cette espèce, M. Schrems reprochait au *Data Protection Commissioner* (la CNIL irlandaise) son refus d'enquêter sur le fait que Facebook Ireland Ltd transférait aux États-Unis les données à caractère personnel de ses utilisateurs et les conservait sur des serveurs situés dans ce pays. Saisie d'une question préjudicielle, la CJUE[2] a invalidé purement et simplement la décision de la Commission du 26 juillet 2000 (2000/520/CE) ayant fixé les principes du *Safe Harbor*. Ce dernier permettait de considérer les transferts de données en provenance de l'Union européenne vers les États-Unis comme s'effectuant avec un niveau de protection jugé équivalent aux standards européens en la matière.

L'arrêt *Schrems* ne saurait surprendre[3]. En effet, il se place dans le droit fil d'une communication de la Commission du 27 novembre 2013[4] dont le point 8 énonçait que « l'*accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis* ». Par ailleurs, une résolution du Parlement européen du 12 mars 2014[5] invitait à cette occasion les États membres à adopter un *habeas corpus* numérique européen et à suspendre, purement et simplement, l'accord *Safe Harbour* ainsi que l'Accord TFTP (Accord Swift).

Les conséquences pratiques de cette décision sont importantes. La CJUE, en annulant l'accord de *Safe Harbor*, prohibe *ipso jure* tout transfert de données personnelles en

1. CJUE 6 octobre 2015, *Schrems c/ Irish Data Protection Commissionner*, C-362/14.
2. Suivant en cela les conclusions remarquées de l'Avocat général Yves Bot en date du 23 septembre 2015.
3. Déjà le 8 avril 2014 (*Digital Rights Ireland et Seitlinger e. a*, aff. C-293/12 et C-594/12. AJDA 2014. 773, 1147), la CJUE avait purement et simplement invalidé, en son entier, la directive 2006/24 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications ; Chron. M. Aubert, E. Broussy et H. Cassagnabère, *D.* 2014, 1355, note C. Castets-Renard, *ibid.* 2317, obs. J. Larrieu, C. C. le Stanc et P. Tréfigny.
4. Communication de la Commission faite au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire COM(2013) 847.
5. Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures.

direction des États-Unis fondé sur ce seul accord[6]. Ce qui ne veut pas dire que tout transfert soit absolument interdit, du moins à la lettre de l'arrêt *Schrems*.

En premier lieu, les entreprises peuvent recourir aux exceptions prévues par la directive 95/46 CE du 24 octobre 1995 et reprises sous l'article 69 de la loi du 6 janvier 1978[7]. Aux remarques de principe faites ci-dessus s'agissant de l'accès massif par les services de renseignement américains aux données personnelles, s'en ajoute une autre. Les exceptions de l'article 69 sont d'application stricte, la CNIL et le G29[8] recommandant que les « *transferts répétitifs, massifs ou structurels de données personnelles* » ou bien encore, ceux « *dont l'importance ou la régularité justifient qu'ils soient encadrés de manière précise* », ne puissent reposer sur ces dérogations. Même si ces recommandations ne sont pas normatives, elles doivent toutefois être prises en considération.

À défaut de référence faite à l'article 69, il faudra recourir à la rédaction des clauses contractuelles types dans les relations entre l'entreprise exportatrice des données et celle les recevant. La décision 2001/497/CE de la Commission du 15 juin 2001 relative à ces clauses en matière de transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE[9] fixe un clausier type assurant des garanties adéquates pour le transfert de données vers des pays tiers.

Hors le recours aux clauses types, il est également possible de recourir aux BCR (*Binding Corporate Rules*), ou règles internes d'entreprise. Les entreprises qui rédigent ces règles, impliquant le respect d'un code de bonne conduite en matière de préservation des données personnelles, les font approuver par la CNIL et ses homologues concernés. Une fois ces engagements de conformité souscrits, les responsables de traitement tiennent à disposition de la CNIL une liste à jour des transferts. Ces deux dernières exceptions posent la question de la protection effective des données personnelles dans le contexte rappelé dans l'affaire Schrems.

