www.jusletter.ch

Nicolas Béguin / Benjamin Vignieu

Fuite de données bancaires : risques et devoirs d'information

Les banques suisses sont confrontées depuis plusieurs années au risque de fuite de données de leurs clients. Ces risques se sont matérialisés dans le cadre de plusieurs affaires retentissantes. Celles-ci ont permis de saisir l'importance que constituent ces données, que ce soit aux yeux de tiers mal intentionnés ou ceux d'autorités gouvernementales étrangères désireuses de sanctionner leurs contribuables indélicats. La contribution analyse les principaux risques juridiques que font courir de telles fuites tant pour les clients que pour les banques concernés, ainsi que les devoirs d'information de ces dernières dans ce contexte.

Catégories d'articles : Contributions
Domaines juridiques : Droit du marché des capitaux ; Protection des données ; Droit bancaire

Proposition de citation : Nicolas Béguin / Benjamin Vignieu, Fuite de données bancaires : risques et devoirs d'information, in : Jusletter 9 avril 2018

Table des matières

I. Introduction

[Rz 1] Outre les données qu'elles doivent collecter dans le cadre de leur activité opérationnelle, les banques sont de par la réglementation qui leur est applicable amenées à traiter un nombre considérable de données concernant leurs clients. Ce phénomène s'est amplifié au fil du temps par l'accroissement de la réglementation et le développement de la numérisation[1] dans le domaine financier, notamment par les nouvelles technologies financières[2]. Autrefois, gardiennes des seules valeurs patrimoniales de leurs clients, les banques sont ainsi devenues également les dépositaires de leurs données.

1 Cf. Rapport du Conseil fédéral du 11 janvier 2017 sur les principales conditions-cadre pour l'économie numérique, disponible sous https ://www.newsd.admin.ch/newsd/message/attachments/46894.pdf (dernière consultation 11 décembre 2017).

2 Cf. Association suisse des banquiers, Numérisation et Fintech, disponible sous http ://www.swissbanking.org/fr/themes/actualite/numerique (dernière consultation 11 décembre 2017) ; Discussion Paper on innovative uses of consumer data by financial institutions de l'Autorité bancaire européenne du 4 mai 2016, disponible sous http ://www.eba.europa.eu/-/eba-seeks-views-on-the-use-of-consumer-data-by-financial-institutions (dernière consultation 11 décembre 2017).

[Rz 2] La sécurité des données collectées par les banques n'est cependant pas infaillible. Des incidents de sécurité peuvent se produire. Ceux-ci peuvent être accidentels ou, au contraire, être orchestrés à dessein à des fins malveillantes ou bienveillantes selon les points de vue. On songe principalement à l'affaire Elmer[3], au vol de données à la filiale genevoise de la banque HSBC par Hervé Falciani[4], ou encore à l'achat par des inspecteurs du fisc du land de Rhénanie du Nord-Westphalie de données bancaires volées par un ex-employé de la banque UBS[5]. La fuite de données peut également intervenir dans le cadre de mesures d'investigation journalistiques. On pense bien sûr à toutes les affaires accolées des suffixes *leaks* ou *papers*, que ce soit les *Offshore Leaks* (avril 2013), les *China Leaks*[6] (janvier 2014), les *Luxembourg Leaks*[7] (novembre 2014), les *Swiss Leaks* (février 2015) et plus récemment l'affaire des *Panama papers*[8] (avril 2016) et des *Paradise papers*[9] (novembre 2017).

[Rz 3] Qu'elle soit accidentelle ou délictuelle, la fuite de données soulève divers problèmes juridiques, commerciaux et réputationnels pour les banques qui en sont victimes aux côtés de leurs clients. Une des questions qui se pose dans ce contexte est de savoir si la banque doit impérativement avertir les clients concernés ou d'autres autorités – notamment son régulateur – par une fuite et, le cas échéant, selon quelle forme et quel délai. Par ailleurs, se pose également la question des risques juridiques et règlementaires pour la banque liée à une absence d'information en temps utile, qu'elle procède d'une simple négligence ou, au contraire, qu'elle soit délibérée en raison de motifs commerciaux jugés prépondérants ou d'une éventuelle obligation de réserve imposée par le droit étranger.

---

3 Le Temps, Rudolf Elmer condamné pour violation du secret bancaire, article publié le 19 janvier 2011, disponible sous https ://www.letemps.ch/monde/2011/01/19/rudolf-elmer-condamne-violation-secret-bancaire (dernière consultation 23 janvier 2018) ; Le Temps, Peine pécuniaire avec sursis pour l'ex-banquier de Julius Baer, article publié le 19 janvier 2015, disponible sous https ://www.letemps.ch/suisse/2015/01/19/peine-pecuniaire-sursis-ex-banquier-julius-baer (dernière consultation 23 janvier 2018) ; Tribune de Genève, L'ex-cadre de Julius Baer condamné en appel, article publié le 23 août 2016, disponible sous https ://www.tdg.ch/suisse/prison-sursis-appel-rudolf-elmer/story/17743438 (dernière consultation 23 janvier 2018).

4 Hervé Falciani a été condamné de manière définitive en novembre 2015 à une peine privative de liberté de cinq ans pour tentative de service de renseignements économiques aggravé, en lien avec les données volées à la filiale genevoise de la banque HSBC (cf. arrêt du Tribunal pénal fédéral SK.2014.46 du 27 novembre 2015). Au moment de la mise sous presse de cette contribution, Hervé Facliani était interpellé à Madrid suite à une demande d'extradition de l'Office fédéral de la justice (OFJ), puis remis en liberté sous contrôle judiciaire.

5 Cet employé devait être jugé par le Tribunal pénal fédéral durant le mois de septembre 2017 (Pascal Schmuck, Le banquier suspect a déménagé en Allemagne, Tribune de Genève, article publié le 22 juin 2017, disponible sous https ://www.tdg.ch/suisse/banquier-suspect-demenage-allemagne/story/22212452 [dernière consultation 11 décembre 2017]).

6 Marina Walker Guevara et al., Leaked records reveal offshore holdings of China's elite, The International Consortium of Investigative Journalists, article publié le 21 janvier 2014, disponible sous https ://www.icij.org/offshore/leaked-records-reveal-offshore-holdings-chinas-elite# (dernière consultation 11 décembre 2017).

7 Leslie Wayne et al., Leaked documents expose global companies' secret tax deals in Luxembourg, The International Consortium of Investigative Journalists, article publié le 5 novembre 2014, disponible sous https ://www.icij.org/investigations/luxembourg-leaks/leaked-documents-expose-global-companies-secret-tax-deals-luxembourg/ (dernière consultation 11 décembre 2017).

8 Joan Tilouine et al., Chefs d'Etats, sportifs, milliardaires : premières révélations des « *Panama papers* » sur le système offshore mondial, Le Monde, article publié le 3 avril 2016, disponible sous http ://www.lemonde.fr/panama-papers/article/2016/04/03/chefs-d-etat-sportifs-milliardaires-premieres-revelations-des-panama-papers-sur-le-systeme-offshore-mondial_4894816_4890278.html (dernière consultation 11 décembre 2017).

9 The International Consortium of Investigative Journalists, About the Paradise Papers Investigation, article publié le 5 novembre 2017, disponible sous https ://www.icij.org/investigations/paradise-papers/about/ (dernière consultation 11 décembre 2017).

[Rz 4] Dans un premier temps, nous identifierons les principaux risques, essentiellement juridiques, liés à une fuite de données (infra **II.**). Nous examinerons tout d'abord les risques juridiques que présente un tel vol pour les clients concernés (infra **II. A.**), avant de se pencher sur les différents risques qu'une telle fuite fait encourir aux banques également victimes (infra **II. B.**). Dans un deuxième temps, nous exposerons les contours du devoir d'information des banques (cf. infra **III.**). Nous distinguerons dans ce contexte l'information qui doit être donnée aux clients dont les données ont fuitées (infra **III. A.**), de l'information qui doit le cas échéant être relayée aux autorités (infra **III. B.**).

II. Risques liés à une fuite de données

A. Risques pour les clients

[Rz 5] Les risques inhérents à une fuite de données sont divers et variés, en fonction de la nature des données transmises, de l'identité des clients concernés, et de leur situation en général. Dans le domaine bancaire, c'est le risque de publicité de l'existence d'une relation d'affaires avec un établissement spécifique, et de la détention d'actifs par le biais de véhicules et constructions juridiques *ad hoc* qui sont problématiques pour les clients concernés.

[Rz 6] Dans la grande majorité des cas, c'est toutefois le risque que les données tombent entre les mains de leur percepteur fiscal, qui est le plus redouté. De telles données sont en effet susceptibles d'être utilisées dans une procédure administrative et/ou pénale diligentée contre le client. Elles peuvent en outre servir de base à une demande d'assistance administrative en matière fiscale.

[Rz 7] Deux récentes affaires illustrent cette dernière problématique. La première concerne l'affaire du vol de données au sein d'une filiale française d'UBS, laquelle a ultimement conduit à l'admission d'une demande d'assistance administrative en matière fiscale (cf. infra **1**.). La seconde se rapporte à l'utilisation de données dérobées dans le cadre de l'affaire *Falciani*, mais cette fois-ci sans que les données en question aient pu être exploitées dans le cadre de l'entraide administrative (cf. infra **2**.).

1. Première illustration : l'affaire UBS (France) SA (ATF 143 II 202)

[Rz 8] Dans cette affaire, une employée de la filiale française d'UBS s'était appropriée une liste de 600 clients de la banque. Saisie d'une dénonciation par cette même employée pour complicité de blanchiment de fraude fiscale et de démarchage illicite sur territoire français, l'Autorité de contrôle prudentiel et de résolution avait initié en 2012 une procédure disciplinaire à l'encontre de la banque et transmis la dénonciation au Parquet de Paris. Ce dernier avait alors ouvert une information judiciaire pour démarchage bancaire ou financier par personne non habilitée et blanchiment de fraude fiscale et de fonds obtenus à l'aide d'un démarchage illicite commis en bande organisée. De son côté, la Direction générale des finances publiques françaises avait déposé en 2013 une demande d'assistance à l'Administration fédérale des contributions (« AFC ») en y joignant une liste de contribuables faisant l'objet d'une enquête par les services fiscaux français en se fondant sur les données volées.

[Rz 9] La demande d'assistance administrative avait été accordée par l'AFC nonobstant le fait qu'elle reposait sur des données volées. Si le Tribunal administratif fédéral avait dans un premier

temps annulé cette décision[10], le Tribunal fédéral a quant à lui confirmé dans un arrêt de principe du 16 février 2017 que la convention de double imposition avec la France (RS 0.672.934.91) ne permettait pas de refuser d'entrer en matière sur une demande d'assistance administrative en raison de la manière dont l'État requérant s'est procuré les données qui ont abouti à la formulation de la demande[11]. En particulier, notre Haute Cour a considéré que le principe posé par la loi sur l'assistance administrative fiscale (LAAF)[12] selon lequel la Suisse n'entrait pas en matière lorsque la demande se fonde sur des renseignements obtenus par des actes punissables au regard du droit suisse, présupposait la réalisation d'actes « *effectivement punissables en Suisse* »[13]. Or, la filiale française d'UBS n'étant pas un établissement soumis à la loi sur les banques (LB)[14], il ne pouvait par conséquent y avoir de violation au secret bancaire (art. 47 LB) à la suite de la transmission des documents par l'employée de cette même filiale. Après avoir également écarté toute violation des art. 162 et 273 al. 2 du Code pénal suisse (CP)[15], le Tribunal fédéral en concluait que la demande d'assistance administrative ne reposait pas sur des renseignements obtenus par des actes effectivement punissables au regard du droit suisse et qu'aucun élément ne permettait de remettre en cause la bonne foi de l'autorité française[16].

