Chronique

Nouveaux moyens de paiement, banque digitale et protection des données

PIERRE STORRER*
Avocat au Barreau
de Paris
Kramer Levin Naftalis
& Frankel LLP

MYRIAM ROUSSILLE
Agrégée des facultés
de Droit
Professeur
Université du Mans
IRJS Sorbonne
Affaires-Finance

LOUISE LAÏDI*
Juriste
BPCE

Premiers regards sur l'impact du RGPD en matière bancaire

Commentaire de Myriam Roussille et Pierre Storrer

Le temps est aux données. Quelques mois après la publication de la DSP 2[1] (23 décembre 2015), voici donc que paraissait le RGPD[2] (4 mai 2016), applicable à partir du 25 mai 2018, cependant que la première entrera en application au 13 janvier 2018. On y ajouterait la décision *Bouclier de protection des données UE-États-Unis* ou *EU-U.S. Privacy Shield* du 12 juillet 2016 voire, dans un registre plus large, la directive (UE) 2016/943 du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites. Cette concordance des temps est assurément bienvenue[3], la protection des données de paiement nous paraissant être l'un des enjeux majeurs du futur droit des paiements.

Côté crédit, les textes ne sont naturellement pas en phase avec le RGPD, la directive Crédit immobilier adoptée le 2 février 2014 n'ayant pas anticipé son adoption[4], bien que les travaux de refonte de la directive de 1995 eussent démarré, tandis que la directive Crédit aux consommateurs était bien plus ancienne encore (2008)[5]. Pourtant, la gestion des données collectées lors de l'octroi des crédits (et durant leur exécution) est incontestablement l'une des contraintes majeures des prochaines années pour les établissements bancaires. À cet égard, les nouveautés introduites par le RGPD pourraient bien prendre une grande importance, l'appréciation de la solvabilité de l'emprunteur impliquant nécessairement un travail sur les données le concernant.

Mais le point de contact le plus problématique tient sans doute à l'articulation du RGPD avec les exigences posées en matière de lutte contre le blanchiment des capitaux et de financement du terrorisme (LCB-FT).

RGPD, données bancaires et données personnelles collectées par les banques. S'il est évident que le RGPD a vocation à s'appliquer aux données collectées, détenues et traitées par les banques et acteurs parabancaires (établissements de paiement, établissements de monnaie électronique et société de financement), il ne leur consacre par pour autant une place particulière. On ne trouve dans le règlement ni définition, ni dispositions spécifiques à ces données[6], alors même

1. Dir. (UE) 2015/2366, 25 nov. 2015, concernant les services de paiement dans le marché intérieur.
2. Règl. (UE) 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).
3. Encore que l'on eût aimé que l'adoption du RGPD précédât celle de la DSP 2, qui aurait permis à celle-ci de se référer à celui-là et non à la directive de 1995.
4. Dir. 2014/17/UE, 4 févr. 2014, concernant les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel.
5. Dir. 2008/48/CE du 23 avril 2008 concernant les contrats de crédit aux consommateurs.
6. Pas plus qu'il n'en figurait dans la directive du 24 octobre 1995.

*Les propos de l'auteur n'engagent que celui-ci.

qu'il est indéniable qu'il s'agit de données personnelles particulières[7], et que les problématiques qu'elles soulèvent le sont tout autant. Il est vrai que si certaines de ces données résultent principalement de la relation de la personne avec son établissement de crédit (données liées au compte, données de paiement), d'autres sont plus « *classiques* » (domicile, informations relatives à la composition du foyer et à la situation matrimoniale). En outre, les suggestions imposées aux établissements (par le dispositif LCB-FT ou les directives Crédit) les conduisent à détenir des informations sensibles[8] auxquelles le RGDP consacre une place spécifique (données de santé, infractions pénales) sans prendre en considération la singularité du traitement qui doit en être fait dans le domaine bancaire[9].

