HAL
archives-ouvertes.fr

Face aux différents enjeux de la protection des données personnelles, quels sont les leviers à disposition des banques ?

Chloé Rouland

▶ **To cite this version:**

Chloé Rouland. Face aux différents enjeux de la protection des données personnelles, quels sont les leviers à disposition des banques ?. Gestion et management. 2019. dumas-02353128

HAL Id: dumas-02353128
https://dumas.ccsd.cnrs.fr/dumas-02353128

Submitted on 7 Nov 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives| 4.0 International License

Mémoire de stage/ de recherche

Face aux différents enjeux de la protection des données personnelles, quels sont les leviers à disposition des banques ?

Présenté par :Chloé ROULAND

Tuteur universitaire : Marie-Laurence CARON

Master 2 Management et Administration des Entreprises en Formation Continue
2018 - 2019

Présenté par : Chloé ROULAND

Tuteur universitaire : Marie-Laurence CARON

Master 2 Management et Administration des Entreprises
2018 - 2019

UNIVERSITÉ Grenoble Alpes

Avertissement :

Grenoble IAE, au sein de l'Université Grenoble Alpes, n'entend donner aucune approbation ni improbation aux opinions émises dans les mémoires des candidats aux masters en alternance : ces opinions doivent être considérées comme propres à leur auteur.

Tenant compte de la confidentialité des informations ayant trait à telle ou telle entreprise, une éventuelle diffusion relève de la seule responsabilité de l'auteur et ne peut être faite sans son accord.

RÉSUMÉ

Alors que les individus peuvent sembler incohérents sur la vision qu'ils ont de l'intrusion dans la vie privée, ils prennent néanmoins conscience du risque encouru à partager leurs données personnelles. La transformation numérique et la modification de leur comportement de consommateur avec la digitalisation de l'offre, les amènent en effet à divulguer de plus en d'informations sur eux-mêmes qui pourraient être volées par des cybercriminels. En Europe, les pouvoirs publics ont pris le sujet au sérieux depuis de nombreuses années et la législation n'a cessé d'évoluer pour renforcer la protection des données et rendre les dispositifs de lutte contre la cybercriminalité encore plus performants.

Les banques, fortement concernées par le sujet, ont pris très tôt conscience de l'intérêt qu'il y avait à protéger les données de leurs clients et ont mis en œuvre les moyens nécessaires. Cela est d'autant plus important que leurs clients sont en attente d'une offre sans cesse renouvelée et que celle-ci ne peut se créer qu'avec toujours davantage de données. La confiance reste le maître mot de la relation entre les banques et leurs clients.

REMERCIEMENTS

Je remercie Mme Caron, ma tutrice à l'IAE, pour l'aide qu'elle m'a apportée pour définir le plan de ce mémoire.

Je remercie également Guy Parmentier, responsable du Master2 MAE FC, pour sa présence bienveillante tout au long de cette formation. Finalement embarqué avec nous tous dans cette aventure humaine, il a toujours su nous apporter son soutien.

SOMMAIRE

INTRODUCTION

Mon expérience de 8 années en back office dans une grande banque française fait que je porte aujourd'hui beaucoup d'intérêt à ce secteur d'activité aux métiers multiples et que l'environnement actuel, tant économique que règlementaire, oblige à réinventer.

Pendant cette expérience professionnelle passée à des postes en lien avec le commerce international, j'ai été sensibilisée aux différents sujets liés à la règlementation financière internationale, aux risques de fraude et aux contrôles de conformité mis en place. Au service des entreprises clientes et en contact quasi-quotidien avec elles, j'ai pu être amenée à leur parler des outils bancaires disponibles et des procédures internes appliquées pour sécuriser leurs transactions. Une courte expérience au service des prêts immobiliers, à l'analyse des dossiers de demande, m'a permis de découvrir la clientèle des particuliers et de me rendre compte de la quantité d'informations qui était recueillie sur eux.

Parallèlement et bien que n'étant pas en contact direct avec la clientèle des particuliers, j'ai suivi l'évolution de digitalisation de l'offre bancaire pour répondre à de nouvelles attentes des clients et également pour contrer la concurrence des banques en ligne ou des néobanques. Le marketing digital, notion étudiée cette année durant ce master et totalement nouvelle pour moi, a d'ailleurs contribué à m'apporter une meilleure compréhension sur ce sujet.

Enfin, des mots un peu barbares comme RGPD, DSP2, cybercriminalité, blockchain ou encore algorithmes ont éveillé mon esprit.

J'ai donc décidé d'orienter mon sujet de mémoire sur les constats suivants :

- des consommateurs hyper-connectés qui veulent toujours plus de services, de flexibilité et d'instantanéité.

- ces mêmes consommateurs n'hésitant pas transmettre via les canaux numériques des informations les concernant, mais qui paradoxalement se sentent extrêmement concernés par ce qui est fait.

- des règlementations européennes et françaises sur la protection des données personnelles renforcées et protectrices pour les individus et de plus en plus contraignante pour les organisations, notamment les banques.

- des outils technologiques de plus en plus innovants.

- des banques disposant d'une mine d'or de données personnelles sur leurs clients pour développer des offres personnalisées,

- mais qui, par conséquence, se retrouvent victimes d'une augmentation croissante de cyberattaques et de tentatives de fraude de la part d'individus malveillants souhaitant récupérer ces données.

D'où une problématique à mes yeux. En effet, face un environnement réglementaire sur la protection de la vie privée de plus en plus contraignant pour elles, des habitudes de consommation modifiées par l'avènement de l'ère digitale et une cybercriminalité en hausse, quels leviers les banques ont-elles pour répondre aux enjeux de la sécurisation des données personnelles de leurs clients ?

Dans une première partie, je poserai les bases de l'étude en abordant des concepts qui touchent à ce sujet grâce à différentes recherches que j'ai pu effectuer. Je parlerai donc :

- du « privacy paradox » dans un contexte d'habitudes de consommation plus digitalisées d'une part, et de cybercriminalité accrue d'autre part.

- de l'arsenal législatif et réglementaire autour de la protection des données clients avec comme dernier aboutissement le RGPD.

- de la banque avec un focus sur ses spécificités dans le cadre de cette étude tant en ce qui concerne la collecte des informations que la règlementation DSP2 qui vient rajouter des contraintes supplémentaires.

Dans une deuxième partie, sur la base de ces concepts, je m'intéresserai davantage à la manière dont les banques, dans ce nouveau contexte sociétal, économique, technologique et réglementaire, gèrent aujourd'hui ces contraintes, aux bonnes pratiques qu'elles ont mises en œuvre.