[Rz 10] Inutile de préciser que l'arrêt du Tribunal fédéral a été mal accueilli[17]. Sur le plan dogmatique, la distinction opérée par le Tribunal fédéral entre d'une part un vol de données perpétré au sein d'une banque en Suisse et d'autre part au sein d'une de ses filiales étrangères, est certes objectivement défendable. Toutefois, cette distinction peut paraître comme quelque peu artificielle à une époque où l'on attend précisément des banques suisses d'avoir une vision extraterritoriale de la gestion de leurs risques juridiques.

---

10 Arrêt du Tribunal administratif fédéral A-6843/2014 du 15 septembre 2015. Le Tribunal administratif fédéral a tout d'abord retenu que l'art. 28 par. 3 let. b de la Convention entre la Suisse et la France en vue d'éliminer les doubles impositions en matière d'impôts sur le revenu et sur la fortune et de prévenir la fraude et l'évasion fiscales conclue le 9 septembre 1966, entrée en vigueur en Suisse le 26 juillet 1967 (RS 0.672.934.91) « *ne permettait pas d'obtenir des renseignements qui ne pourraient être obtenus sur la base de la législation ou dans le cadre de la pratique administrative normale suisse ou de celles de l'autre Etat contractant* » (consid. 7.4.1). Dès lors, contrevenant à la pratique administrative suisse, l'autorité française ne pouvait obtenir des renseignements sur la base de données volées. Par ailleurs, le droit interne français ne permettait pas l'utilisation de données volées. Les autorités françaises n'étaient partant pas fondées à obtenir ces informations par la voie de l'assistance administrative internationale alors qu'elles ne pouvaient les obtenir en vertu de sa propre législation (consid. 7.4.2). Enfin, une demande d'assistance administrative fondée sur des renseignements obtenus par des actes punissables contrevenait au principe de la bonne foi, implicitement compris dans la convention (consid. 7.4.2).

11 Arrêt du Tribunal fédéral 2C_893/2015 du 16 février 2017 consid. 6.3.6 (publié au ATF 143 II 202) ; pour un résumé de cet arrêt cf. Fabien Liégeois, Données volées : Arrêt de principe du Tribunal fédéral, Centre de droit bancaire et financier, publié le 21 mars 2017, disponible sous https ://www.cdbf.ch/969/ (dernière consultation 11 décembre 2017).

12 Loi fédérale sur l'assistance administrative internationale en matière fiscale du 28 septembre 2012 (LAAF ; RS 651.1) ; cf. art. 7 let. c LAAF.

13 Arrêt du Tribunal fédéral 2C_893/2015 du 16 février 2017 consid. 8.5.6.

14 Loi fédérale sur les banques et les caisses d'épargne du 8 novembre 1934 (LB ; RS 952.0).

15 Code pénal suisse du 21 décembre 1937 (CP ; RS 311).

16 Arrêt du Tribunal fédéral 2C_893/2015 du 16 février 2017 consid. 8.7.5.

17 Cf. notamment Liégeois (n. 11) ; Alexis Favre/Christian Lüscher : « Le Tribunal fédéral se trompe sur la volonté du législateur », Le Temps, article publié le 15 mars 2017, disponible sous https ://www.letemps.ch/suisse/2017/03/15/christian-luscher-tribunal-federal-se-trompe-volonte-legislateur (dernière consultation 14 décembre 2017).

2. Deuxième illustration : l'affaire HSBC / Falciani (ATF 143 II 224)

[Rz 11] En 2014, la Direction générale des finances publiques françaises avait adressé une demande d'assistance administrative à la Suisse portant sur un couple de contribuables résidents en France soupçonné de détenir un compte bancaire non déclaré auprès d'une banque en Suisse. Bien que les autorités françaises aient découvert le nom du couple dans les données volées par Hervé Falciani, l'AFC avait accordé l'assistance administrative à la France. Comme dans l'affaire UBS précitée, le Tribunal administratif fédéral[18] avait annulé cette décision, mais cette fois-ci sans que le Tribunal fédéral ne remette en cause cette appréciation[19].

[Rz 12] Contrairement à l'affaire jugée dans l'arrêt ATF 143 II 202, la demande d'assistance administrative se fondait sur des renseignements obtenus en violation du principe de la bonne foi par des actes effectivement punissables au regard du droit suisse. D'une part, les données avaient été volées à Genève et non pas dans une filiale étrangère ; d'autre part, ces actes relevaient de la compétence des autorités de poursuite pénale suisse. La punissabilite des actes etait d'autant moins contestable apres la condamnation d'Herve Falciani par le Tribunal pénal fédéral à une peine privative de liberté de cinq ans pour tentative de service de renseignements économiques aggravé (art. 273 al. 2 et 3 CP)[20]. Il était également relevé par le Tribunal fédéral qu'au cours des négociations entre la Suisse et la France concernant un Avenant à la convention fiscale franco-suisse signé le 27 août 2009, que la France a confirmé à la Suisse « *l'assurance qu'aucune des données dérobées à la filiale genevoise de la banque HSBC ne sera*[it] *utilisée dans le cadre de la demande d'assistance administrative* »[21]. Reposant sur les données volées par Hervé Falciani, cette demande se heurtait ainsi à la confiance légitime que la Suisse pouvait avoir dans l'engagement de la France à ne pas procéder à une demande d'assistance administrative.

B. Risques pour les banques

[Rz 13] Une fuite de données présente pour les établissements bancaires différents risques opérationnels. Outre le risque commercial et le risque de réputation (cf. infra **1.**), la banque sera exposée à différents risques, en particulier un risque réglementaire (cf. infra **2.**), un risque de responsabilité pénale (cf. infra **3.**) ou encore un risque de responsabilité civile (cf. infra **4.**). Ces risques sont brièvement exposés ci-dessous.

1. Risque commercial et risque de réputation

[Rz 14] Toute publicité liée à une fuite de données est évidement néfaste et met à mal la confiance que les clients peuvent placer dans leur établissement. Selon la nature de la fuite, celle-ci est susceptible de générer une publicite négative mettant en lumière certaines défaillances de sécurité.

---

18 Cf. arrêt du Tribunal administratif fédéral A-6849/2014 du 22 octobre 2015.

19 Arrêt du Tribunal fédéral 2C_1000/2015 du 17 mars 2017 consid. 6.7 (publié au ATF 143 II 224).

20 Cf. arrêt du Tribunal pénal fédéral SK.2014.46 du 27 novembre 2015.

21 Arrêt du Tribunal fédéral 2C_1000/2015 du 17 mars 2017 consid. 6.5 ; cf. également, communiqué de presse du Département fédéral des finances du 12 février 2010, La Suisse et la France ont clarifié les questions fiscales restées ouvertes, disponible sous https ://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-31623.html (dernière consultation 11 décembre 2017).

[Rz 15] À la fuite de données peut ainsi succéder une diminution de nouveaux apports, voire une fuite des capitaux. Si le préjudice financier lié à la matérialisation d'un tel risque est difficilement chiffrable, il n'en demeure pas moins qu'elle impactera le volume des dépôts et, par voie de conséquence, les rendements de la banque.

2. Risque réglementaire

[Rz 16] De manière générale, toute banque doit se doter d'une organisation lui permettant, même en présence d'éléments criminels, de limiter les occasions de vol mais également l'étendue quantitative et qualitative d'une éventuelle soustraction[22]. Une fuite de données peut mettre en lumière certaines *carences organisationnelles* de l'établissement assujetti (art. 3 al. 2 let. a LB), et révéler un manquement à la garantie d'une activité irréprochable (art. 3 al. 2 let. c LB).

[Rz 17] Le fonctionnement et la sécurité du système informatique constituent typiquement un risque opérationnel[23/24]. En tant qu'élément essentiel de l'organisation administrative d'une banque, l'organisation du secteur informatique est une condition à l'autorisation d'exercer une activité bancaire[25]. Une fuite de données peut ainsi faire apparaître une *déficience de l'organisation informatique* de la banque procédant d'une violation du droit de la surveillance.

[Rz 18] Par ailleurs, une fuite de données soulève différents problèmes sous l'angle de la législation en matière de traitement des données, qui concrétise également le secret bancaire[26]. L'art. 7 al. 1 de la Loi fédérale sur la protection des données (LPD)[27] prévoit notamment que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées[28]. Ces mesures concrétisent le principe de la sécurité des données qui englobe l'intégrité, la disponibilité et la confidentialité des données[29]. À la violation des règles contenues dans la LPD peut ainsi s'ajouter une violation du droit de la surveillance, exposant la banque à se voir reprocher une déficience dans son organisation ou un manquement à l'obligation de la garantie d'une activité irréprochable[30].

[Rz 19] Ainsi qu'il le sera exposé ci-après (cf. infra 4.), une violation de l'obligation de discrétion du banquier procède en principe également d'une violation des obligations contractuelles. Or,

---

22 Bulletin FINMA 4/2013, p. 68 ss, 77.

23 Bulletin FINMA 4/2013, p. 68 ss, 75. La Circ.-FINMA 08/21 « *Risques opérationnels – banques* » du 20 novembre 2008 révisée le 22 septembre 2016 (ci-après « Circ.-FINMA 08/21 ») définit les risques opérationnels comme étant « *le risque de pertes provenant de l'inadéquation ou de la défaillance de procédures internes, de personnes, de systèmes ou suite à des évènements externes* » (Cm. 2). L'Annexe 3 Circ.-FINMA 08/21 énonce certains principes en cas de risque d'incidents en relation avec la confidentialité de grandes quantités de données de clients par le biais de l'utilisation de systèmes électroniques, et impose notamment de définir préalablement une stratégie de communication en cas d'incident de sécurité (cf. infra III. A. 2.2).

24 Rapport de gestion CFB 2004, p. 53.

25 Ainsi, les banques doivent se doter d'un concept de gestion des risques en lien avec les « *cyberrisques* » (cf. Cm. 135.6 Circ.-FINMA 08/21).

26 Werner Wyss, Datenschutz im Finanzwesen, in : Nicolas Passadelis / David Rosenthal / Thür Hanspeter (édit.), Datenschutzrecht, Bâle (Helbing Lichtenhahn) 2015, p. 356 N 11.4 et références citées.

27 Loi fédérale sur la protection des données du 19 juin 1992 (LPD ; RS 235.1).

28 Matthias Ebneter, Informationspflichten im Zusammenhang mit «Data Security Breaches», in : Jusletter 7 juin 2010, Rz 15.

29 Christa Stamm-Pfister, in : Urs Maurer-Lambrou/Gabor-Paul Blechta (édit.), Basler Kommentar, Datenschutzgesetz Öffentlichkeitsgesetz, 3e éd., Bâle (Helbing Lichtenhahn) 2014, N 7 ad art. 7 LPD.