Changements institutionnels. Compte tenu des risques importants résultant des données qu'ils collectent et traitent quotidiennement, tous les établissements bancaires (et parabancaires) vont devoir se doter d'un délégué à la protection des données (l'acronyme anglais DPO s'imposera sans doute[10]) d'ici mai 2018, ce qui constitue une contrainte organisationnelle majeure[11]. Le RGPD oblige en effet les établissements responsables de traitement à procéder à la désignation d'un DPO lorsque leurs activités de base « *consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées* »[12]. Aussi, même si les procédures étaient jusqu'à présent bien organisées dans les établissements[13], le RGPD obligera tous les établissements à se doter d'un DPO, compte tenu des traitements de masse qu'exige l'activité bancaire et des risques qui y sont associés. Le changement est important, car au regard de la loi Informatique et libertés, la nomination d'un « *correspondant informatique et libertés* » (CIL en pratique) était facultative[14], de sorte que peu d'établissements français s'étaient dotés d'un tel correspondant. Les établissements pourront soit désigner un membre de leur personnel, soit un prestataire[15], auquel cas le régime des prestations de services essentiels externalisés s'appliquera[16]. Les coûts et aménagements organisationnels sont sérieux, car le DPO devra être mis en mesure d'exercer pleinement ses missions, et ce en toute indépendance par rapport à la direction de l'établissement[17].

L'un des changements majeurs résulte aussi du régime applicable en cas de recours à des sous-traitants, même établis hors de l'Union européenne[18], ce qui est une situation fréquente en matière bancaire et qui a vocation à se développer avec le *Big Data*. Les établissements qui sous-traitent une prestation impliquant un traitement de données personnelles, ne pourront faire appel qu'à des prestataires présentant des garanties suffisantes sur le plan tant technique aussi bien qu'organisationnel et l'établissement devra en répondre[19]. Ceux qui sont sous-traitants d'autres établissements (notamment dans les groupes) devront se doter de leur propre DPO dès lors que la prestation qui leur est confiée implique des traitements de masse. À cet égard, l'articulation avec les règles posées par l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiements et des services d'investissement (ci-après « arrêté relatif au contrôle interne des établissements financiers ») alimente déjà des questions[20].

Plan. Le RGDP ayant d'ores et déjà fait l'objet d'une riche étude dans cette Revue[21], nous nous centrerons sur son articulation avec les principales réglementations bancaires, en commençant par la DSP 2 s'agissant de l'accès au compte et aux données de paiement (I.) avant d'aborder les règles et contraintes en matière de crédit (II.) et enfin les exigences en matière de LCB-FT (III.).

7. Que l'on en envisage un numéro de compte, un RIB, une donnée attachée à une carte de paiement ou même simplement une donnée de transaction permettant de faire le lien avec l'une de ces informations, il s'agit de données « *purement* » bancaires. En visant les données qui permettant de faire le lien avec une « *personne physique identifiable* » par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, l'article 4.1 du RGPD recouvre ainsi une grande partie des données détenues par les banques.
8. À dire vrai, toutes les données collectées par les établissements bancaires et para-bancaires peuvent être considérées comme des « *données sensibles* » au sens large, bien que le RGDP ne leur consacre pas un régime particulier, comme pour les données de santé ou les données d'infractions. Curieusement, le RGPD paraît flottant sur la notion de « *données sensibles* », qu'il érige en notion à son considérant 10 (« *Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées "données sensibles"). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite* »), sans plus jamais y faire référence par la suite.
9. Ce constat avait déjà été réalisé dans des études consacrées aux données personnelles en matière bancaire sous l'empire du régime antérieur (directive de 1995, loi informatique et libertés) : J. Morel-Maroger, « La protection des données personnelles des clients des banques : bilan et perspectives », *RDBF* n° 2, mars 2011, étude 10 ; voir aussi C. Torrés, « Informatique et libertés : La protection des données à caractère personnel dans le secteur bancaire », *Revue Banque* n° 730, déc. 2010, p. xxx. Renouvelant ce constat avec l'étude de la proposition de règlement : J. Morel-Maroger, M. Roussille en collaboration avec P. Storrer, « Données et services bancaires », in *La proposition de règlement européen relatif aux données à caractère personnel : proposition du réseau Trans Europe Experts* (sous la dir. N. Martial-Braz), coll. « Trans Europe Expert » 2014, p. 395. Voir encore : P. Storrer, « De la protection européenne des données personnelles bancaires », *Revue Banque* n° 769, janv. 2014.
10. DPO pour *Data Privacy Officer*.
11. En ce sens, E. Jouffin, « Les lignes de force du règlement général sur la protection des données », *Banque et Droit* n° 168, juill.-août 2016, p. 8, p. 14 ; E. Jouffin, X. Lemarteleur et M.-N. Gibon, « Le Règlement sur la Protection des données : les 10 Commandements à connaître pour passer de la théorie à la pratique », *Revue de droit bancaire et financier*, juill.-août 2016, p. 11., spéc. p. 17.
12. RGPD, art. 37.1. b), avant que le développement de l'identification par biométrie ne les conduise à tomber dans l'hypothèse visée au 37.1.c).
13. Les obligations liées à la protection des données personnelles sont généralement gérées par les services de conformité, en collaboration avec les services juridiques et parfois les services informatiques.
14. Loi n° 78-17 du 6 janvier 1978, art. 22 III.
15. RGPD, art. 37.6.
16. Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement, art. 10 q et art. 231 à 240.
17. Sur les missions du DPO et les conditions de leur exercice : E. Jouffin, art. précit., spéc. p. 14.
18. RGPD, art. 27.
19. RGPD, art. 28.1.
20. E. Jouffin, art. précit., spéc. p. 10.
21. Cf. E. Jouffin, art. précit.