Enfin, dans une troisième partie, j'étudierai les solutions sur lesquelles travaillent les banques pour le futur, tant en matière de cybersécurité et d'innovations technologiques pour développer des offres clients encore plus ciblées, tout en gardant à l'esprit de rester en conformité avec la réglementation.

Pour ce mémoire, j'ai fait le choix d'étudier uniquement la clientèle particulière des banques, sachant que la clientèle entreprises est, elle aussi, touchée par les tentatives de fraude visant à dérober des données sensibles.

La zone d'étude est restreinte à la France et à l'Europe pour des raisons que j'expliquerai.

J'ai puisé mes recherches dans la littérature des sciences de gestion, sur les sites internet d'organismes publics français et européens et aussi dans la presse spécialisée et vulgarisée pour le grand public. Mon étude « terrain » repose sur le témoignage d'experts trouvés dans ces journaux. J'ai également pu interroger un directeur d'agence d'une banque dont j'ai choisi de ne pas citer le nom.

PARTIE 1 :
LES ENJEUX AUTOUR DES DONNEES PERSONNELLES

CHAPITRE 1 – ETUDE DES CONCEPTS LIES A LA PROBLEMATIQUE

I. LE « PRIVACY PARADOX »

En octobre 2018 et sur les 7,6 milliards d'habitants que compte la terre, 4,2 milliards étaient des internautes et 3,4 milliards utilisaient les réseaux sociaux [1]. Cela n'est pas sans avoir de conséquences sur notre vie privée.

La notion de « privacy paradox » a été étudiée dès les années 2000 pour tenter de décrire un phénomène lié aux conséquences de l'apparition des réseaux sociaux sur la vie privée, notamment sur celle des adolescents. Les premières études académiques se sont concentrées sur le fait que les utilisateurs dévoilaient sur les réseaux sociaux des informations sur leur vie privée sans avoir forcément pris conscience que ces espaces de discussions étaient quasi-publics [2].

Les réponses légales se sont d'abord focalisées sur les risques encourus pas les adolescent(e)s de faire des mauvaises rencontres via les réseaux sociaux et la mise en place de dispositifs pour les protéger de ces individus mal attentionnés, occultant ainsi un autre aspect du « privacy paradox », à savoir l'utilisation à mauvais escient des données personnelles privées, désormais présentes en masse sur l'espace public [3].

II. DES EVOLUTIONS DANS LA COLLECTE DES DONNEES

Les entreprises ont besoin d'informations sur leurs clients pour définir leur offre marketing. Aujourd'hui, la stratégie de collecte des données personnelles ne repose plus seulement sur l'exploitation des informations qui circulent sur les réseaux sociaux. En effet, les évolutions technologiques (internet, messagerie, applications numériques) ont permis une collecte, un stockage et une transmission des données, toujours plus rapide et plus massive.

Le smartphone, notamment, accompagnant désormais l'utilisateur dans toutes ses démarches dématérialisées, et pourtant importante source de fuite de données, n'a fait qu'accentuer ce « privacy paradox » [4]. En effet, une enquête menée par l'institution française la CNIL, Commission Nationale de l'Informatique et des Libertés, et ses homologues européens en mai 2014 montrait que ¾ des applications mobiles (sur 1200 testées) collectaient des données personnelles sur les utilisateurs, très souvent à leur insu. Plus précisément, 49% des applications géolocalisaient l'utilisateur et 26% accédaient à ses contacts [5].

Les objets connectés que l'on retrouve désormais dans beaucoup de domaines de la vie courante, comme par exemple les enceintes à commande vocale donnent également lieu à la collecte et au stockage de nombreuses données personnelles. L'historique des requêtes et les données sont stockés sur des serveurs pouvant présenter des failles dans leur sécurité.

Parallèlement, s'est développée la possibilité pour les consommateurs d'acheter sur internet. La fédération e-commerce et vente à distance, la FEVAD, indique que les ventes sur internet avaient atteint 92,6 milliards d'euros de chiffre d'affaire en 2018, soit une croissance de 13,4% par rapport à 2017 [6].

Ces nouvelles technologies désormais utilisées au quotidien sont devenues pour les entreprises un nouveau moyen d'obtenir des informations sur leurs consommateurs. N'étudiant jusque-là que des données liées à leur marché pour développer leurs stratégies commerciales, elles ont vite compris l'intérêt de posséder de plus en plus d'informations personnelles sur leurs clients (âge, sexe, géolocalisation, habitudes d'achats, classe socioculturelle...) pour mieux les connaitre et leur proposer des offres de mieux en mieux ciblées. Proposer de nouveaux parcours clients peut en effet leur permettre de dégager un avantage concurrentiel. Très vite, elles ont donc mis en œuvre les moyens pour obtenir et maitriser le maximum d'informations sur leurs clients et prospects [7].

III. OU SONT STOCKEES NOS DONNEES ?

Pour stocker les données de leurs clients, beaucoup d'entreprises font appel à des bases de données externes. Les données sont donc souvent stockées physiquement dans des datacenters. Il s'agit classiquement de grands entrepôts avec des salles remplis de serveurs pour héberger les données et les entreprises louent une partie de ces datacenters pour le stockage de leurs données. Ils existaient 4081 sites répartis dans 118 pays en 2017 [8].

Cet hébergement traditionnel a évolué vers le Cloud computing où les ressources sont « virtuelles ». Les entreprises ne louent plus des serveurs dans des datacenters classiques et ne paient plus pour des infrastructures. Beaucoup d'entreprises louent à des prestataires des cloud privés qui leur sont dédiés, et leurs données ne sont pas partagées. A l'inverse, dans les cloud publics, les données sont réparties sur plusieurs serveurs partout dans le monde et les ressources informatiques sont mutualisées**.** En 2018, 1 entreprise sur 4 dans le monde avait subi un vol de données sur le cloud [9].

Bien que les entreprises ne sachent plus où se trouvent leurs données, le cloud est néanmoins bien physique et les données sont traitées dans des mégadatacenters dont on ne connait pas la localisation [10].

Quand les données qu'elles détiennent sur leurs clients sont trop sensibles, certaines entreprises ont des datacenters en internes.