30 Wyss (n. 26), p. 357 N 11.5 ; cf. ég. David Rosenthal, in : David Rosenthal/Yvonne Jöhri (édit.), Handkommentar zum Datenschutzgesetz, Zurich, Bâle, Genève (Schulthess) 2008, N 13 ad art. 12 LPD.

bien qu'elle ne soit pas compétente pour apprécier et exécuter d'éventuels litiges de droit privé, la FINMA considère dans sa pratique que l'exigence prudentielle de la garantie d'une activité irréprochable indique le respect rigoureux des obligations civiles[31]. Cette appréciation ne semble du reste pas contestée par la doctrine, à tout le moins en cas de *violations qualifiées d'obligations contractuelles*[32].

[Rz 20] Enfin, une fuite de données rendue publique peut mettre en lumière l'existence de certaines relations bancaires pouvant intéresser l'autorité de surveillance et susciter des questions de sa part, voire l'ouverture d'une procédure d'*enforcement*. À la suite des révélations des *Panama papers*, la FINMA a ainsi procédé à des clarifications auprès de 30 banques suisses. Ces procédures ont conduit la FINMA à ordonner des mesures destinées à améliorer le dispositif anti-blanchiment des banques concernées. Dans ce contexte, la FINMA a rendu à l'encontre de Gazprombank (Suisse) SA une décision constatant de graves lacunes dans le dispositif de prévention du blanchiment d'argent et lui a même interdit jusqu'à nouvel ordre d'accepter de nouveaux clients privés[33].

3. Risque de responsabilité pénale

[Rz 21] Lorsque la fuite de données résulte d'un vol commis par un employé de la banque, celui-ci sera exposé en première ligne à des poursuites pénales. L'éventail d'infractions pouvant être commises par le responsable d'une fuite dans un tel contexte s'étendant de la soustraction de données (art. 143 CP), l'accès indu à un système informatique (art. 143bis CP), la violation d'un secret commercial (art. 162 CP), le service de renseignements économiques (art. 273 CP) et la violation du secret bancaire (art. 47 LB). C'est en réalité dans les cas où l'auteur de la fuite ne peut pas être identifié qu'une éventuelle responsabilité pénale de la banque pourrait entrer en ligne de compte.

[Rz 22] Dans des circonstances exceptionnelles, une fuite de données pourra engager la responsabilité pénale (subsidiaire) de la banque du chef de violation du secret bancaire (art. 102 al. 1 CP[34]). Selon cette disposition, la responsabilité pénale d'une entreprise peut être mise en œuvre si à la suite d'un manque d'organisation de l'entreprise, un crime ou un délit est commis en son sein dans l'exercice d'activités commerciales conformes à son but, s'il ne peut être imputé à aucune personne physique. Dans le régime de l'art. 102 al. 1 CP, le manque d'organisation n'est pas causal pour la commission de l'infraction mais pour la non-identification de l'auteur[35]. Partant,

---

31 Communication FINMA 41 (2012), Rétrocessions – mesures prudentielles, du 26 novembre 2012, p. 5, disponible sous https ://www.finma.ch/fr/recherche/#query=R%C3%A9trocessions%20mesures%20prudentielles&Order=4 (dernière consultation 11 décembre 2017).

32 Beat Kleiner/Renate Schwob, in : Dieter Zobl/Renate Schwob/Rolf H. Weber/Christoph Winzeler/Christine Kaufmann/Stefan Kramer (édit.), Kommentar zum Bundesgesetz über die Banken und Sparkassen vom 8 November 1934 sowie zu der Verordnung vom 17. Mai 1972 und der Vollziehungsverordnung vom 30. August 1961, Zurich (Schulthess) 2015 (Ausgabe Oktober 2009 und April 2005), N 172 ad art. 3 LB.

33 Communiqué de presse de la FINMA, la FINMA achève la procédure concernant les « Panama papers » à l'encontre de Gazprombank Suisse, disponible sous https ://www.finma.ch/fr/news/2018/02/20180201-mm-gazprombank-schweiz/ (dernière consultation 1er février 2018).

34 La banque pourra également être recherchée si l'enquête rendrait nécessaire à l'égard des personnes punissables des mesures d'instruction hors de proportion par rapport à la peine encourue et que l'amende entrant en ligne de compte ne dépasse pas 50'000 francs (art. 49 de la loi fédérale sur l'Autorité fédérale de surveillance des marchés financiers du 22 juin 2007, LFINMA ; RS 956.1).

35 Ursula Cassani, Responsabilité(s) pénale(s) dans l'entreprise, in : Christine Chappuis/Bénédict Winiger (édit.), Responsabilité civile – Responsabilité pénale, Genève (Schulthess), p. 103 ss, 120.

la banque aura tout intérêt, afin de limiter tout risque pénal, à instaurer des dispositifs de *tracing* adéquats tels que la tenue de fichiers-journaux afin de permettre l'identification des utilisateurs ayant accès à une grande quantité ou à des données sensibles, conformément à ses obligations prudentielles[36].

4. Risque de responsabilité civile

[Rz 23] *Sur le plan contractuel*, une fuite de données constitue en principe une violation de l'obligation de discrétion[37], pouvant donner lieu à des prétentions en dommages-intérêts[38]. Ce sera en particulier le cas si la fuite a été commise par un employé indélicat dans l'accomplissement de son travail (cf. art. 101 al. 1 du Code des obligations ; CO).

[Rz 24] *Sous l'angle de la protection des données*, la violation de la sécurité des données peut également entraîner une perte de contrôle de la personne concernée sur ses données voire une utilisation abusive de celles-ci, et engendrer une atteinte à la personnalité de la personne concernée par la divulgation d'informations que celle-ci souhaitait garder secrètes[39]. Notamment, lorsque l'atteinte résulte d'une violation du principe de la bonne foi (art. 4 al. 2 LPD) ou d'une défaillance de sécurité (art. 7 al. 1 LPD ; art. 8–12 de l'Ordonnance relative à la loi fédérale sur la protection des données ; OLPD[40]), celle-ci est illicite au sens de l'art. 12 al. 1 LPD[41]. De même, la violation du secret bancaire doit être considérée comme une atteinte illicite à la personnalité même si les conditions de l'art. 12 al. 2 LPD ne sont pas réunies[42]. Une fuite pourra ainsi donner lieu à une action sur la base des art. 28, 28*a* et 28 du Code civil suisse (CC) (art. 15 al. 1 LPD), y compris une action en dommages-intérêts et en réparation du tort moral (cf. art 28*a* al. 3 CC), notamment en lien avec d'éventuels frais engagés pour faire supprimer des données communiquées à un tiers[43].

[Rz 25] *Sur le plan délictuel*, les actes mal intentionnés d'un organe ou d'un auxiliaire de la banque pourront être imputés à celle-ci aux conditions de l'art. 55 al. 3 CC, respectivement de l'art. 55 al. 1 CO. Lorsque l'acte délictuel a été commis par un auxiliaire, notamment un employé, de la banque, celle-ci pourra tenter de se disculper en démontrant avoir pris tous les soins commandés par les circonstances pour éviter que la fuite de données ne se produise, ou encore, que sa diligence n'eût pas empêché le dommage de se produire (art. 55 al. 1 in fine CO). Cette preuve devrait à notre sens pouvoir être apportée par la banque qui a strictement suivi ses obligations prudentielles, notamment en implémentant un système efficace d'autorisation fondé sur les fonctions et

36 Cf. Cm. 35 Annexe 3 Circ.-FINMA 08/21.

37 Daniel Guggenheim/Anath Guggenheim, Les contrats de la pratique bancaire, 5e éd., Berne (Stämplfi) 2014, p. 100 n° 270 ; Carlo Lombardini, Droit bancaire suisse, 2e éd., Zurich, Bâle, Genève (Schulthess) 2008, p. 985 N 74.

38 ATF 104 II 199 ; Maurice Aubert/Pierre-André Béguin/Paolo Bernasconi/Johanna Graziano-Von Burg/Renate Schwob/Raphaël Treuillaud, Le secret bancaire suisse, 3e éd., Berne (Stämpfli) 1995, p. 70.

39 Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, p. 119 (ci-après « Message LPD ») FF 2017 6565.

40 Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (OLPD ; RS 235.11).

41 L'art. 12 al. 2 LPD facilite la preuve de l'atteinte à la personnalité en prévoyant notamment que personne n'est en droit de traiter des données personnelles en violation des principes définis aux art. 4, 5 al. 1 et 7 al. 1 (art. 12 al. 2 let. a LPD). Le P-LPD reprend pour l'essentiel les dispositions actuelles en matière d'atteintes à la personnalité moyennant quelques modifications rédactionnelles (cf. art. 26 P-LPD).

42 Philippe Meier, Protection des données, Berne (Stämpfli) 2011, N 1536.

43 Pour une liste exemplative : cf. Meier (n. 42), N 1783, en particulier 4ème tiret.

les rôles des collaborateurs et des tiers afin que ceux-ci aient accès uniquement aux informations et aux fonctionnalités nécessaires à l'exercice de leurs tâches[44].

[Rz 26] Toutefois, quel que soit le chef de responsabilité choisi, la victime de la fuite faisant valoir des prétentions en dommages-intérêts à l'encontre de la banque devra, pour que celles-ci soient couronnées de succès, apporter la preuve de son dommage et faire la démonstration d'un lien de causalité entre celui-ci et la violation reprochée. Une telle démonstration sera généralement très difficile à effectuer[45/46].

[Rz 27] Notamment, en cas de livraison de données bancaires aux autorités fiscales, le préjudice que le client subirait du fait d'une taxation d'arriérés d'impôts, d'une peine pécuniaire ou d'une majoration fiscale, en d'autres termes un « *dommage fiscal* » ne constituera en principe pas un dommage réparable. En effet, en matière de responsabilité, lorsque le dommage consiste en une augmentation du passif, le dommage survient à la naissance de la dette et non au moment du paiement de celle-ci[47]. Partant, un dommage fiscal constitue une augmentation du passif et naît dès le moment où naît dans le patrimoine du contribuable, de par la loi, une dette d'impôts envers la collectivité publique et non pas au moment où celui-ci s'acquitte de cette dette[48]. Ainsi, si la fuite des données a pour conséquence de provoquer une décision de taxation qui aurait dû être prononcée aux termes de la loi, le contribuable ne pourra se retourner contre la banque pour la réparation de ce dommage.

[Rz 28] Concernant en particulier l'amende fiscale, le Tribunal fédéral considère que le caractère strictement personnel de l'amende constitue un obstacle à la réparation de ce dommage par le biais d'une action en responsabilité[49]. Bien qu'en principe l'amende fiscale ne soit pas indemnisable, on peut se demander si une annonce tardive ou une omission de la banque d'informer le client entrainant des pénalités fiscales évitables peut déboucher à une indemnisation. Selon Vito Roberto, la violation contractuelle ne résulterait ainsi pas de la fuite de données mais d'une violation d'informer le client en temps utile[50]. Dans un tel cas de figure, le dommage représenterait la différence entre le montant des pénalités effectives et le montant des pénalités si le client avait ete averti en temps utile, permettant a celui-ci de regulariser sa situation[51]. Cependant, même si l'on admettait que le client aurait pu éviter ou limiter des pénalités en raison d'une auto-dénonciation grâce à la réactivité de la banque en informant son client, celui-ci supporte une certaine responsabilité personnelle et devrait prouver que, nonobstant les indications contenues dans la presse,

44 Cm. 21 s. Annexe 3 Circ.-FINMA 08/21 ; cf. infra III. A. 2.2.

45 Meier (n. 42), N 1783, et la réf. citée.

46 En matière de violation du secret bancaire, certains auteurs citent ainsi l'exemple où un client, craignant qu'un tiers communique ses données à des autorités fiscales étrangères, décide pour échapper à une peine privative de liberté, de ne plus retourner dans son pays de domicile et de vendre tous ses biens non transférables (immeubles, etc.) à des conditions défavorables. Pour être réparable, le client devra ainsi prouver qu'il existe un risque concret de dénonciation, que ce risque peut avoir de lourdes conséquences pour lui, que ce risque est bien la cause de la vente de ses biens et que la vente a effectivement été réalisée à des conditions défavorables (cf. Aubert/Béguin/Bernasconi/Graziano-Von Burg/Schwob/Treuillaud [n. 38], p. 90).