I. DSP 2, ACCÈS AU COMPTE ET DONNÉES DE PAIEMENT (par P. Storrer)

DSP 2 et données personnelles. Quels sont les points de contact, d'interaction, voire de friction, entre DSP 2 et RGPD ? Ils sont nombreux, ne serait-ce que par l'ouverture du compte de paiement à des prestataires qui ne le gèrent pas, en particulier aux prestataires de services d'information sur les comptes (PSIC), dont le métier sera précisément de traiter les données de compte[22].

Consentement au traitement des données. La seule prescription générale de la DSP 2 en matière de protection des données figure à son article 92 qui, par comparaison avec la disposition sœur de la DSP[23], ajoute cette précision significative : « *Les prestataires de services de paiement n'ont accès à des données à caractère personnel nécessaires à l'exécution de leurs services de paiement, ne les traitent et ne les conservent qu'avec le consentement explicite de l'utilisateur de services de paiement* ». Or l'on sait[24] que si le RGDP n'innove pas en la matière : un traitement n'est licite que si, et avant tout, « *la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques* »[25], des précisions sur le recueil de celui-ci sont notablement apportées à son article 7, qui imposeront à coup sûr de revisiter les conditions générales et autres contrats-cadres de services de paiement.

De l'*accountability*. C'est sans nul doute, dans l'esprit, l'innovation majeure apportée par le RGPD : le basculement d'une approche formaliste *ex ante* à une logique de conformité ex post, souvent nommé *accountability* ou « *principe de responsabilité* »[26], ainsi inscrit, presque de manière anodine, à l'article 5, 2 du règlement : « *Le responsable de traitement est responsable du respect du paragraphe 1* [conditions de licéité du traitement] *et est en mesure de démontrer que celui-ci est respecté (responsabilité)* ».

L'*accountability* a-t-elle gagné la DSP 2 ? Sans doute sur le terrain de la sécurité, en vertu, nous semble-t-il, d'une approche par les risques chère au droit antiblanchiment[27]. L'illustre notamment le considérant 91 : « *Les prestataires de services de paiement sont responsables des mesures de sécurité. Celles-ci doivent être proportionnées aux risques de sécurité concernés. Les prestataires de services de paiement devraient établir un cadre permettant d'atténuer les risques et maintenir des procédures efficaces de gestion des incidents. Il convient de mettre en place un dispositif de déclaration régulière, permettant de veiller à ce que les prestataires de services de paiement fournissent régulièrement aux autorités compétentes une évaluation à jour de leurs risques de sécurité ainsi que des informations à jour sur les mesures prises en réponse à ces risques* ».

A ainsi été ajouté dans la DSP 2 un chapitre entier relatif aux « *risques opérationnels et de sécurité et authentification* », prévoyant par exemple que les PSP fourniront à leur autorité de contrôle, chaque année au moins, « *une évaluation à jour et exhaustive des risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent et des informations sur le caractère adéquat des mesures d'atténuation et des mécanismes de contrôle mis en œuvre pour faire face à ces risques* »[28].