À cet égard, dans un communiqué de presse du 16 octobre[10], la CNIL fait état d'une demande du G29 auprès des institutions et gouvernements européens afin que soient trouvées des solutions juridiques et techniques avant le 31 janvier 2016. D'ici là, la CNIL estime que les solutions alternatives que sont les BCR et clauses contractuelles types conservent toute leur pertinence. Le communiqué poursuit en soulignant que « *si aucune solution satisfaisante n'était trouvée avec les autorités américaines avant la fin du mois de janvier 2016 et en fonction de l'évaluation en cours des outils de transferts par le G29, les autorités s'engagent à mettre en œuvre toutes les actions nécessaires, y compris des actions répressives coordonnées* ».

Dix jours plus tard, le 26 octobre, la commissaire européenne Vera Jourová[11] annonçait qu'un accord sur les questions de principe avait été trouvé avec les autorités américaines, de telle sorte que les engagements souscrits soient « *suffisamment contraignants pour répondre pleinement aux exigences de la Cour* ». Toutefois, il est souligné que le mécanisme de préservation des données personnelles n'assurera pas nécessairement une protection identique, mais « *globally equivalent to the ones we have in Europe* », l'important étant d'empêcher l'accès ou l'utilisation de données personnelles sur une « *base généralisée* »[12]. Tout ceci reposera sur un « *statu quo dynamique* »[13] conduisant à des révisions annuelles tenant notamment compte d'impératifs sécuritaires. En dernier lieu, les orientations prises la Commission le 6 novembre[14] rappellent la faculté de recourir aux instruments dérogatoires ci-dessus décrits et confirme la poursuite des discussions avec les États-Unis.

Rappelons que quatre ans de négociations entre l'Union européenne et les États-Unis avaient été nécessaires avant que soit conclu, le 8 septembre 2015, un accord-cadre « Umbrella Agreement » relatif aux transferts de données personnelles en matière policière et judiciaire pénale[15]. Cet accord ne deviendra définitif qu'après l'adoption du *Judicial Redress Bill*[16] devant accorder aux citoyens de l'Union européenne des droits de recours identiques à ceux des citoyens américains. On le voit, les accents martiaux du Communiqué du 16 octobre sont bien loin.

En attendant la diffusion de lignes directives, reflets des discussions en cours, il convient de recenser les transferts concernés et les solutions alternatives envisageables (conclusion de contrats de transferts basés sur les clauses type de la Commission, préparation de « BCR », relocalisation des données dans des pays assurant une protection des données adéquates, renégociations contractuelles liées à ces diverses décisions...). Par ailleurs, il convient de vérifier si l'existence de sous-prestations de services n'est pas menacée. Enfin, peut-être faut-il anticiper d'éventuelles interrogations de la clientèle sur ce sujet médiatiquement sensible. ■

6. En ce sens, le communiqué de presse de la CNIL en date du 7 octobre 2015.
7. La personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes : 1° A la sauvegarde de la vie de cette personne ; 2° À la sauvegarde de l'intérêt public ; 3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ; 4° À la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ; 5° À l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ; 6° À la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers. Enfin, sont possibles les transferts autorisés par décret en Conseil d'État.
8. http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/exceptions/. Voir également le document de travail du G29 relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive du 24 octobre 1995, WP114, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_fr.pdf.
9. JO L 181 du 4.7.2001, p. 19.
10. http://www.cnil.fr/linstitution/actualite/article/article/safe-harbor-le-g29-demande-aux-institutions-europeennes-et-aux-gouvernements-dagir-sous-3-mois/
11. http://europa.eu/rapid/press-release_SPEECH-15-5916_fr.htm
12. « [...] *And we are working hard with the US to do just that : to ensure that there are sufficient limitations and safeguards in place to prevent access or use of personal data on a "generalised basis" and to ensure that there is sufficient judicial control over such activities.* »
13. « [...] *the Court has confirmed that an adequacy decision is a living document ; it must be periodically reviewed in light of developments of the foreign system.* »
14. Communiqué de presse : http://europa.eu/rapid/press-release_IP-15-6015_fr.htm
15. http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm et http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm
16. Le Congrès US estime que l'adoption de cette loi est « *an important step forward in the EU US negotiations over the data transfer regime that now needs a new solution after the Court of Justice of the European Union ruled the Safe Harbor arrangement illegal* » : https://www.congress.gov/bill/114th-congress/house-bill/1428