47 Benoît Chappuis, La responsabilité contractuelle du conseiller fiscal, in : Pascal Pichonnaz/Franz Werro (édit.), La pratique contractuelle 4, Symposium en droit des contrats, Genève, Zurich, Bâle (Schulthess) 2015, p. 165 ss, 189.

48 *Ibidem*.

49 ATF 115 II 72 consid. 3b, in : JdT 1989 I 349 ; arrêt du Tribunal fédéral 4C.3/2007 du 12 novembre 2007 ; ATF 134 III 59, in : SJ 2008 I p. 169 ss.

50 Vito Roberto, Informationspflichten der Bank bei «Datenleaks», in : Susan Emmenegger (édit.), Bankvertragsrecht, Schweizerische Bankrechtstagung 2017, Bâle (Helbing Lichtenhahn) 2017, p. 105 ss, 129.

51 Roberto (n. 50), p. 129.

les informations supplémentaires qu'il aurait obtenues de la part de la banque auraient changé sa décision[52]. Par ailleurs, le fait de considérer ces pénalités comme étant un dommage réparable serait contraire au but punitif et au caractère strictement personnel d'une telle peine. Dans un arrêt de 2007, le Tribunal fédéral avait laissé ouverte la possibilité d'admettre certaines exceptions au caractère non indemnisable des amendes fiscales, notamment lorsqu'un conseiller fiscal qui, par un comportement fautif, avait privé le contribuable de la faculté de se dénoncer spontanément et d'obtenir une réduction de l'amende ou amène son client à commettre un délit fiscal faute d'information suffisante[53]. Dans une affaire recente, le Tribunal fédéral a toutefois considere qu'une telle exception n'est pas admise lorsque le contribuable assume un risque en toute connaissance de cause et qu'il devait savoir, indépendamment des informations reçues de son mandataire, qu'il se trouvait en infraction avec la loi fiscale[54]. Ainsi, un client ne saurait reprocher à sa banque de ne pas l'avoir informé d'un vol de données et partant de l'avoir empêché de se mettre spontanément au bénéficie d'une amnistie, dans la mesure où il savait pertinemment que sa situation n'était pas conforme sur le plan fiscal[55].

[Rz 29] La responsabilité civile de la banque en raison de fuite fautive de données ne semble avoir que peu occupé les tribunaux, sous réserve d'une affaire actuellement pendante devant le Tribunal de première instance de Genève, opposant notamment HSBC à l'un de ses anciens clients touché par le vol des données commis par Hervé Falciani en 2006/2007[56/57]. Le caractère non réparable du dommage fiscal, les difficultés liées à la démonstration d'un dommage et du lien de causalité, ainsi qu'une certaine volonté de discrétion, expliquent sans doute le peu d'appétit des clients victimes de vol de données pour d'éventuelles démarches sur le plan civil.

III. Devoirs d'information

[Rz 30] Les clients n'ont en principe pas connaissance avant la banque de la survenance d'un incident de sécurité. Toutefois, lorsque la fuite de données fait l'objet d'une remise à des autorités étrangères, les clients sont très rapidement avertis par les médias. L'expérience montre que les autorités étrangères s'empressent généralement de rendre publique la fuite de données, sans divulguer d'informations sur les clients concernés, afin de maintenir le plus grand nombre de clients potentiellement touchés dans un certain flou et ainsi augmenter les chances d'auto-dénonciation, y compris de la part des clients dont les données n'ont pas fuitées[58]. Dans ce contexte, le devoir d'information de la banque revêt un aspect essentiel.

---

52 Roberto (n. 50), p. 130 s.

53 Arrêt du Tribunal fédéral 4C.3/2007 du 12 novembre 2007 (ATF 134 III 59) consid. 2.3.3 et 2.3.4, in : SJ 2008 I p. 169 ss et références citées.

54 Arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017 consid. 4.6, in : SJ 2017 I 454.

55 Arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017, in : SJ 2017 I 454.

56 Dejan Nikolic, Contre HSBC et Falciani, pour l'honneur et pour des millions, Le Temps, article publié le 29 septembre 2017, disponible sous https ://www.letemps.ch/economie/2017/09/29/contre-hsbc-falciani-lhonneur-millions (dernière consultation 14 décembre 2017).

57 Les juridictions tessinoises puis le Tribunal fédéral ont également été saisis d'une action en responsabilité à l'encontre d'une banque, action intentée par des clients pour défaut d'information à la suite de la divulgation de la liste Falciani aux autorités fiscales italiennes (cf. arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017, in : SJ 2017 I 454, discuté infra III. A.3.).

58 Cf. Roberto (n. 50), p. 119 ss.

[Rz 31] Une présentation de tous les devoirs préventifs et réactifs de la banque en matière de lutte contre des fuites de données de ses clients excèderait le cadre de la présente contribution. Nous nous limiterons ainsi à présenter de manière générale les devoirs d'information de la banque consécutifs à une fuite de données, en distinguant d'une part l'information due aux clients concernés (cf. infra **A.**), et d'autre part, l'information aux autorités compétentes (cf. infra **B.**).

A. Information aux clients concernés

[Rz 32] Un devoir d'information de la banque envers ses clients en cas de perte accidentelle, falsification, vol, utilisation, copie, accès ou tout autre traitement non autorisé de données personnelles peut découler de trois sources distinctes, à savoir la réglementation en matière de protection des données (infra **1.**), la réglementation bancaire et financière (infra **2.**) et des dispositions de droit civil (infra **3.**). Après un examen de ces sources, nous exposerons brièvement de quelle manière l'information aux clients concernés doit en principe être mise en œuvre (infra **4.**).

1. Réglementation en matière de protection des données

1.1. Droit suisse

[Rz 33] Ni la loi sur la protection des données (LPD) ni l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) ne consacrent explicitement un devoir d'information en cas de perte accidentelle, falsification, vol, utilisation, copie, accès ou tout autre traitement non autorisé de données[59]. Un droit d'information est cependant régulièrement déduit de plusieurs principes généraux consacrés dans la LPD, à savoir le principe de la bonne foi (cf. infra **a)**) et le principe de sécurité des données et le principe de transparence (cf. infra **b)**).

[Rz 34] Enfin, il y a lieu d'exposer de quelle manière le devoir d'information devrait être concrétisé dans le cadre de la prochaine mouture de la loi sur la protection des données (cf. infra **c)**).

a) Le principe de la bonne foi

[Rz 35] Certains auteurs déduisent du principe de la bonne foi prévu à l'art. 4 al. 2 LPD un devoir d'information en faveur de la clientèle concernée ou, plus largement, du public et des autorités en cas de défaillance de sécurité dans son système d'information (perte, destruction ou vol de données à large échelle) ou de panne[60]. La jurisprudence déduit des règles de la bonne foi des obligations ou des devoirs accessoires non prévus par le contrat ou la loi, tel qu'un devoir d'information[61]. Lorsque l'existence d'un tel devoir accessoire est retenue, la violation de celui-ci entraine l'obligation de réparer le dommage subi par le cocontractant[62].

---

59 Cf. Ebneter (n. 28), p. 3.

60 Meier (n. 42), N 657 ; Bruno Baeriswyl, in : Bruno Baeriswyl/Kurt Pärli (édit.), Stämpflis Handkommentar, Datenschutzgesetz, Berne (Stämpfli) 2015, N 18 ad art. 4 LPD ; Rosenthal (n. 30), N 16 ad art. 4 LPD ; Astrid Epiney, in : Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (édit.), Datenschutzrecht, Berne (Stämpfli) 2011, § 9 N 22.

61 Christine Chappuis, in : Pascal Pichonnaz/Bénédict Foëx (édit.), Commentaire Romand, Code Civil I, Bâle (Helbing Lichtenhahn) 2010, N 19 ad art. 2 CC et références citées.

62 *Ibidem*.

[Rz 36] Sous l'angle du droit de la surveillance, l'obligation de respecter les règles de la bonne foi découle également des exigences d'une activité irréprochable[63]. En effet, en raison de la confiance sollicitée par les banques à leurs clients, en tant que fondement essentiel de leurs activités, le principe de la bonne foi constitue une importance primordiale et suppose pour les banques des exigences très élevées en la matière[64].

[Rz 37] Selon Philippe Meier, un devoir d'information s'impose en vertu du principe de la bonne foi lorsque le risque pour la personnalité est grave et que les données volées ou détruites représentent des données sensibles ou au moins délicates[65]. Si les données concernant le revenu et la fortune ne figurent pas dans la liste exhaustive de l'art. 3 let. c LPD et ne sont pas considérées comme des données sensibles, elles constituent néanmoins des données délicates[66] dont la fuite nécessite une information aux clients concernés. Une information de la fuite de données aux clients de la banque s'imposera généralement en vertu du principe de bonne foi, si la fuite présente un grave risque pour les clients.

b) Le principe de sécurité des données et le principe de transparence

[Rz 38] L'obligation d'informer les personnes concernées en cas de perte ou de destruction de données découle également du principe de la sécurité des données prévu à l'art. 7 LPD et 8 ss OLPD[67]. La sécurité des données régit les mesures qui doivent être prises pour que des personnes non autorisées n'aient pas accès aux données en question[68]. Les mesures devant être prises sont d'ordre organisationnel (p. ex. procédure d'identification et d'accès pour consulter, modifier ou copier des données déterminées) et technique (p. ex. sécurité informatique), qui combinées permettent d'éviter la destruction et la perte des données ainsi que les accès non autorisés[69].

[Rz 39] L'obligation d'informer les personnes concernées peut en outre résulter du principe de transparence qui fonde, selon le Préposé, un devoir général d'information en vertu duquel la finalité et le nombre des données traitées des personnes concernées doivent faire l'objet d'une information claire et complète[70].

---

63 Christian Bovet/Anne Héritier Lachat, La garantie d'une activité irréprochable, in : Christian Bovet (édit.), Schweizerisches Bundesverwaltungsrecht, Band XV, Finanzmarktaufsicht/Surveillance des marchés financiers, Bâle (Helbing Lichtenhahn) 2016, p. 165 ss, N 386.

64 Bulletin CFB 45/2003, p. 164 ss, 171.

65 Meier (n. 42), N 657.

66 Meier (n. 42), N 478.

67 Ebneter (n. 28), N 11 ss ; Rosenthal (n. 30), N 16 ad art. 4 LPD.

68 Meier (n. 42), N 780.

69 Sébastien Fanti, Protection des données informatiques, in : Jean-Philippe Dunand/Pascal Mahon (édit.), La protection des données dans les relations de travail, Genève, Zurich, Bâle (Schulthess) 2017, p. 229 ss, 237 note 44.