Vers une *privacy by design* ? La notion a fait couler beaucoup d'encre. Elle se retrouve aujourd'hui au point 1 de l'article 25 du RGPD, assez simplement exposée : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée* ».

Est-ce de la protection des données dès la conception ? En tout cas, figurent désormais parmi les 17 catégories d'information qu'une entreprise doit fournir afin d'être agréée établissement de paiement, les deux suivantes relatives aux données de paiement sensibles et/ou à caractère personnel : i) une description du processus en place pour enregistrer, surveiller et restreindre l'accès aux données de paiement sensibles et garder la trace de cet accès et ii) un document relatif à la politique de sécurité, comprenant une analyse détaillée des risques en ce qui concerne les services de paiement proposés et une description des mesures de maîtrise et d'atténuation prises pour protéger les utilisateurs de services de paiement de façon adéquate contre les risques décelés en matière de sécurité, y compris la fraude et l'utilisation illicite de données sensibles ou à caractère personnel[29].

Accès aux données de compte. La DSP 2 ne contient aucune définition des données de compte ni des données de paiement, seulement celle des « *données de paiement sensibles* », entendues (mollement) comme les « *données, y compris les données de sécurité personnalisées, qui sont susceptibles d'être utilisées pour commettre une fraude* », étant ajouté – c'est le plus important – qu'« *en ce qui concerne les activités des prestataires de services d'initiation de paiement et des prestataires de services d'information sur les comptes, le nom du titulaire du compte et le numéro de compte ne constituent pas des données de paiement sensibles* »[30]. Cette

22. Cf. P. Storrer, « Du droit de donner libre accès à son compte de paiement », *Banque et Droit*, Hors-Série « DSP 2 : le futur du paiement », juill.-août 2016, p. 14.
23. DSP, art. 79.
24. Cf. E. Jouffin, art. précit.
25. RGPD, art. 6, 1, a.
26. Cf. RGPD, cons. 85, dans sa version anglaise.
27. V. *infra*.
28. DSP 2, art. 95, 2.
29. DSP 2, art. 5, g et j.
30. DSP 2, art. 4, 32

absence de définition est évidemment malheureuse à l'heure où les comptes de paiement sont (le seront bientôt) ouverts à d'autres que ceux qui les gèrent.

Aussi bien, du côté du PSIC, c'est la règle du consentement explicite qui prévaut : ce dernier, en effet et en premier lieu, « *fournit des services uniquement sur la base du consentement explicite de l'utilisateur de services de paiement* » et « *n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'information sur les comptes expressément demandée par l'utilisateur de services de paiement, conformément aux règles relatives à la protection des données* »[31]. Le prestataire de services d'initiation de paiement (PSIP), de son côté, est soumis au principe de finalité, en ce sens qu'il « *ne demande pas à l'utilisateur de services de paiement des données autres que celles nécessaires pour fournir le service d'initiation de paiement* » ni « *n'utilise, ne consulte ou ne stocke des données à des fins autres que la fourniture du service d'initiation de paiement expressément demandée par le payeur* »[32].

Quant à l'authentification forte du payeur (notamment requise lorsqu'il accède à son compte de paiement en ligne ou initie une opération de paiement électronique), on note que parmi les normes techniques de réglementation que l'Autorité bancaire européenne (ABE) est chargée de prendre[33], figurent les mesures de sécurité propres à protéger la confidentialité et l'intégrité des données de sécurité personnalisées de l'utilisateur de services de paiement[34]. Plus généralement, l'ABE doit élaborer ses normes en vue de garantir non seulement la sécurité des fonds mais aussi celle des données à caractère personnel des utilisateurs[35].

Droit à la portabilité des données et mobilité du compte de paiement. Le RGPD crée de manière significative un droit à la « portabilité des données », ainsi prévu au point 1 de l'article 20 : « *Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* [...] ».