IV. La Cybercriminalite

Outre le côté éthique de la non-maitrise de leurs données personnelles par les individus, les risques d'un usage mal-attentionné de celles-ci sont également pointés du doigt. Le but pour les fraudeurs et les pirates est d'obtenir ces données afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). On utilise les termes de cyber-risques ou cybercriminalité pour parler de ces fraudes et attaques. Les conséquences de ces actes sont graves : usurpation d'identité, risques d'e-réputation, image de marque dégradée pour les entreprises…

Parmi les fraudes les plus classiques touchant les particuliers mais aussi les entreprises ou les organisations, le phishing (hameçonnage en français) est une technique qui consiste pour le fraudeur à usurper l'identité d'une entreprise ou d'une organisation bien connue et à contacter des millions d'internautes via e-mail pour leur demander des informations sensibles en prétextant souvent le besoin d'une mise à jour : numéro de carte bancaire, code d'accès. Redirigées vers un site falsifié, les victimes renseigneront les informations demandées que le cybercriminel peut récupérer. Le taux de réussite de cette fraude reste encore très élevé malgré les nombreuses opérations de communication préventive des entreprises ou organisations dont le nom est usurpé.

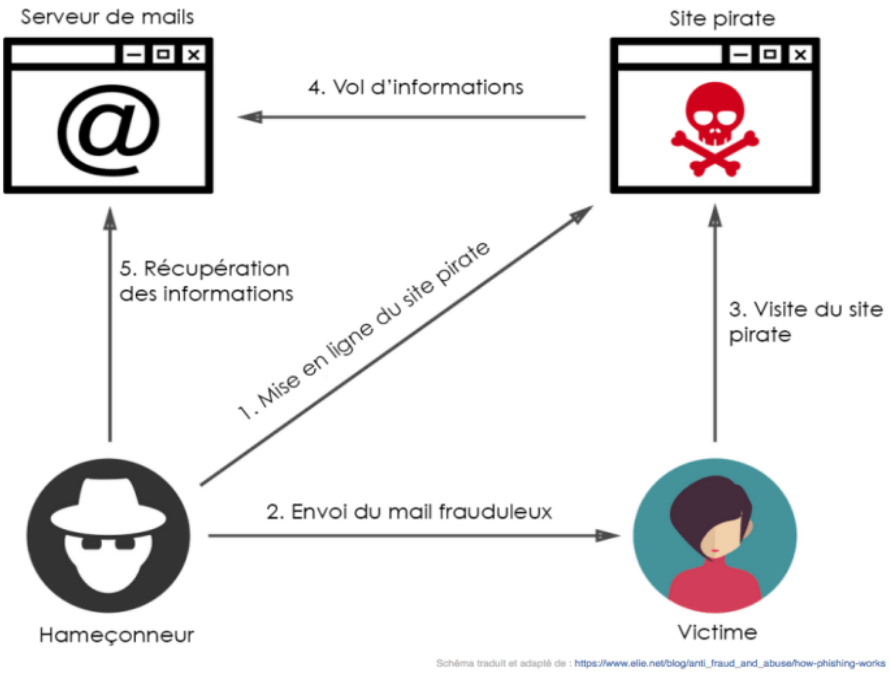

Schéma de la technique de phishing : https://visionarymarketing.com/blog/tag/phishing/

Le malware (pour malicious sofware), quant à lui, est un virus qui souvent diffusé par e-mails et invoque des problèmes liés à une commande ou une facturation pour infecter l'ordinateur, la tablette ou le téléphone portable de l'utilisateur. Ils peuvent notamment voler ses données personnelles. Le nombre de malware bancaires a doublé en 2018, selon une étude de Kaspersky Lab [11].

Pour ce qui est des attaques sur les systèmes d'informations des entreprises afin d'accéder aux bases de données de leurs clients, les criminels exploitent souvent une faille informatique. Le 7 septembre 2017, l'agence américaine d'analyse de crédit Equifax révélait le piratage de sa base de données clients qui a permis d'accéder aux données personnelles d'environ 145,5 millions de ses clients aux Etats-Unis. Equifax n'avait pas corrigé une faille informatique, connue pourtant dès le mois de mars [12].

« Les effets de la cybercriminalité sur l'économie ont été multipliés par cinq depuis 2013 et les cyberattaques coûtent quelque 400 milliards d'euros par an à l'économie mondiale » [13].

Pourtant, les risques ne sont pas encore bien compris par les individus et les entreprises. Selon la Commission européenne, en 2017, « 51 % des Européens se sentent peu informés au sujet des cybermenaces » et « 69 % des entreprises n'ont qu'une compréhension de base, ou n'ont pas de compréhension, de leur exposition aux cyber-risques. » [13].

V. UNE PRISE DE CONSCIENCE DES DEUX PARTIES

Tous ces enjeux éthiques, ces dérives potentielles et ces risques encourus à dévoiler ainsi une partie de leur vie privée et de leurs habitudes personnelles ont néanmoins permis une certaine prise de conscience de la part des consommateurs des [14]. En 2016, en France, d'après le baromètre annuel de l'intrusion publié par l'agence Publicis ETO, 72% des personnes interrogées étaient dérangées par le fait que des informations soient collectées et enregistrées dans des bases de données [15]. Toutefois, ils restent très contradictoires en continuant par exemple encore souvent d'utiliser les réseaux sociaux sans avoir pris soin de bien avoir défini tous les paramètres de confidentialité [16].

La notion de « privacy paradox » semble donc avoir évoluée depuis les premières études sur le sujet. Aujourd'hui, les utilisateurs de nouvelles technologies sont certes de plus en plus avisés et méfiants quant aux risques que leurs données personnelles soient exploitées et divulguées de manière indue, mais ils ne semblent pas prêts à modifier leurs habitudes. Ils restent souvent poings et mains liés avec les réseaux sociaux craignant sans doute de perdre un grand pan de leur vie sociale qui se concrétise désormais par ce biais. En tant que consommateurs, ils ne sont pas non plus disposés à renoncer aux bénéfices que les nouvelles technologies leur procurent désormais, comme la flexibilité et le gain de temps offert par la possibilité des achats en ligne ou la consultation à tout moment de leur compte bancaire. Ils préfèrent souvent voir les avantages plutôt que les inconvénients et continuent, en ayant ou non pesé le pour ou le contre, de dévoiler une partie de leur vie privée. Restent également ceux d'entre eux qui n'ont pas encore pris conscience des enjeux.

Parallèlement, les entreprises ont également pris conscience des conséquences pour leur image et leur réputation si les données qu'elles détiennent sur leurs clients étaient frauduleusement utilisées.

Les gouvernements européens ne sont pas non plus restés inactifs et une prise de conscience quant à la nécessité de protéger les données personnelles des citoyens et de développer les moyens nécessaires à la mise en place de mesures de cybersécurité fiables, efficaces et évolutives s'est concrétisée par des moyens légaux.