70 Christian Bovet/Alexandre Richa, Protection des données et nouvelles procédures de communication aux autorités fiscales et de surveillance étrangères, in : SZW/RSDA 2/2017, p. 144 ss, 153, note 72, et références citées ; Note du Préposé fédéral à la protection des données et à la transparence à l'attention des banques sur la transmission de données personnelles aux autorités américaines du 20 juin 2013, disponible sous https ://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2013/06/merkblatt_fuer_bankenzuruebermittlungvonpersonendaten.pdf.download.pdf/note_a_l_attentiondesbanquessurlatransmissiondedonneespersonnell.pdf (dernière consultation 11 décembre 2017).

c) Projet de révision totale de la loi sur la protection des données

[Rz 40] Lors de sa séance du 15 septembre 2017, le Conseil fédéral a adopté un projet de révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales (P-LPD), lequel vise à renforcer la protection des données, « *au travers notamment d'une amélioration de la transparence des traitements et du contrôle que les personnes concernées peuvent exercer sur leurs données* »[71/72].

[Rz 41] Cette refonte de la LPD permet de créer les conditions nécessaires à la ratification de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE 108) du Conseil de l'Europe en cours de révision (ci-après « P-STE 108 »)[73] et à la reprise de la Directive européenne (UE) 680/2016 relative à la protection des données dans le cadre de poursuites pénales[74]. En outre, cette révision rapprochera le droit suisse sur la protection des données des exigences du Règlement (UE) 2016/679 (ci-après « RGPD »)[75], étape indispensable pour que l'Union européenne continue de reconnaître la Suisse comme un État tiers ayant un niveau de protection des données suffisant pour préserver la possibilité d'échanger des données avec les États membres de l'Union européenne[76].

[Rz 42] Contrairement aux textes en vigueur, le projet de la LPD énonce explicitement les conditions dont la réalisation entraîne pour le responsable du traitement une obligation de notification au Préposé[77] à laquelle peut s'ajouter une obligation d'annonce aux personnes concernées en tenant compte de l'utilité que peut avoir l'exécution de ces obligations[78].

[Rz 43] Le projet de révision de la loi sur la protection des données prévoit une obligation d'annonce à la personne concernée « *lorsque cela est nécessaire à sa protection ou lorsque le préposé l'exige* »[79]. Afin de déterminer si une annonce à la personne concernée doit être effectuée, il convient de se demander si l'information peut réduire les risques pour la personnalité et les droits fondamentaux de celle-ci en lui permettant de prendre les dispositions nécessaires pour se

71 Message LPD (n. 39), p. 3.

72 Selon un communiqué du 12 janvier 2018, la Commission des institutions politiques du Conseil national a adopté une motion demandant la scission du projet de révision. Elle opérera dans un premier temps les adaptations au droit européen qui s'imposent et dans un deuxième temps, elle procédera à la révision totale de la loi sur la protection des données (disponible sous https ://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-01-12.aspx ?lang=1036 [dernière consultation 23 janvier 2018]).

73 Projet disponible sous http ://www.coe.int/fr/web/data-protection/convention108/modernisation (dernière consultation 11 décembre 2017). Ce projet a pour objectifs d'harmoniser et de renforcer le niveau de protection des données au plan international et de faciliter les flux transfrontières de données entre les États parties à la Convention (Message LPD [n. 39], p. 53).

74 Directive (UE) 2016/680 du Parlement européen et du conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4 mai 2016, p. 89. Cette directive constitue pour la Suisse un développement de l'acquis de Schengen qui doit être repris dans sa législation (Message LPD [n. 39], p. 23, p. 25 et p. 49 s.).

75 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 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, et abrogeant la directive 94/46/CE, JO L 119 du 4 mai 2016, p. 1.

76 Message LPD (n. 39), p. 24.

77 Cf. infra B. 1.2.

78 Ces obligations implémentent les exigences fixées par l'art. 7 par. 2 P-STE 108 (n. 73) et aux art. 30 s. Directive (UE) 2016/680.

79 Cf. art. 22 al. 4 P-LPD.

protéger[80]. Ainsi, le but de l'information donnée aux clients est de leur permettre d'entreprendre des mesures nécessaires afin de se protéger ou réduire l'atteinte à leur personnalité de toute autre manière[81]. Selon le projet, le responsable du traitement devrait toutefois restreindre, différer ou renoncer à informer la personne concernée dans certains cas spécifiques[82].

[Rz 44] En matière de fuite de données bancaires, le projet de révision ne dispensera pas la banque d'évaluer l'utilité qu'une communication, en principe individualisée, pourrait avoir pour les clients concernés, notamment eu égard à des mesures protectrices qu'ils pourraient concrètement prendre en l'espèce. Si une telle utilité apparaîtra d'une manière évidente en cas de vol de données, tel ne sera pas forcément le cas si des données ont été accidentellement rendues provisoirement accessibles par un tiers ne présentant pas de risque de contagion (p. ex. une autre banque). En cas de doute, la banque devrait toutefois privilégier une communication aux personnes concernées (« *in dubio pro informatio* »).

1.2. Droit étranger : l'exemple du droit européen

[Rz 45] De manière générale, les banques doivent déterminer, limiter et contrôler les risques juridiques, ainsi que les risques susceptibles de ternir leur réputation[83]. S'agissant des risques juridiques transfrontières, ces obligations ont été pour la première fois concrétisées dans la prise de position de la FINMA du 22 octobre 2010, intitulée « *Position de la FINMA à propos des risques juridiques et de réputation dans le cadre des activités transfrontières* »[84], et sont aujourd'hui intégrées dans Circulaire 2008/21 « *Risques opérationnels – banques* » remaniée[85]. Cette obligation de contrôle des risques impose aux banques une obligation de s'assurer de la conformité avec la réglementation étrangère en matière de protection des données.

---

80 Message LPD (n. 39), p. 120.

81 Ebneter (n. 28), N 3 ; Meier (n. 42), N 658.

82 Tout d'abord, ce devoir d'information sera limité lorsque des intérêts prépondérants d'un tiers l'exigent (art. 22 al. 5, let. a et 24, al. 2 let. b P-LPD), le responsable du traitement est un organe fédéral (art. 22 al. 5 let. a et 24, al. 2 let. b P-LPD) ou un devoir de garder le secret l'interdit (art. 22 al. 5 let. a P-LPD). De même, lorsque le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés pour identifier les personnes concernées, le responsable du traitement pourra renoncer à les informer (art. 22 al. 5 let. b P-LPD). On estime que l'information individuelle nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées alors que les coûts engendrés sembleraient excessifs par rapport aux gains qu'en retireraient les personnes concernées (cf. Message LPD [n. 39], p. 121). Une limitation de l'information peut également intervenir lorsque l'information de la personne concernée peut être garantie de manière équivalente par une communication publique (art. 22 al. 5 let. c P-LPD).

83 Pour les titulaires d'autorisations en matière de placements collectifs : cf. art. 12a al. 2 de l'Ordonnance sur les placements collectifs de capitaux du 22 novembre 2006 (OPCC ; RS 951.311).

84 Pour une présentation de cette position, cf. Alexandre Richa, Gestion des risques transfrontières : la Circulaire de la FINMA qui ne dit pas son nom, in : Regards de marathoniens sur le droit suisse, Genève (Slatkine) 2015.

85 La circulaire prévoit ainsi que « [q]*uand des établissements ou leurs filiales fournissent des services financiers ou de distribution de produits financiers dans le cadre d'opérations transfrontières, les risques résultant d'une application des législations étrangères (droit fiscal, droit pénal, législation en matière de blanchiment d'argent, etc.) doivent également être identifiés, limités et contrôlés de façon appropriée. En tant qu'autorité de surveillance, la FINMA s'attend en particulier à ce que les banques respectent le droit étranger de la surveillance* » (Cf. Circ.-FINMA 08/21, Cm. 136.2).

[Rz 46] Notamment, les banques suisses sont susceptibles d'être soumises au RGPD[86] qui dispose d'un champ d'application territorial étendu[87]. Tout d'abord, seront soumises à la nouvelle législation européenne, les banques suisses disposant d'un établissement au sein de l'UE, qui au cours de leurs activités effectuent un traitement de données, que le traitement ait lieu ou non dans l'UE[88]. En cas de sous-traitance, si le sous-traitant est localisé dans l'Union européenne, l'ensemble du traitement ainsi que les modalités de la délégation seront aussi soumis au RGPD. Le champ d'application territorial sera également rempli lorsque la banque suisse ou son sous-traitant, sans être présent sur le territoire de l'UE, met en œuvre des traitements liés à l'offre de biens ou de services aux résidents européens[89]. L'entreprise doit cependant envisager d'offrir des biens ou des services dans un ou plusieurs États de l'UE. Une telle intention ne saurait être déduite que d'une simple accessibilité d'un site Internet, d'une adresse électronique ou d'autres coordonnées, mais d'un faisceau d'indices (affichage de prix en euros, utilisation de plusieurs langues, modalités de livraison spécifiques, mention de clients ou d'utilisateurs de l'UE[90]). Enfin, seront aussi concernées les entreprises suisses suivant le comportement de personnes (profilage) se trouvant sur le territoire de l'UE, dans la mesure où il s'agit d'un comportement qui a lieu au sein du même territoire[91].

[Rz 47] Au même titre que le droit suisse, le droit européen prévoit une obligation d'annonce à la personne concernée si la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique[92]. Une violation de données à caractère personnel est définie comme une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données[93]. Cette définition englobe tant la panne et la fuite de données que le piratage informatique[94]. Un risque est réputé être élevé pour les droits et libertés de la personne concernée lorsque la violation de données à caractère personnel peut causer un dommage physique, matériel ou non matériel, tel que notamment un préjudice moral, une perte financière, une atteinte à la réputation ou une perte de confidentialité de données protégées par le secret profes-

86 Le RGPD (Règlement général sur la protection des données) est en vigueur depuis le 24 mai 2016, mais il sera directement applicable à partir du 25 mai 2018 (art. 99 RGPD), sans nécessiter de transposition dans les différents États membres.

87 Pour une présentation détaillée, cf. Préposé fédéral à la protection des données et à la transparence PFPDT, Le RGPD et ses conséquences sur la Suisse (décembre 2017), disponible sous https ://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/VODSG%20EU.pdf.download.pdf/Le%20RGPD%20et%20ses%20conséquences%20sur%20la%20Suisse_FR.pdf (dernière consultation 14 décembre 2017).

88 Cf. art. 3 par. 1 RGPD.

89 Cf. art. 3 par. 2, let. a RGPD.

90 Note marginale N 23 RGPD.

91 Cf. art. 3 par. 2 let. b RGPD.

92 Cf. art. 34 par. 1 RGPD.

93 Cf. art. 4 par. 12 RGPD.

94 Nicole Beranek Zanon, Melde- und Benachrichtigungspflichten nach EU DSGVO + rev. DSG, in : Jusletter 2 octobre 2017 Rz 2.

sionnel[95]. Les pertes concernant des données financières constituent notamment un risque élevé pour les droits et libertés de la personne concernée[96].