Cette disposition accompagnera utilement, nous semble-t-il, le droit à la mobilité bancaire inscrit à l'article L. 312-1-7 du CMF et, plus largement, celui au changement de compte posé par la directive « Comptes de paiement » 2014/92/UE du 23 juillet 2014. Directive qui composera demain (elle est toujours en attente de transposition, alors que l'échéance était au 18 septembre... 2016 !), avec la DSP 2, le droit des paiements nouveau.

II. RGPD ET DONNÉES DE CRÉDIT : ENTRE SOUPLESSE ET CONTRAINTES

(Par M. Roussille)

Directives Crédit et données personnelles. Les grands textes européens adoptés ces dernières années en matière de crédit ne développent pas autant la problématique du traitement des données que ne le fait la DSP 2. Même la directive Crédit immobilier[36], la plus récente, ne consacre que quelques lignes au sujet, sous forme de préconisations presque informelles, dans ses considérants : « *le prêteur devrait informer le consommateur qu'il va consulter une base de données sur le crédit avant de procéder à cette consultation, et le consommateur devrait avoir le droit d'accéder aux données à caractère personnel le concernant qui sont traitées dans cette base de données afin, si nécessaire, de les faire rectifier, effacer ou verrouiller lorsqu'elles sont inexactes ou ont fait l'objet d'un traitement illégal* »[37] ; « *lorsqu'une décision de rejet d'une demande de crédit se fonde sur les données obtenues par la consultation d'une base de données, ou sur l'absence de données pertinentes dans cette base de données, il conviendrait que le prêteur en informe le consommateur et qu'il lui communique le nom de la base de données consultée ainsi que tout autre élément requis par la directive 95/46/CE, afin de permettre au consommateur d'exercer son droit d'accéder aux données à caractère personnel le concernant qui sont traitées dans cette base de données et, lorsque cela est justifié, de les faire rectifier, effacer ou verrouiller. Lorsqu'une décision de rejet d'une demande de crédit résulte d'une évaluation de solvabilité négative, le prêteur devrait en informer le consommateur dans les meilleurs délais* »[38].

La Directive de 2008 énonce, quant à elle, par une disposition-balai dans l'article consacré à l'accès aux bases de données que « *le présent article est sans préjudice de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* »[39].

Scoring. Que l'on envisage le crédit immobilier, le crédit à la consommation ou même le crédit aux entreprises – qui peut aussi impliquer le traitement de données personnelles, ne serait-ce que par l'identification des bénéficiaires effectifs des opérations au titre de la LCB-FT (voir *infra*) –, l'ensemble des opérations de crédit est fondé sur une évaluation du risque de solvabilité de l'emprunteur, qui se fonde généralement sur une notation dite « *scoring* ».

Cette opération met en cause le droit des emprunteurs à la protection de leurs données à divers égards. Elle prend en effet appui sur les données collectées dans les fichiers officiels mis en place pour centraliser les événements de crédit, dont la tenue donne lieu à des sanc-

31. DSP 2, art. 67, 2, a et f.

32. DSP 2, art. 66, 3, f et g.

33. Cf. EBA, *Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2*, 12 août 2016.

34. DSP 2, art. 98, 1, c.

35. DSP 2, art. 98, 2, b.

36. Dir. 2014/17/UE du 4 février 2014 concernant les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel.

37. Dir. 2014/17/UE, cons. 59.

38. Dir. 2014/17/UE, cons. 61.

39. Dir. 2008/48/CE du 23 avril 2008, art. 9.4.

tions (inscriptions abusives ou radiation tardives)[40], sans évoquer le serpent de mer du fichier central des crédits aux particuliers (dit « *fichier positif* »)[41].