CHAPITRE 2 – EVOLUTION DE LA REGLEMENTATION RELATIVE A LA PROTECTION DES DONNEES PERSONNELLES

I. QUELQUES DEFINITIONS

Il me parait important de détailler certaines notions avant d'aller plus loin dans cette étude.

S'agissant ici du respect des droits des citoyens et des consommateurs et de l'utilisation qui pourraient être faites de leurs données sans leur consentement, je trouve la définition de la vie privée donnée par Garfinkel (2000) particulièrement adaptée : la vie privée, c'est « le droit de contrôler quelle partie de votre vie reste à la maison et qu'est-ce qui peux passer à l'extérieur » [17].

D'après la CNIL, on entend par une donnée personnelle « toute information, identifiant directement ou indirectement une personne physique (ex. nom, numéro d'immatriculation, numéro de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale …) » [18].

Concernant ce que les utilisateurs entendent par un usage non approprié de leurs données, six pratiques sont plus particulièrement décriées selon Wang et Wang (1998) [19] : la collecte de trop de données ou des données trop sensibles, le stockage non autorisé de ces données, les modifications accidentelles ou délibérées des données fournies, l'accès à ces données par des personnes non autorisées, ainsi que l'utilisation que l'entreprise fait de ces données, soit en interne pour envoyer des offres commerciales non désirées et non sollicitées aux clients, soit en externe en cédant les données à d'autres entreprises sans autorisations préalables de la part des clients.

II. UN ARSENAL DE DISPOSITIFS EN EUROPE ET EN FRANCE

J'ai volontairement choisi de concentrer mon étude sur l'Europe et la France car on ne considère pas les atteintes à la vie privée de la même manière partout dans le monde : par exemple, « aux Etats-Unis, la vie privée n'est pas un droit garanti par la Constitution mais un privilège légal. En Europe par contre, elle fait partie des droits de l'Homme, au même titre que la liberté » [16].

C'est sans doute pour cette raison qu'il semblerait que les européens soient plus attachés à la protection de leurs données personnelles que d'autres et que les entreprises européennes en aient pris conscience plus rapidement. En effet, des études montraient déjà au début des années 2000 que les sites commerciaux européens étaient moins demandeurs d'informations personnelles sur leurs clients que les sites commerciaux américains. Par contre, ils ne donnaient pas clairement le choix à l'utilisateur d'autoriser ou non l'utilisation et la transmission de ses informations [20].

Les législations européenne et française se sont parallèlement intéressées très tôt au respect des données personnelles des citoyens en cherchant à les responsabiliser d'un côté et à s'assurer qu'il soit fait bon usage de leurs informations d'un autre côté. Elles ont souhaité leur reconnaitre un droit démocratique à décider de l'utilisation qui devait être faite de leurs données. Pour cela, les instances gouvernementales ont cherché à imposer de bonnes pratiques aux entreprises via des leviers juridiques. Les lois, décrets, directives et autres déclarations n'ont cessé de se renforcer en Europe comme en France, notamment ces dernières années. Il s'agit en effet d'un enjeu majeur pour l'Union Européenne qui cherche également à promouvoir le développement de l'activité numérique.

L'acteur français œuvrant pour la protection des données personnelles en France est la CNIL (Commission Nationale de l'Informatique et des Libertés) : il s'agit d'un organisme public français indépendant. En tant que régulateur, elle veille à ce que l'informatique se développe mais sans porter atteinte à la vie privée des citoyens en s'attachant à la protection des données personnelles des citoyens. Les entreprises doivent en principe déclarer à la CNIL leurs fichiers contenant des données sur leurs clients ainsi que le traitement qu'ils en font.

Voici quelques grandes dates liées à l'évolution de cet enjeu autour de la vie de privée :

6 janvier 1978 : la loi « Informatique et Libertés » est la première pièce de l'édifice en France concernant le traitement des données personnelles. Elle impose notamment le consentement des individus pour l'utilisation de leurs données et leur autorise à y accéder et à demander leur effacement. Elle a créé la CNIL.

24 octobre 1995 : la directive européenne 95/46/CE a pour but d' aider à l'application de deux objectifs qui peuvent paraître antinomiques : « respecter les libertés et droits fondamentaux des personnes, notamment la vie privée » et « contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus » [8].

04 mai 2016 : l'Union Européenne vote la nouvelle réglementation sur la protection des données personnelles qui entre en vigueur le 25 mai 2018 (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). Jean-Charles Croiger, Directeur de Capgemini Consulting et expert du secteur bancaire, explique en 2016 que 90% des européens souhaitent la mise en place d'un cadre commun de protection des données à travers toute l'Europe [21]. La décision de réviser la directive européenne 95/46/CE est liée à l'évolution du contexte technologique.

25 mai 2018 : en Europe, le Règlement Général sur la Protection des Données (RGPD) rentre en vigueur et remplace la directive 95/46/EC. Il constitue une avancée majeure pour les citoyens et les consommateurs à plusieurs égards. Ce texte, qui vise à harmoniser la réglementation en matière de protection des données personnelles, s'applique aux 28 pays membres de l'Union européenne. C'est la CNIL qui doit notamment veiller à la mise en action du RGPD sur le territoire français.

Le RGPD œuvre à la traçabilité, la transparence et la sécurité des données personnelles des individus. Ces derniers pourront désormais demander aux entreprises de leur expliquer ce qui est fait de leurs données et elles seront obligées de les en informer. Le texte a donc un impact fort sur l'ensemble des sociétés détenant des données personnelles sur leurs clients.

III. FOCUS SUR LE RGPD

Le RGPD constitue un renforcement des mesures de sécurité déjà existantes et plusieurs nouveaux droits pour les clients font leur apparition :

- le droit à l'accès : il s'agit pour l'utilisateur de pouvoir demander à n'importe quel moment un document recensant l'ensemble de ses données personnelles dont l'entreprise est en possession
- la droit à demander la modification de leurs données si elles sont inexactes
- la portabilité des données : ce droit permet à un utilisateur de demander à récupérer ses données pour faciliter, par exemple, le passage à la concurrence
- le droit à l'oubli : il permet désormais à l'utilisateur de demander à tout moment à ce que ses informations soient effacées de manière définitive
- le droit de s'opposer à l'utilisation de leurs données, par exemple pour du démarchage

Le RGPD apporte en parallèle de nouvelles contraintes aux entreprises :

- le traitement des données de leurs clients doit être fait conformément à la règlementation et de manière transparente. Les consommateurs doivent être informés de manière claire et précise de ce qui sera fait de leurs données et avec qui elles seront partagées.
- l'obligation d'obtenir le consentement des clients quant à l'utilisation de leurs données dans le but de leur proposer de nouveaux services. Sur ce sujet, le RGPD renforce la législation en vigueur en ce sens que le consentement du client doit être donné de manière libre, non ambiguë et après avoir été informé. Il est nécessaire d'avoir l'opt-in, le consentement explicite de la personne, avant de pouvoir la contacter par email