[Rz 48] La communication à la personne concernée doit intervenir dans les meilleurs délais et en des termes clairs et simples afin de permettre à celle-ci de prendre les précautions qui s'imposent. La communication doit au moins indiquer la nature de la violation, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact, une description des conséquences probables de la violation et une description des mesures prises ou proposées par le responsable du traitement pour remédier à la violation ou pour atténuer les éventuelles conséquences négatives[97]. Le responsable du traitement doit choisir le moyen de communication qui maximise les chances de contacter effectivement les personnes concernées[98]. La notification pourra par exemple intervenir par voie électronique (email ou SMS), par une annonce ou une notification sur le site Internet du responsable du traitement, par une communication postale ou par une annonce dans la presse[99]. Si les personnes concernées peuvent être informées de manière tout aussi efficace et qu'une communication individuelle exige des efforts disproportionnés, une communication publique sera privilégiée[100]. Le responsable du traitement peut toutefois renoncer à effectuer toute annonce lorsque des mesures techniques et organisationnelles ont été appliquées aux données affectées par la violation, rendant les données incompréhensibles pour des personnes tierces, telles que le chiffrement[101] ou lorsque le responsable du traitement a pris des mesures immédiates afin de supprimer les risques encourus par les personnes concernées[102]. Enfin, le responsable du traitement est tenu de conserver une trace documentée de chaque violation indiquant son contexte, ses effets et les mesures prises pour y remédier[103].

[Rz 49] Ainsi, à l'instar de ce qui prévaut en droit suisse, une communication aux clients concernés présuppose une pesée des intérêts en présence et une appréciation de l'utilité qu'une telle communication pourrait avoir pour les clients concernés.

2. Réglementation bancaire et financière

[Rz 50] De manière générale, la législation bancaire suisse ne contient aucune disposition spécifique relative à une obligation d'informer les clients en cas de perte accidentelle, falsification, vol, utilisation, copie, accès ou tout autre traitement non autorisé de données les concernant[104].

---

95 Cf. note marginale N 75 RGPD ; Guidelines on Personal data breach notification under Regulation 2016/679 du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel du 3 octobre 2017 (ci-après « Guidelines on Personal data breach notification under Regulation 2016/679 »), p. 20, disponible sous http ://ec.europa.eu/newsroom/just/item-detail.cfm ?item_id=50083 (dernière consultation 11 décembre 2017).

96 Dans le même sens, Guidelines on Personal data breach notification under Regulation 2016/679 (n. 95), p. 21.

97 Cf. art. 33 par. 3 let. b, c et d et art. 34 par. 2 RGPD.

98 Guidelines on Personal data breach notification under Regulation 2016/679 (n. 95), p. 18.

99 *Ibidem*.

100 Cf. art. 34 par. 3 let. c RGPD.

101 Cf. art. 34 par. 3 let. a RGPD.

102 Cf. art. 34 par. 3 let. b RGPD.

103 Cf. art. 33 par. 5 RGPD.

104 Le devoir d'information visé par l'Ordonnance de la FINMA du 8 septembre 2011 sur le traitement des données (OFTD ; RS 956.124) ne porte que sur la saisie de données dans le fichier de la FINMA sur les garanties d'une activité irréprochable, et ne traite pas spécifiquement de l'information à donner en cas de fuite desdites données, nonobstant le principe de sécurité visé par l'art. 4 OFTD.

[Rz 51] La loi fédérale sur l'Autorité fédérale de surveillance des marchés financiers (LFINMA) ne consacre pas non plus une telle obligation. Si l'art. 29 al. 2 LFINMA prévoit que les assujettis et leurs sociétés d'audits renseignent sans délai la FINMA sur tout fait important susceptible de l'intéresser[105], cette disposition ne fonde qu'une obligation de renseignement envers l'autorité de surveillance. Elle ne crée pas une obligation indépendante d'information vis-à-vis des clients concernés.

[Rz 52] Une telle obligation d'information vis-à-vis des clients est cependant susceptible d'être déduite de deux circulaires de la FINMA, à savoir la Circulaire Outsourcing[106], d'une part, et la Circulaire Risques Opérationnels, d'autre part. Bien que les circulaires de la FINMA ne constituent pas une source de droit indépendante, elles concrétisent des normes légales ouvertes et indéterminées et contiennent des instructions relatives au pouvoir d'appréciation[107]. Il y a donc lieu de s'y référer. Ainsi qu'on le verra ci-après, c'est véritablement la deuxième des circulaires précitées qui fonde une autre base à l'obligation d'information des banques en cas de perte de données.

2.1. Circulaire Outsourcing

[Rz 53] L'application de la Circulaire Outsourcing présuppose que des prestations de services essentielles à l'activité de la banque soient externalisées[108]. De manière générale, toutes les activités permettant à un tiers d'avoir accès aux données de clients tombent en principe dans le champ d'application de la Circulaire Outsourcing[109]. La Circulaire Outsourcing n'instaure pas explicitement un devoir d'information en cas de perte accidentelle, falsification, vol ou utilisation, copie, accès ou tout autre traitement non autorisé[110]. Elle ne prévoit pas non plus expressément un tel devoir en cas d'accès indu par une autre entreprise qui aurait également transféré des activités essentielles au même délégataire[111]. Cependant, la circulaire prévoit dans le cadre du principe n°6 « *Informations des clients* » que « [l]*es clients doivent être informés du transfert de données les concernant* »[112]. Si cette section vise avant tout un transfert de données avant la transmission des données au délégataire[113], on peut toutefois déduire du texte clair du Cm. 37 qu'un transfert accidentel de données, survenu dans le cadre d'une activité déléguée, implique également une information aux clients concernés.

---

105 Sur ce point cf. infra B. 3.

106 Circ.-FINMA 08/7 « *Outsourcing – banques* » du 20 novembre 2008 (ci-après « Circ.-FINMA 08/7 »). Cette circulaire sera remplacée dès le 1er avril 2018 par la Circ.-FINMA 18/3 « *Outsourcing – banques et assureurs* » du 21 septembre 2017 (ci-après « Circ.-FINMA 18/3 »).

107 Les circulaires établies par la FINMA font partie intégrante du droit suisse dans la mesure où elles sont publiées au Recueil systématique (cf. arrêt ACJC/1691/2016 de la Cour de justice de Genève du 2 décembre 2016, consid. 4.1.3, p. 20).

108 Au sens de la Circulaire Outsourcing sont « *essentielles* » les prestations de services qui peuvent en particulier avoir un effet sur la détermination, la limitation et le contrôle des risques de crédit et de pertes, des risques liés au marché, à l'exécution des transactions et au manque de liquidités, des risques opérationnels et juridiques, ainsi que des risques susceptibles de ternir sa réputation (Cm. 2 Circ.-FINMA 08/7). L'annexe à la Circulaire Outsourcing 08/7 énumère des exemples pratiques d'externalisations soumises à ladite circulaire et d'autres qui ne le sont pas.

109 Philipp Fischer, L'externalisation de services dans le domaine bancaire et financier, in : SZW/RSDA 2/2016, p. 137 ss, 138.

110 Cf. Cm. 31 Circ.-FINMA 08/7.

111 Cf. Cm. 36, *in fine* Circ.-FINMA 08/7.

112 Cm. 37 Circ.-FINMA 08/7.

113 Cf. Cm. 38, *ab initio*Circ.-FINMA 08/7 ; cf. ég. Fischer (n. 109), p. 138.

[Rz 54] Cela étant, il semble acquis que la Circulaire Outsourcing n'ait pas pour vocation première de protéger les intérêts des clients dans le cadre de fuite de données et qu'elle ne constitue qu'un fondement très subsidiaire par rapport à la législation en matière de protection des données. Du reste, la FINMA a pris acte du fait que les règles en matière de protection des données prévues par la Circulaire Outsourcing pouvaient faire un doublon inutile avec le droit suisse de la protection des données[114]. Partant, la section relative au principe n°6 de la Circulaire Outsourcing 08/7 a été radiée dans le cadre de la Circulaire 2018/3 « *Outsourcing – banques et assureurs* »[115].

2.2. Circulaire Risques Opérationnels

[Rz 55] La Circulaire Risques Opérationnels énonce à son annexe 3 les principes de bonne gestion des risques en lien avec la confidentialité des données électroniques des personnes physiques[116]. Les principes contenus dans cette annexe sont applicables en cas de risque d'incidents en relation avec la confidentialité de grandes quantités de données de clients par le biais de l'utilisation de systèmes électroniques[117]. Afin de préserver la confidentialité des données et de prévenir d'éventuels vols de données, la banque doit notamment mettre en place un système d'autorisation fondé sur les fonctions et les rôles des collaborateurs et des tiers afin que ceux-ci aient accès qu'aux informations et aux fonctionnalités nécessaires à l'exercice de leurs tâches (*need to know*)[118].

[Rz 56] La circulaire précise notamment que « *la banque doit disposer d'une stratégie de communication claire en cas d'incidents graves en lien avec la confidentialité des CID. Il convient notamment de définir la forme et le moment précis de la communication à la FINMA, aux autorités de poursuite pénale, aux clients concernés et aux médias* »[119]. Ces obligations ne créent toutefois pas en tant que telle une obligation d'informer indépendante. Au vu du Cm. 1 de la circulaire, elle concrétise les exigences découlant du droit de la surveillance, de la législation relative à la protection des données et du droit civil. On en déduit toutefois que la FINMA attend en pratique des banques que celles-ci informent leurs clients en cas d'incidents graves relatifs à la confidentialité des CID.

---

114 Le rapport explicatif relatif au projet de la Circ.-FINMA 18/3 (projet de circulaire 2017/xx « *Outsourcing – banques et assureurs* ») précise à cet égard ce qui suit (cf. § 4.4.5, 2ème para., p. 12) : « *Afin d'éviter des doublons et d'éventuelles divergences dans les développements du droit de la protection des données, et de garantir, parallèlement, une délimitation claire entre les exigences prudentielles de la surveillance des marchés financiers et les obligations ancrées dans le droit privé conformément à la loi sur la protection des données, les dispositions figurant jusqu'à présent dans la Circ.-FINMA 08/7 en lien avec la protection des données sont radiées (cf. les anciens Cm. 31 à 33, Cm. 36 et Cm. 37 à 39). Pour les mêmes raisons, l'ancien principe 6 (information des clients) sur lequel la Circ.-FINMA 08/7 allait au-delà des exigences relevant du droit de la protection des données, notamment sur les obligations d'information complètes et sur le droit de résiliation extraordinaire selon le Cm. 39 de la Circ.-FINMA 08/7, est supprimé* », disponible sous https ://www.finma.ch/fr/news/2016/12/20161206—mm—rs—outsourcing/ (dernière consultation 11 décembre 2017) ; Cf. également Rapport sur l'audition concernant le projet de circulaire FINMA 2018/3 « *Outsourcing – banques et assureurs* » du 21 septembre 2017, p. 32, disponible sous https ://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/rs-outsourcing/ab_rs18_03_20170921_de.pdf?la=fr (dernière consultation 11 décembre 2017).

115 Le projet de révision de la LPD concrétisera toutefois un devoir d'information à la charge du délégataire. En effet selon le projet, si la violation de la sécurité des données intervient auprès d'un sous-traitant, celui-ci devra annoncer cet incident dans les meilleurs délais au responsable du traitement (art. 22 al. 3 P-LPD) qui devra à son tour évaluer l'opportunité d'une annonce auprès du Préposé ou de la personne concernée.