Le projet initial du règlement excluait que l'octroi de crédit puisse être fondé sur un simple calcul de données informatiques. Finalement, le RGPD consacre *a contrario* le traitement automatisé de données, en affirmant le droit de la personne concernée de ne pas faire l'objet d'une décision fondée exclusivement sur un tel traitement automatisé[42]. En outre, le texte affirme que ce droit ne s'applique pas dans trois hypothèses, lorsque la décision (comprendre ici l'octroi de crédit) est : (a) soit nécessaire à la conclusion ou l'exécution d'un contrat entre la personne concernée et le responsable de traitement, (b) soit autorisée par le droit de l'Union (ou le droit national) avec des garanties suffisantes pour les droits et libertés et les intérêts légitimes de la personne (comprendre le candidat au crédit), (c) soit encore fondée sur le consentement explicite de la personne concernée. Bref, on comprend que l'octroi de crédit – pour lequel les directives européennes mettent aujourd'hui à la charge des établissements une obligation d'évaluer la solvabilité de l'emprunteur[43] – peut être fondé sur un *scoring* automatisé qui implique une collecte et un traitement de données peu compatibles avec la maîtrise que chacun peut entendre avoir sur les informations qui le concerne. Dès lors, comme la prise de décision automatisée en matière d'octroi de crédit est de nature à avoir des conséquences juridiques pour le candidat à l'emprunt, les établissements devront y apporter les garanties appropriées : ainsi, les banques devront au moins permettre « *à la personne concernée d'obtenir une intervention humaine de la part du responsable de traitement, d'exprimer son point de vue et de contester la décision* »[44]. Cela nécessitera une information spécifique de la personne.

III. RGPD ET LUTTE ANTIBLANCHIMENT

Approches par les risques. La réglementation antiblanchiment (LCB-FT), dans sa nouvelle version[45], et le RGPD introduisent tous deux une méthode commune : l'approche par les risques[46]. En réalité, cette approche n'est que le reflet de la volonté de responsabiliser les établissements, en allégeant du coup les autorités de contrôle qui ne sont plus tenues d'une approche *a priori* (ex : autorisation préalable à la CNIL) mais seulement d'un contrôle *a posteriori* (sous réserve de la procédure de déclaration). Aussi, les établissements bancaires qui ont déjà internalisé l'approche par les risques devraient-ils avoir plus de facilités que les acteurs d'autres secteurs à se mettre au pas !

Mais les deux textes ne sont toujours pas articulés[47]. Ils sont pourtant, dans leur esprit, radicalement antinomiques : la LCB-FT impose aux établissements de traiter et de collecter des données parfois très sensibles, alors que la réglementation des données personnelles tend à permettre aux personnes physiques de rester maîtresses de leurs données en exigeant qu'elles consentent à leur collecte et à leur traitement (et en instaurant un droit à l'oubli[48]).

Respect de la finalité des données et traitement à des fins autres. La quatrième directive antiblanchiment de 2015 semblait avoir réalisé une avancée certaine sur ce terrain[49], en interdisant aux personnes assujetties de traiter les données collectées aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme, d'une manière incompatible avec les finalités et de les utiliser toute autre finalité, par exemple à des fins commerciales[50]. Cette interdiction est cohérente avec le RGPD qui donne une place centrale à la finalité du traitement, et impose que les données soient collectées pour une ou plusieurs finalités spécifiques, nécessaires à l'exécution du contrat ou à l'obligation légale pesant sur le responsable de traitement ou à d'autres considérations (sauvegarde des intérêts vitaux, mission d'intérêt public…) qui sont toutes remplies dans le cadre du KYC imposé par la réglementation LCB-FT[51].

D'une manière concrète, cela signifie que les informations recueillies au moment de l'entrée en relation (par exemple ouverture de compte) pour accomplir l'obligation de KYC ne sont pas supposées être utilisées à des fins de démarchage ou de promotion par exemple : l'établissement est donc supposé faire une

40. À ce sujet, voir J. Morel-Maroger, M. Roussille en collaboration avec P. Storrer, art. précit., spéc. p. 406 et 407.

41. É.-A. Caprioli, « Refus de la CNIL d'autoriser un fichier central sur les crédits aux particuliers », *RD bancaire et fin.* n° 3, mai 2007, p. 123 ; Rapp. du comité chargé de préfigurer la création d'un registre national des crédits aux particuliers, 2 août 2011 : www.economie.gouv.fr. CE 30 déc. 2009, n° 306173, *Sté Experian : Juris-Data* n° 2009-017446 ; Comm. com. électr. 2010, comm. 36, note A. Lepage, H. Claret, « Le fichier positif, serpent de mer ou Leviathan », *JCP* 2013, 695.