- les données doivent être collectées dans un but spécifique, explicite et légitime et si elles sont utilisées à des fins autres que celles prévues au départ, celles-ci ne doivent pas être incompatibles avec le but initial. C'est le principe de « purpose limitation »
- les entreprises ont la responsabilité du traitement des données et doivent y mettre les moyens comme le « privacy by design » qui consiste à intégrer la sécurité dès la conception des applications gérant ces données

- elles se voient infliger des amendes en hausse en cas de non-respect de la règlementation. Fixé à 4% du CA global, le montant est fortement dissuasif
- elles doivent mettre en place d'une démarche d'informations auprès de leurs clients sur le RGPD et ses conséquences
- elles ont l'obligation de créer un poste de délégué à la protection des données (DPO)
- en cas de violations de leur système de sécurité, elles doivent informer la CNIL

Il semblerait que le RGPD ait été bien accueilli par les citoyens. Selon l'étude Toluna QuickSurveys réalisée pour Affinion International en mai 2018 sur un échantillon représentatif de la population française âgée de 18 à 55 ans et plus, 80% des Français craignent une utilisation frauduleuse de leurs données personnelles et voient donc l'arrivée du RGPD d'un bon œil, espérant plus de transparence. [22].

La prochaine étape souhaitée par l'Union Européenne est l'adoption d'une loi dite «e-privacy », sur la confidentialité des données électroniques pour s'adapter aux nouveaux modes de communications.

Les entreprises sont donc fortement impactées par cet attirail législatif qui va de pair avec une règlementation en matière de cybersécurité.

CHAPITRE 3 – EVOLUTION DE LA REGLEMENTATION RELATIVE A LA CYBERSECURITE

Les enjeux sont importants. Jean-Claude Juncker, président de la Commission Européenne, déclarait le 13 septembre 2017 que l'Europe reste "mal équipée face aux cyberattaques" [23]. D'après le Conseil de l'Union Européenne, « 87 % des Européens considèrent que la cybercriminalité est un défi majeur à relever pour la sécurité intérieure de l'UE » [13].

Les principaux acteurs dans la lutte dans la prévention et la lutte contre la cybersécurité sont :

L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : son rôle est de lutter, prévenir et sensibiliser à la l'importance de la cybersécurité et de lutter contre les risques.

L'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) : elle intervient comme experte auprès de l'Union Européenne et des états membres.

Voici quelques dates clés :

18 décembre 2013 : la loi de programmation militaire française pour la période 2014-2019 impose aux opérateurs d'importance vitale (OIV) de mettre en place des mesures de sécurité informatique renforcées pour éviter le piratage des systèmes informatiques. L'ANSSI les accompagne. Un OIV est un opérateur public ou privé, qui « exploite ou utilise des installations jugées indispensables pour la survie de la Nation » [24].

06 juillet 2016 : Adoption de la directive européenne NIS sur la sécurité des réseaux et des systèmes d'information (NIS pour Network and Information Security) qui devait être transposée au droit national de chacun des états membres avant mai 2018, crée le concept d'OSE, opérateur de services essentiels au maintien de l'économie et de l'activité sociale. Plus nombreux que les OIV dont certains pays européens n'avaient pas d'équivalent, ils doivent eux aussi se conformer à de nouvelles mesures en termes de cybersécurité. « La directive NIS répond également à ce besoin partagé de protection des acteurs économiques européens » [25].

13 septembre 2017 : Le « paquet cyber », présenté par la Commission Européenne, regroupe un nombre de mesures pour mieux lutter contre la cybercriminalité et prévoit d'en faire une « véritable agence de cybersécurité pour l'Europe » en plus d'une augmentation de ses effectifs et de son budget [23].

CHAPITRE 4 – LES SPECIFICITES DU SECTEUR BANCAIRE

I. UNE COLLECTE SPECIFIQUE DE DONNEES

En partie due a la règlementation propre au secteur bancaire :

Pourquoi les banques savent-elles tant de choses sur nous ? La raison en est pour partie réglementaire.

Si les banques demandent à leurs clients ou futurs clients de leur fournir tant de données sur eux, c'est d'abord car elles y sont obligées. Les banques ont notamment une obligation de vigilance afin de

respecter le cadre réglementaire de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Cette collecte et analyse d'informations sur les clients s'appelle le KYC pour Know Your Customer. Ainsi, l'ouverture d'un compte ne peut se faire sans l'obtention de justificatifs d'identité et de domicile. D'autres informations qu'elles jugeront pertinentes pour vérifier la cohérence des opérations pourront également être demandées : bulletins de salaire, déclaration de revenus, acte de propriété, etc... De plus, au cours de la relation avec leurs clients, les banques pourront leur demander de fournir à nouveau des explications pour certaines opérations : retrait d'un moyen de paiement (chèque ou carte), transfert d'argent hors espace économique européen, obtention d'un prêt... Les banques ont en fait l'obligation d'avoir une connaissance à jour de leurs clients et ces derniers seront plus ou moins sollicités selon le niveau de risque qui leur est attribué. De même, si elles détectent une transaction sur leur compte qui paraîtrait inhabituelle, et toujours pour des raisons de conformité, les banques demanderont des explications relatives à la provenance et la destination des fonds ainsi qu'à l'identité du donneur d'ordre ou de l'émetteur et les clients pourront là encore avoir la nécessité de fournir des justificatifs supplémentaires comme un contrat d'achat de voiture ou de vente de maison.

La typologie des documents à fournir peut varier d'une banque à l'autre mais la liste est souvent édictée par la direction conformité de chaque banque et il y a peu de marge de négociation entre les clients et leur conseiller. D'ailleurs, si les clients refusent de répondre, ils risquent le refus par la banque de traiter leurs opérations et également de faire l'objet d'une déclaration à l'organisme spécialisé dans la lutte contre la fraude Tracfin (Traitement du Renseignement et Action contre les Circuits Financiers clandestins). Si les banques ne respectent pas ces obligations de vigilance, elles encourent quant à elles des mesures disciplinaires, voire pénales [26].

Dans le cadre de la procédure FATCA, les banques devront également demander à leurs clients s'ils ont la nationalité américaine car l'autorité fiscale américaine souhaite savoir si ses ressortissants possèdent des comptes à l'étranger. L'OCDE (Organisation de Coopération et de Développement Economiques) qui participe à la lutte contre l'évasion fiscale requiert également des banques qu'elles obtiennent un justificatif de résidence fiscale de la part de leurs clients [27].