116 Cf. Cm. 1 Annexe 3 Circ.-FINMA 08/21.

117 Cf. Cm. 1 Annexe 3 Circ.-FINMA 08/21.

118 Cf. Cm. 21 s. Annexe 3 Circ.-FINMA 08/21.

119 Cm. 46 Annexe 3 Circ.-FINMA 08/21.

Aussi, un devoir d'information de la banque est susceptible de découler également des exigences posées par l'Annexe 3 de la Circulaire Risques Opérationnels.

[Rz 57] Le Cm. 57 de l'Annexe 3 de la Circulaire Risques Opérationnels définit un incident grave relatif à la confidentialité des CID comme un « *incident relatif à la confidentialité des données de clients qui implique une fuite significative de CID (comparée au nombre total des comptes/à la taille totale du portefeuille* ». Le critère retenu semble donc essentiellement quantitatif. Il est toutefois vraisemblable qu'en pratique la FINMA apprécie cette notion également sur la base de critères qualitatifs, notamment l'étendue de la fuite. La situation n'est en effet pas la même si des données ont été transmises dans le cadre d'un *hacking* dont la banque aurait été victime ou si cette transmission s'est limitée à un ou plusieurs collaborateurs d'une banque tierce soumis (notamment) au secret bancaire (art. 47 LB)[120/121] suite à une erreur de manipulation informatique.

[Rz 58] En présence d'une fuite significative de données de clients, la Circulaire Risques Opérationnels oblige ainsi non seulement la banque concernée à satisfaire à ses obligations d'information, en particulier envers les clients concernés, mais de le faire sur la base d'une stratégie prédéfinie détaillant notamment les modalités de communication.

3. Aspects civils

[Rz 59] Un devoir d'informer les clients en cas de fuite ou de perte de données peut éventuellement découler des *obligations contractuelles* du responsable du traitement des données[122], en l'occurrence de la banque. En effet, le devoir d'information découle de l'obligation de fidélité du mandataire[123], laquelle est susceptible de s'appliquer même en cas de simples dépôts bancaires. En vertu de l'obligation d'information, le cocontractant doit aviser l'autre partie de tout ce qui est important pour cette dernière en relation avec le contrat[124/125].

[Rz 60] Par ailleurs, certains auteurs déduisent du principe général de l'obligation de réduire le dommage (*Obliegenheit zur Schadenminderung* ; art. 44 al. 1 CO), applicable à la responsabilité en matière contractuelle par renvoi de l'art. 99 al. 3 CO, un devoir d'information en cas de perte de données[126]. Cependant, le principe de l'obligation de réduire le dommage s'impose en principe à celui qui subit le dommage alors que le responsable aura seulement un intérêt à ne pas l'accroître. Nous sommes d'avis sur le plan dogmatique que l'obligation – ou plutôt l'incombance – de réduire le dommage ne saurait servir de fondement additionnel sur le plan civil à un devoir d'information.

---

120 Les employés de banque sont également soumis au secret bancaire selon l'art. 47 al. 1 let. a et al. 4 LB. La notion d'« *employé* » doit être appréhendée largement et inclut notamment « *tout personne ayant une activité dans une banque (apprentis, stagiaires rémunérés ou non, etc.), même s'ils exercent une activité seulement temporaire ou comme auxiliaires* » (Aubert/Béguin/Bernasconi/Graziano-Von Burg/Schwob/Treuillaud, [n. 38], p. 103).

121 L'obligation de discrétion du banquier porte sur tout ce qui lui est confié, de même que tout ce qu'il apprend dans l'exercice de sa profession (Aubert/Béguin/Bernasconi/Graziano-Von Burg/Schwob/Treuillaud [n. 38], p. 91 ss). Une information apprise accidentellement devrait par conséquent être couverte par le secret bancaire.

122 Du même avis : Rosenthal (n. 30), N 16 ad art. 4 LPD.

123 Franz Werro, in : Luc Thévenoz/Franz Werro (édit.), Commentaire Romand, Code des obligations I, 2e éd., Genève, Bâle, Munich (Helbing Lichtenhahn) 2012, N 16 ad art. 398 CO et références citées.

124 *Ibidem.*

125 Pour une analyse détaillée des sources du devoir d'information, cf. Roberto (n. 50), p. 111 ss.

126 Rosenthal (n. 30), N 16 ad art. 4 LPD ; Ebneter (n. 28), N 11 et 15.

[Rz 61] Enfin, selon le principe de l'interdiction de la création d'un état de fait dangereux (*Gefahrensatz*)[127], la personne qui expose autrui à un danger est tenue de prendre toutes les précautions propres à éviter qu'un dommage ne se produise[128]. Certains auteurs déduisent de ce principe un devoir d'information de la part du responsable du traitement afin que la personne concernée puisse prendre des mesures nécessaires[129].

[Rz 62] Le devoir d'information sous l'angle civil n'est toutefois pas absolu. Dans une récente contribution, Roberto examine différents cas de figure où la question d'une renonciation à l'information se pose de manière légitime[130], notamment (i) lorsque la personne concernée est déjà informée[131], (ii) lorsqu'elle ne compte plus parmi les clients de la banque et qu'elle n'est plus joignable[132], (iii) lorsqu'une information entre en conflit avec un devoir de réserve (*Tipping-Off-Verbot*) qui s'imposerait à la banque en vertu du droit étranger (*Pflichtenkollision*)[133] ou encore (iv) lorsque l'information aux clients peut mettre en lumière un comportement fautif (*Fehlverhalten*) de la banque[134].

[Rz 63] La nécessité d'informer les clients concernés par une fuite de données est principalement fonction de la nature de l'incident de sécurité, de l'étendue de la fuite et du cercle de personnes pouvant accéder aux données en question[135]. Dans les cas bénins ne présentant aucun risque pour les clients concernés, notamment aucun risque fiscal (cf. supra II. A.), la nécessité d'informer les clients concernés pourra notamment s'effacer devant l'opportunité de ne pas affoler inutilement les clients de la banque et ternir la confiance que ces derniers placent en celle-ci, la banque considérant le risque commercial et de réputation (cf. supra II. B. 1.) comme prépondérant par rapport aux risques réglementaire et civil précités (cf. supra II. B. 2. et 4.).

[Rz 64] Si la banque décide de renoncer à informer ses clients, le risque civil encouru par celle-ci serait relativement faible si l'on se réfère à un arrêt non publié du 29 juin 2017. Dans cette affaire, le Tribunal fédéral a refusé une demande d'indemnisation d'une cliente italienne qui a fait l'objet d'un redressement fiscal à la suite de la découverte de la liste Falciani par les autorités italiennes[136]. La cliente invoquait un dommage composé du montant d'impôts, des sanctions

127 Werro (n. 123), N 79 ad art. 41 CO et références citées.

128 ATF 126 III 113 consid. 2aa ; ATF 123 III 306 consid. 4 ; ATF 112 II 138 consid. 3.

129 Ebneter (n. 28), N 15.

130 Roberto (n. 50).

131 Roberto (n. 50), p. 119 ss.

132 Roberto (n. 50), p. 113 ss.

133 Roberto (n. 50), p.121 ss. Cet auteur distingue les clients dont les avoirs sont fiscalisés des clients dont les avoirs ne le sont pas, seuls ces derniers étant susceptibles d'être concernés par une interdiction d'informer imposée à la banque. Enfin, parmi les clients non-fiscalisés, Roberto distingue les clients qui sont encore en mesure de remédier à leur situation de non-conformité fiscale (lesquels pourraient être informés par la banque), par exemple dans le cadre d'une procédure de dénonciation spontanée, de ceux qui ne le peuvent plus (pour lesquels une interdiction d'informer pourrait s'imposer). Si sur le plan dogmatique, ces distinctions trouvent leur justification, on peut toutefois se demander si en pratique elles peuvent être opérées dans un délai raisonnable, à tout le moins lorsqu'un grand nombre de clients est concerné.

134 Roberto (n. 50), p. 123 ss. Cet auteur considère qu'il n'existe pas d'obligation indépendante de la banque d'informer ses clients de son comportement fautif (*Offenbarungspflicht*) ; cette appréciation ne doit toutefois pas permettre à la banque de renoncer à une information au motif que celle-ci révèlerait des carences de sa part.

135 Cf. également les motifs susceptibles de justifier une renonciation développés par Roberto (n. 50).

136 Arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017, in : SJ 2017 I 454 ; pour un résumé de cet arrêt cf. Yvan Mario Platino, Données volées et avoirs non-déclarés : Le TF refuse l'indemnisation de clients en indélicatesse avec leur fisc, Centre de droit bancaire et financier, publié le 4 octobre 2017, disponible sous https ://www.cdbf.ch/985/ (dernière consultation 11 décembre 2017).

payées aux autorités fiscales italiennes ainsi que des frais relatifs à l'assistance judiciaire. Il était notamment reproché à la banque de ne pas avoir informé la cliente du vol de données – malgré le fait que la correspondance afférente à la relation bancaire était conservée en banque restante – et ainsi l'avoir empêchée de régulariser sa situation volontairement. Après avoir constaté que la banque avait violé ses obligations contractuelles en n'informant pas convenablement la cliente en question des conséquences du vol de données, le Tribunal fédéral a rappelé sa jurisprudence relative à l'indemnisation de la dette fiscale et de l'amende fiscale. Les juges de Mon-Repos ont ainsi confirmé que, d'une part, une dette fiscale naît de par la loi et ne saurait être supportée par des tiers[137], et d'autre part, que les amendes fiscales revêtent un caractère strictement personnel et ne sauraient être des dommages réparables selon le droit civil[138]. Le Tribunal fédéral retient que malgré le fait que les violations contractuelles de la banque soient graves (vol de données, violation du secret bancaire et violation du devoir d'information), c'est bien le comportement de la cliente, en ne déclarant pas ses avoirs en Suisse au fisc italien qui était à l'origine de la sanction prononcée[139].

[Rz 65] Selon l'opinion défendue ici, les banques devraient, sauf circonstance particulière et de manière non généralisée, pouvoir sur cette base renoncer à une information aux clients concernés dans les cas bénins, sans encourir de risques majeurs sur le plan civil. Elles devraient néanmoins informer la FINMA de la nature de l'incident de sécurité ainsi que de sa renonciation à avertir ses clients. Dans les cas plus graves, une telle renonciation ne devrait plus être possible et les clients devraient être informés dès que possible.

4. Mise en œuvre de l'information aux clients

[Rz 66] De manière générale, l'information doit intervenir d'une manière individuelle, ou par voie médiatique lorsqu'une communication individuelle ne peut raisonnablement être exigée compte tenu du nombre de personnes concernées[140]. Dans le cadre d'une fuite de données bancaires, une information individuelle devra néanmoins de toute évidence être privilégiée, y compris lorsque le client et la banque ont conclu une convention de banque restante[141].