42. RGPD, art. 22.1.

43. Dir. 2008/48/CE du 23 avril 2008, art. 8 ; Dir. 2014/17/UE du 4 février 2014, art. 18. C'est à cet égard que la directive 2014/17/UE énonce que « 7. *Le présent article est sans préjudice de la directive 95/46/CE* » (dir. précit., art. 18. 7). À ce sujet, voir J. Morel-Maroger, **xxx**.

44. RGPD, art. 22.3. Ce régime est assez proche de ce que nous connaissons aujourd'hui avec la loi Informatique et Libertés.

45. Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'uilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme. Sur ce texte : P. Storrer, « Lutte antiblanchiment : le pas de deux du législateur européen », *Revue Banque* n° 786, juin 2015 ; M. Roussille, « Régulation et conformité : Quatrième directive Antiblanchiment : consécration d'une nouvelle approche fondée sur les risques », *Banque et Droit* n° 162, juill. 2015 ; V. Hauser, « Blanchiment et terrorisme : 4e directive : une opportunité pour les établissements ? », Revue Banque n° 788, sept. 2015.

46. RGPD, art. 32, 1 : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque […]* ».

47. Sur l'articulation entre ces deux textes : A. Bank, « 4e directive Antiblanchiment et protection des données : quels impacts possibles ? », *Revue Banque* n° 762, juillet-août 2013.

48. RGPD, art. 17.

49. Selon les termes de l'exposé des motifs de la proposition de directive, les autorités européennes ont tenu à « clarifier l'interaction » entre les deux réglementations.

50. Dir. Préc., art. 41.2.

51. RGPD, art. 6.1.

autre collecte des données telles que l'adresse postale, l'adresse mail… pour pouvoir envoyer de la documentation publicitaire ou promotionnelle. En pratique, les conventions de compte prévoient toujours que la collecte des données permettant l'identification du client poursuit les deux finalités (LAB-FT + prospection), ce qui autorise les établissements à utiliser les données (coordonnées) pour les deux finalités. En revanche, les données propres au blanchiment restent cloisonnées.

En outre, le RGPD introduit une exception, en admettant que les données puissent être traitées à des fins autres que celles pour lesquelles elles ont été collectées, même en l'absence de consentement explicite de la personne concernée ou de règle légale (droit de l'Union ou droit de l'État). Un tel détournement est autorisé lorsqu'il existe « éventuellement » un lien entre les finalités pour lesquelles les données ont été collectées et le traitement ultérieur envisagé. Cela ne permettait-il pas d'utiliser des données collectées à des fins de LCB-FT pour d'autres opérations bancaires pour lesquelles les établissements financiers sont toujours soumis aux règles de LCB-FT ? Autrement dit, les données collectées lors d'une ouverture de compte ou d'une opération occasionnelle pourraient être utilisées pour d'autres opérations bancaires (nouvelles applications de paiement, opérations de crédit-bail…) alors même que l'intéressé n'avait pas donné son consentement à une telle utilisation.

Données d'infractions. Enfin, les deux textes apparaissent difficilement conciliables concernant les données dites « *d'infractions* » : le RGPD réserve une disposition spécifique aux traitements de données relatives à des condamnations pénales, infractions ou mesures de sûretés (ci-après « *données d'infractions* »). Il les enserre dans un cadre très restrictif, en prévoyant que ces données d'infractions ne peuvent être traitées que sous le contrôle de l'autorité publique ou si le traitement est autorisé par le droit de l'Union dans un dispositif assurant des garanties appropriées[52]. Or le dispositif LCB-FT, depuis la troisième directive de 2005[53], impose aux établissements assujettis l'obligation de prévenir et de déclarer des faits de blanchiment, qui peuvent provenir de la commission d'infractions punie d'une peine ou d'une mesure de sûreté supérieure à un an (qualifiées dans le texte d'« *infractions graves* »), sans pour autant autoriser explicitement les établissements à traiter les données qui peuvent en attester : la directive ne fait qu'autoriser les établissements assujettis à transmettre à la cellule de renseignements financiers (TRACFIN) à fournir toutes les informations nécessaires pour étayer la déclaration. Le sujet avait déjà retenu l'attention du G29[54]. Mais toutes les difficultés ne semblent pas en l'état résolues. ■

52. RGPD, art. 10.

53. Dir. 2005/60/CE du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.

54. 01008/2011/EN. WP 186.