Enfin, lors d'une demande d'obtention d'un prêt immobilier par exemple, les banques demanderont à leurs clients ayant un compte chez un de leurs confrères de leur fournir une copie des derniers relevés de compte afin de s'assurer que leurs clients pourront bien les rembourser.

Et à la digitalisation de l'offre bancaire :

Une autre raison pour laquelle les banques amassent de plus en plus de données sur leurs clients est qu'elles sont désormais bien présentes sur le marché du numérique, que ce soit via les banques en ligne (qui sont des filiales de banques traditionnelles) ou des néobanques (100% mobile). Comme vu précédemment, l'avènement du numérique a eu pour conséquence une modification des habitudes de consommation des clients qui sont devenus de plus en plus digitalisés. La banque n'a pas échappé à ce phénomène. « Les clients veulent désormais accéder à leurs services bancaires en ligne de n'importe quel outil, n'importe où et n'importe quand » [28].

D'après une étude menée ACPR / Banque de France sur la révolution numérique dans le secteur bancaire, les utilisateurs ont modifié leur choix d'accès à leurs services bancaires [29]. Ils s'enthousiasment pour les services en ligne et la relation avec les clients se fait de moins en moins en agence. Déjà en 2016, 86% des contacts entrants (donc à l'initiative du client) se faisait via les canaux digitaux à la Société Générale [30]. 20% des français fréquentaient leur agence plusieurs fois par mois en 2016 contre 52% en 2010 [31]. En 2016, l'accès à un espace bancaire en ligne se faisait à 60% via un ordinateur et 40% via un smartphone contre respectivement 93% et 7% en 2012 [29].

Ce changement culturel montre que les consommateurs sont en attente de réactivité et d'expérience client de la part de leur banque. « Le réflexe systématique de rechercher l'information et de comparer les offres avant de solliciter le conseil et la volonté d'être davantage autonome dans ses usages. » [29].

II. LA DIRECTIVE DSP2

Impactant fortement les banques, la seconde directive européenne sur les services de paiement (DSP2) est entrée en vigueur le 13 janvier 2018. DSP2 impose que les banques ouvrent leurs systèmes d'informations à des acteurs tiers via la mise en commun des bases de données pour qu'ils puissent y récupérer des données et également y déclencher des paiements. Selon Gil Dellile, directeur des risques IT chez Crédit Agricole SA, la volonté des régulateurs d'ouvrir le marché financier à la concurrence s'interprète comme une façon « de dynamiser l'économie des services péri-bancaires et de permettre l'émergence de nouveaux acteurs et de nouveaux services propices au développement de l'économie européenne » [32]. Ses acteurs, souvent des fintechs, sont essentiellement des prestataires qui offriront des services d'informations sur les comptes ou des fournisseurs de services de paiement.

Nous avons analysé pourquoi les banques étaient en possession de tant de données particulièrement sensibles sur leurs clients, que ce soit pour des raisons purement réglementaires ou liées au développement des nouvelles technologies. Avec le RGPD imposant des mesures fortes et contraignantes aux entreprises concernant la protection de ces données, l'industrie bancaire est plus particulièrement impliquée et les nouveaux usages numériques sont autant de nouveaux défis pour elle. Dans la partie suivante, nous verrons comment elle s'adapte à ce nouvel environnement et quelles sont les difficultés rencontrées.

III. LES BANQUES ET LA CYBERSECURITE

Les banques sont en effet davantage exposées à la cybercriminalité et aux attaques informatiques, dont j'ai déjà parlé précédemment, que d'autres entreprises dû à la typologie des informations, souvent plus sensibles, qu'elles possèdent sur leurs clients et des millions d'euros qu'elles font transiter. La cybermenace pour les banques, c'est, selon Gil Delille, directeur des risques IT chez Crédit Agricole, la « possibilité d'une intrusion au cœur des systèmes d'informations qui, si elle n'était pas détectée à temps, permettrait de passer des ordres pour le compte de la banque ou d'en extraire une grande quantité de données » [32]. En Effet, les attaques et tentatives de fraude sont quasi-quotidiennes. En février 2016, des pirates informatiques ont dérobé 81 millions de dollars à la banque centrale du Bangladesh via de faux ordres de virement adressés à la Réserve fédérale de New-York.

Le risque se retrouve exacerbé car les interactions entre les systèmes d'informations bancaires et l'extérieur augmentent. La transformation digitale des banques a ouvert une partie des systèmes informatiques à leurs clients et prospects. La directive DSP2, quant à elle, les a ouverts à des prestataires. Elles se sont donc retrouvées face à des risques de fraudes accrues [30].

Côté clients, c'est sur les paiements à distance que se concentrent les deux tiers de la fraude à la carte bancaire en France, d'après l'Observatoire de la sécurité des cartes de paiements [30]. Elle provient essentiellement de problèmes liés à l'identification.

PARTIE 2

-

LES REPONSES « TERRAIN » DES BANQUES A CETTE PROBLEMATIQUE

CHAPITRE 1 – LE MANAGEMENT DE LA MISE EN CONFORMITE AVEC LE RGPD

I. INFORMER LES CLIENTS ET RESPECTER LEUR DROITS

Dans le cadre du RGPD, les banques sont désormais tenues d'informer leurs clients de ce qui est fait de leurs données. Ainsi, comme toutes les banques françaises et européennes, Fortunéo, banque en ligne, met à leur disposition un document expliquant sa politique de confidentialité et téléchargeable sur le lien suivant : https://mabanque.fortuneo.fr/datas/files/politique-de-confidentialite.pdf.

Parmi leurs droits (nouveaux ou renforcés) issus du RGPD, les plus importants sont les droits à l'accès, à la portabilité et à l'oubli:

- l'utilisateur peut demander à accéder à ses données à tout moment. La banque devra lui fournir un fichier informatique recensant toutes les informations personnelles sous un mois maximum. La demande peut se faire en remplissant un formulaire en ligne via le site web des banques [33].
- Concernant le droit à la portabilité, les banques ont désormais l'obligation de proposer la mobilité bancaire à leurs clients. S'il s'agit d'une portabilité vers une autre banque, celles-ci peuvent utiliser le mandat de mobilité, mis en œuvre dans le cadre de la loi pour la croissance, l'activité et l'égalité des chances économiques, dite loi Macron. C'est la nouvelle banque qui se charge, à la place du client, de toutes les démarches autour du changement de domiciliation bancaire après lui avoir fait signer un mandat de mobilité bancaire. Pour ce qui est du transfert de données vers des acteurs autres que les banques, il semblerait que ce soit encore flou et qu'il y ait des discussions à venir avec les régulateurs, la CNIL et l'ACPR principalement, sur le sujet.
- le droit à l'oubli représente, quant à lui, un casse-tête pour les banques car il sera extrêmement compliqué d'effacer des données se retrouvant dans plusieurs systèmes d'informations simultanément. Les banques ont donc fait une demande d'exception auprès de la CNIL et de l'ACPR. Ce droit à l'oubli devrait rester théorique pour ce qui est des banques car à contrario, certaines réglementations les contraignent à conserver les données de leurs clients sur le long terme, comme la loi dite « Eckert » de lutte contre la déshérence des produits d'épargne [34].