[Rz 67] En cas de fuite de données, en particulier lorsque celles-ci ont été volées, l'information aux clients prendra ainsi généralement la forme d'un courrier standardisé aux clients concernés. Ce courrier devrait *idéalement* contenir une information suffisante sur les éléments suivants :

- la nature de l'incident de sécurité ;
- les risques auxquels font face les clients (essentiellement un risque que les données tombent dans le domaine public) ;
- les mesures prises par la banque pour limiter les conséquences de la fuite, notamment sur le plan civil et pénal ;
- les coordonnées des personnes à même de renseigner les clients ;

137 Arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017 consid. 4.4, in : SJ 2017 I 454 ; arrêt du Tribunal fédéral 4A_171/2015 du 19 octobre 2015 consid. 5.1 et 5.2.

138 Arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017 consid. 4.4, in : SJ 2017 I 454 ; arrêt du Tribunal fédéral 4C.3/2007 du 12 novembre 2007 consid. 2.3.2, in : SJ 2008 I p. 169 ss.

139 Arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017 consid. 4.8, in : SJ 2017 I 454.

140 Meier (n. 42), N 657.

141 Cf. dans ce sens, arrêt du Tribunal fédéral 4A_21/2017 du 4 octobre 2017, in : SJ 2017 I 454.

- les coordonnées de conseillers juridiques à même de sauvegarder les intérêts des clients en Suisse ou à l'étranger ; et
- une mise en garde quant à d'éventuelles sollicitations des médias intéressés à l'affaire[142].

[Rz 68] Le contenu de l'information sera évidemment fonction des circonstances et pourra être bien plus succinct dans des cas moins graves, n'impliquant notamment aucun vol de données.

B. L'information aux autorités

1. Préposé fédéral à la protection des données et à la transparence (PFPDT)

1.1. De lege lata

[Rz 69] La LPD ne prévoit une obligation d'informer le *Préposé* que dans des cas biens particuliers, à savoiren cas de communication de données à l'étranger (cf. art. 6 al. 3 LPD ; art. 34 al. 2 let. a LPD ; art. 6 al. 1 OLPD) et lorsque le maître du fichier entend être délié de son devoir de déclaration s'il a désigné un conseiller à la protection des données indépendant chargé d'assurer l'application interne des dispositions relatives à la protection des données et de tenir un inventaire des fichiers (art. 11*a* al. 5 let. e LPD *cum* art. 12*a* al. 1 let. b OLPD).

[Rz 70] Par conséquent, le Préposé ne doit être informé[143] en cas de fuite de données que s'il existe un risque concret que celles-ci soient communiquées à l'étranger, ce qui sera généralement le cas lorsque des données de clients sont volées pour être vendues à une autorité étrangère ou rendues accessibles de toute autre manière à des personnes sises hors de Suisse. S'agissant de données dont il y a lieu de présumer qu'elles feront l'objet d'une publicité médiatique, voire que les données pourront être publiquement accessibles sur une plateforme électronique[144], leur fuite doit selon nous faire l'objet d'une annonce au Préposé.

1.2. Projet de révision totale de la loi sur la protection des données

[Rz 71] En cas de perte de données personnelles, l'art. 22 al. 1 P-LPD prévoit que le responsable du traitement annonce dans les meilleurs délais[145] au Préposé les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Par violation de la sécurité des données on entend toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données (art. 4 let. g P-LPD). Le message indique qu'il n'importe pas

142 Selon une information du quotidien français *Le Monde*, c'est du reste de cette manière que la filiale genevoise d'HSBC aurait prévenu ses clients quelques jours avant la publication par le Consortium international des journalistes d'investigations (ICIJ), cf. Simon Piel, HSCB a prévenu par lettre ses clients de l'imminence des révélations, Le Monde, article publié le 9 février 2015, disponible sous http ://www.lemonde.fr/evasion-fiscale/article/2015/02/09/hsbc-a-prevenu-par-lettre-les-clients-de-l-imminence-des-revelations_4572758_4862750.html (dernière consultation 11 décembre 2017).

143 Ebneter (n. 28), préconise cette mesure (Rz 15).

144 Cf. notamment la base de données sur le site Internet de The International Consortium of Investigative Journalists, disponible sous https ://offshoreleaks.icij.org/ (dernière consultation 14 décembre 2017).

145 Contrairement à l'avant-projet qui prévoyait que le responsable du traitement notifie « *sans délai* » au préposé (art. 17 al. 1 AP-LPD), le projet laisse une plus grande marge au responsable du traitement pour notifier les cas de violation de la sécurité des données.

que la divulgation ou un accès non autorisés se soient effectivement produits ou aient simplement été rendus possibles, il suffit que l'événement en question ait eu lieu[146].

[Rz 72] En revanche, une certaine marge d'appréciation pour la notification est laissée au responsable du traitement, en fonction notamment de l'ampleur du risque pour la personne concernée. En ce sens, plus ce risque est élevé et le nombre de personne concernée important, plus son intervention doit être rapide[147]. Le responsable du traitement peut même renoncer dans certains cas à procéder à une notification au Préposé afin d'éviter la notification de violations insignifiantes qui ne mettent pas en péril la personnalité ou les droits fondamentaux de la personne[148]. L'annonce faite au Préposé doit au moins indiquer la nature de la violation de la sécurité des données, ses conséquences pour la personne concernée et les mesures prises ou envisagées pour remédier à la situation (art. 22 al. 2 P-LPD). Le projet n'énonce en revanche pas le moyen par lequel le Préposé doit être informé[149].

2. Autorités étrangères

[Rz 73] Au même titre que le P-LPD, le RGPD prévoit une obligation de notifier à l'autorité de contrôle en cas de violation de données à caractère personnel[150]. Cependant, contrairement au droit suisse qui laisse une marge d'appréciation au responsable du traitement, le droit de l'Union européenne prévoit explicitement que la notification d'une violation de données à caractère personnel doit intervenir « *dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* »[151]. À défaut, si la notification n'a pas lieu dans les 72 heures, celle-ci est accompagnée des motifs du retard[152]. En cas de sous-traitance, le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance[153]. Il est toutefois recommandé que cette notification intervienne immédiatement et qu'elle soit accompagnée de toutes les informations utiles afin de permettre, le cas échéant, au responsable du traitement de procéder à une notification à l'autorité de contrôle dans un délai de 72 heures[154].

[Rz 74] Si la banque dispose d'un établissement principal ou d'un établissement unique dans l'Union européenne, le principe du *one-stop-shop* prévaut[155]. Ainsi, en cas de traitement de données transfrontières, l'autorité compétente est l'autorité de contrôle du siège de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant[156]. Lorsque les décisions quant aux finalités et aux moyens du traitement de données à caractère

146 Message LPD (n. 39), p. 79.

147 Message LPD (n. 39), p. 120.

148 Message LPD (n. 39), p. 120.

149 Beranek Zanon (n. 94), N 13 qui indique que l'annonce au Préposé pourrait intervenir par le biais d'un formulaire en ligne.

150 Pour la notion de « *violation de données à caractère personnel* » cf. supra III. A. 1.2.

151 art. 33 par. 1 RGPD.

152 *Ibidem*.

153 art. 33 par. 2 RGPD.

154 Guidelines on Personal data breach notification under Regulation 2016/679 (n. 95), p. 11.

155 Beranek Zanon (n. 94), N 10.

156 Cf. art. 56 par. 1 et 2 RGPD.

personnel ne sont pas prises par l'établissement principal mais par un autre établissement, cet établissement est considéré comme l'établissement principal[157]. En revanche, chaque autorité de contrôle est compétente pour traiter les cas de portée locale[158]. Si la banque ne dispose pas d'établissement au sein de l'Union européenne et qu'elle est soumise au RGPD[159], le principe du o*ne-stop-shop* n'est pas applicable et dans ce cas, toutes les autorités de contrôle du lieu où les personnes concernées sont supposées se trouver devraient être informées[160].

3. FINMA

[Rz 75] La banque pourra également se voir imposer une obligation d'annonce spontanée à la FINMA (art. 29 al. 2 LFINMA). Cette annonce doit intervenir sans délai et doit porter sur tout fait susceptible d'intéresser la FINMA. L'art. 29 al. 2 LFINMA constitue ainsi une clause générale permettant d'appréhender toutes les situations non anticipées par les lois sur les marchés financiers[161]. Cette obligation d'annonce couvre uniquement les événements qui revêtent une importance primordiale pour la surveillance, notion qui doit toutefois être interprétée dans un sens large en raison de la compétence étendue de la FINMA[162]. Une perte de données pouvant causer une violation grave du droit de la surveillance constitue notamment un fait important qui doit être annoncé spontanément à la FINMA. L'annonce doit intervenir immédiatement, ou à tout le moins sans retard injustifié[163], et être accompagnée des informations nécessaires.

IV. Conclusion

[Rz 76] Les risques que font courir une fuite de données aux clients et aux établissements concernés sont divers et variés. Ils ne seront généralement pas ou difficilement réparables, d'où la nécessité pour les banques de renforcer régulièrement leur système de sécurité informatique, de mettre en place des processus de gestion de crises efficaces et d'évaluer à intervalle régulier si les mesures implémentées sont adéquates compte tenu notamment des développements en matière de cybercriminalité. Par ailleurs, en présence d'une fuite de données, la banque doit agir rapidement et décider, notamment en suivant des processus prédéfinis, si la fuite en question doit faire l'objet d'une information, auprès de quelles personnes et autorités et selon quelles modalités.

[Rz 77] Les titulaires des données devraient en principe être notifiés de la situation en cas de perte accidentelle, falsification, vol, utilisation, copie, accès ou tout autre traitement non autorisé. L'information aux clients devra généralement intervenir de préférence de manière individualisée. Le

157 art. 4 par. 16 let. a RGPD.

158 L'art. 56 par. 2 RGPD prévoit que chaque autorité de contrôle est compétente pour traiter une réclamation introduite auprès d'elle ou une éventuelle violation du règlement si son objet concerne uniquement un établissement dans l'État membre dont elle relève ou affecte sensiblement des personnes concernées dans cet État membre uniquement.

159 Cf. supra III. A. 1.2.

160 Beranek Zanon (n. 94), N 11.

161 Jean-Baptiste Zufferey/Franca Contratto, FINMA – The Swiss Financial Market Supervisory Authority, Bâle (Helbing Lichtenhahn) 2009, p. 104.

162 Roland Truffer, in : Rolf Watter/Nedim Peter Vogt (édit.), Basler Kommentar, Börsengesetz Finanzmarktaufsichtsgesetz, 2e éd., Bâle (Helbing Lichtenhahn) 2011, N 38 ad art. 29 LFINMA.

163 Truffer (n. 162), N 44 ad art. 29 LFINMA.

PFPDT, la FINMA voire toutes autres autorités compétentes étrangères devront également être informés dans les meilleurs délais. Dans les cas bénins ne présentant pas de risque pour les données des clients concernés, les banques devraient pouvoir en principe renoncer à une information aux clients concernés, sans au demeurant encourir de risques majeurs sur le plan civil. Elles devraient néanmoins informer la FINMA de la nature de l'incident de sécurité ainsi que de sa renonciation à avertir ses clients.

[Rz 78] Au vu de la multiplication des fuites dont certaines banques ont été l'objet ces dernières années, la protection des données des clients et de manière générale l'infrastructure technologique doivent demeurer une priorité et faire l'objet de mesures préventives adéquates. Ces mesures incluent une stratégie de communication adéquate en cas de situation de crise et une clarification des devoirs d'information de la banque.

Nicolas Béguin, avocat, LL.M. (Georgetown University), ABR Avocats.

Benjamin Vignieu, MLaw, ABR Avocats.