De par leur activité, les institutions bancaires possèdent des informations dites sensibles comme le montant des revenus, le patrimoine, le niveau des finances, l'état civil, etc. Avec le RGPD, les banques ne peuvent exploiter ces données sans un consentement préalable clair, explicite et sans équivoque

de la part de leurs clients. Les données collectées doivent par ailleurs être adéquates, pertinentes et limitées. Si les banques veulent exploiter les dépenses de leurs clients pour proposer des services à valeur ajoutée, elles peuvent le faire à condition qu'ils aient manifesté leur adhésion à ce service, en cochant une case ou signant un document, à condition toujours que ce dernier soit spécifique à l'usage qui serait fait de leurs données [34]. Les délais de conservation doivent également être abordés.

Concernant la directive DSP2 dont j'ai parlé dans la première partie, elle se veut également protectrice pour le client en demandant aux prestataires, que les banques doivent désormais laisser accéder à leurs bases de données clients, de ne collecter, traiter et conserver que les données sur les clients nécessaires pour la réalisation du service, avec leur accord explicite, et de ne pas les utiliser à d'autres fins.

II. EVOLUTION DES SERVICES CONFORMITE

La mise en place de process internes propres à la gestion de l'épineuse question des données personnelle est en cours dans de nombreuses banques. Jean-Charles Croiger, Directeur de Capgemini Consulting et expert du secteur bancaire, explique qu'elle peut se faire de différentes manières :

- autour de la fonction du délégué à la protection des données (DPO pour Data Protection Officer), dont le RGDP impose la nomination à toute entreprise collectant les données personnelles de ses clients.
- au sein du service conformité avec la création d'un département dédié
- en lien avec la fonction du Chief Data Officer dont le rôle est de de s'occuper de la transformation digitale et de récupérer les données les stratégiques
- sous la gouvernance de la direction générale

Le management de ce changement pourra se faire soit de manière descendante avec comme objectifs d'appliquer la méthodologie globale définie autour du RGPD ou ascendante avec un traitement très opérationnel du sujet [21].

Un exemple concret est celui mis en place par le Crédit Mutuel Arkea qui a décidé de créer un département dédié à la protection des données. Ce département est rattaché à la direction de la conformité. Comme l'explique le directeur général d'Arkéa Ronan le Moal, ce service est dirigé par un délégué à la protection des données ou DPO pour Data Protection Officer. Ce DPO est en contact régulier avec la CNIL, organisme chargé de veiller à la bonne application du texte du RGPD en France. Un service dédié comme celui-ci se retrouve donc à l'interface avec les différentes entités et filiale du

groupe et se positionne dans un rôle de conseil et d'appui en matière de protection des données personnelles des clients mais aussi de ces collaborateurs [35].

Une conséquence directe de la montée en puissance du service conformité est l'augmentation des effectifs via des recrutements en interne ou en externe. Par exemple, la Banque Postale recrutait en juin 2019 un assistant Chargé de Conformité RGPD & Data en stage.

Le process d'accompagnement des clients sur le sujet délicat de la protection de leurs données personnelles s'est mis en place grâce à une communication adaptée et pédagogue envers les clients. Ainsi, Société Générale dédie sur son internet, une page à la question : https://particuliers.societegenerale.fr/engagements/gestion-donnees-personnelles-rgpd. A travers une FAC (foire aux questions ou frequently asked questions) les clients trouvent des réponses à leurs interrogations sur le traitement de leurs données personnelles et leurs droits. Une adresse mail dédiée est également à leur disposition s'ils n'ont pas trouvé la réponse.

Pour autant, les clients se sentent-ils vraiment concernés ? J'ai pu interroger un directeur d'une agence bancaire. Depuis la mise en place du RGPD en mai 2018, seul un client a demandé à savoir quelles données cette banque possédaient sur lui. C'est le siège à qui la demande avait été remontée qui lui a répondu directement.

Si les entreprises bancaires mettent tant de moyens dans la protection des données personnelles, c'est que la cybercriminalité à leur encontre ne cessent de croître.

CHAPITRE 2 – LA CYBERSECURITE AU CENTRE DES PROCESS BANCAIRES

I. LES SOLUTIONS

Les lois et directives dont j'ai parlé dans la 1ère partie de ce mémoire ont eu un impact fort sur le secteur bancaire. Les banques ont dû se plier à de nouvelles exigences en termes de renforcement des dispositifs de cybersécurité. Considérées comme des opérateurs d'importance vitale (OIV), les banques ont l'obligation de trouver les réponses pour sécuriser leurs systèmes informatiques. Des acteurs, telle la Banque Centrale Européenne, contrôlent leurs actions en ce sens.

En pratique la gestion du risque se manifeste de différentes manières, à la fois basées sur la prévention, la détection et l'innovation.

La prévention :

Sur son site internet, Société Générale oriente ses clients vers une page dédiée à sa sécurité (https://particuliers.societegenerale.fr/securite#vosmoyensdeprotection) avec une liste de bonnes pratiques à adopter lors des consultations en ligne. Elle y propose également un logiciel de sécurité pour sécuriser la connexion.

La détection :

Une sensibilisation des salariés tant en agence qu'en back-office est primordiale : « près de 90 % des attaques au niveau mondial surviennent via les salariés de l'entreprise exemple » [28]. Tout repose sur la connaissance du client, de ses habitudes, pour détecter ce qui est inhabituel. De par mon expérience, avec la clientèle entreprises cette fois, j'ai pu me rendre compte de l'importance de connaitre les habitudes bancaires des clients. Dans le service des moyens de paiements, les équipes arrêtaient régulièrement des virements frauduleux. Ils les identifiaient par exemple car la destination ou le montant du virement était inhabituel.

L'utilisation d'algorithmes permet une analyse automatisée des données compilées, là encore pour détecter des opérations inhabituelles et suspectes et définir la réaction appropriée. Il peut s'agir, d'un virement inhabituel de la part d'une client ou d'une connexion du client à son compte à un horaire inhabituel. A la Société Générale, le Security Operating Center surveille 24h/24 et 7j/7 les infrastructures informatiques et les applications bancaires [28].

Le directeur d'agence que j'ai interrogé m'a expliqué que dans sa banque il y 30 critères qui ont été identifiés comme étant critiques et pouvant ainsi ressortir en alerte en cas de suspicion de fraude.

L'amélioration continue :

Enfin, les banques travaillent à l'amélioration continue de l'inviolabilité de leurs systèmes d'informations pour empêcher les hackers, aux méthodes de plus en plus élaborées de pénétrer les systèmes. Pour reprendre l'exemple cité précédemment de la Bank of Bangladesh, les hackers avaient réussi à attaquer les systèmes SWIFT. Elles n'hésitent pas non plus, « à déployer des leurres dans le système d'information pour piéger et comprendre les méthodes des attaquants » [36].

Les budgets :

Pour répondre aux enjeux de la cybersécurité, les banques ont donc mis les bouchées doubles sur le budget. En réponse à ce piratage informatique à l'automne 2014 qui avait dérobé des noms, numéro de téléphone et adresses électroniques de 76 millions de foyers américains, la JPMorgan, première banque américaine en termes d'actifs, prévoyait en 2016 d'investir 500 millions de dollars dans la cybersécurité, le double de son budget habituel. Société Générale prévoyait fin 2017 un budget cybersécurité de 650 millions d'euros jusqu'à020 [30].

L'innovation :

Face à une cybercriminalité de plus en plus ingénieuse, elles se sont également lancées dans des innovations technologiques et numériques corrélées avec un tout un arsenal de cybersécurité.

Des innovations ont été développées pour sécuriser les paiements à distance :

- Les cartes à cryptogramme dynamique, c'est-à-dire que les trois chiffres figurant au dos de la carte changent toutes les 45 minutes ; des hackers qui se le seraient procurait auraient peu de temps pour l'utiliser.

- Le téléphone comme instrument de validation des paiements à distance avec un système qui associe l'identifiant bancaire du client (son code d'accès aux services en ligne) à son smartphone. Il faudrait alors que le hacker ait pu se procurer l'identifiant bancaire et le smartphone d'un particulier pour commettre sa fraude. Cette technologie à destination des des particuliers s'appelle Pass Sécurité chez Société Générale

- Le recours à la biométrie qui trouve sa source dans l'analyse de caractéristiques physiques comme les empreintes digitales, la forme du visage... ou comportementales comme la reconnaissance vocale. La biométrie « permet l'identification et l'authentification d'une personne à partir de données reconnaissables et vérifiables, qui lui sont propres et sont uniques » [37]. Ainsi, la Banque Postale a obtenu en mars 2016 l'accord de la CNIL (Commission Nationale de l'informatique et des Libertés) pour généraliser à l'ensemble de ses clients ce système d'authentifications pour les paiements à distance. La par biométrie vocale appelée « Talk to Pay » et testé depuis trois ans auprès de 650 clients et collaborateurs. En effet, la CNIL avait jusqu'à présent refusé la conservation d'échantillons biométriques sur un serveur central [30]. De même, Société Générale expérimente également une carte biométrique avec

un capteur d'empreinte digitale. Le client s'authentifie avec son doigt à la place du code PIN après avoir enregistré son empreinte digitale dans la carte biométrique [38]. Enfin, Société Générale a également reçu l'accord de la CNIL pour ouvrir des comptes à distance grâce à la biométrie faciale. Un algorithme compare les pièces d'identité envoyées au préalable à des selfies effectués en direct. « Cette opération d'authentification par biométrie faciale est dix fois plus performante que la reconnaissance humaine » [37].

II. LES NOUVEAUX ENJEUX POSES PAR DSP2

Concernant la directive DSP2, les obligations relatives au RGDP incombant aux banques en matière de sécurité imposent également à ces tiers de sécuriser leurs services en ligne. Il n'en reste pas moins que des acteurs tiers pourront désormais rentrer au cœur même de l'écosystème de sécurité des banques. Or, ils sont très souvent peu matures vis-à-vis de la cybersécurité et de la confidentialité des données [29]. Les banques seront donc obligées d'associer dans leurs démarches de sécurisation de leurs systèmes des tiers pas forcément en mesure ni volontaires pour mettre en place « des moyens de prévention et de détection proportionnels à l'impact potentiel de la cybercriminalité qui s'exercera sur eux et leurs clients » [32]. En cas d'une éventuelle faille dans la sécurité des systèmes des prestataires, l'impact en termes d'image et de conséquences financières risque d'être supporté par les banques.

Plutôt vue comme une contrainte réglementaire, DSP2 semble aller dans le sens d'une fragilisation encore plus accrue de la sécurité des données personnelles des consommateurs et parait antinomique avec l'enjeu de sécurisation de celles-ci imposé par la législation et que nous avons vu auparavant. Néanmoins, d'un point de vue technique, l'accès aux systèmes d'informations des banques se fera via la création d'interfaces de programmation (API pour le terme anglais Applications Programming Interfaces) qui seront des canaux spécialement dédiés aux échanges entre les banques et les acteurs tiers et qui seront donc différents de ceux utilisés par la banque pour les contacts avec ses clients [39]. L'autre avantage est qu'en cas de cyber-attaque ou de fraude sur les systèmes d'informations des banques, il leur sera possible d'identifier qui, des systèmes d'informations des prestataires ou des bases de données clients, ont été ciblés. L'analyse des risques devrait être donc être facilitée.

Enfin, les interfaces de programmation (ou en anglais « Application Programmation Interface » - API) peuvent aussi faciliter la construction de solutions bancaires innovantes avec des partenaires externes [29].

Alors que les banques semblent déjà avoir trouvé des solutions et mis en place des process pour répondre aux enjeux de la sécurisation des données de leurs clients, il reste encore les étapes à franchir et comment les banques peuvent-elles encore tirer profit de ces données ?

PARTIE 3
-
ET DEMAIN ?

CHAPITRE 1 – ENCORE DU TRAVAIL EN TERMES DE CONFORMITE

I. CONTINUER D'INFORMER SUR LE RGPD

L'entreprise Ogury, spécialisée dans le marketing mobile, a mené une enquête mi-février 2019 dans des pays européens dont la France sur le ressenti des consommateurs quant à l'utilisation de leurs données moins d'un an après l'entrée en vigueur du RGPD. 33% des personnes interrogées en France estiment que le RGPD ne leur a pas apporté une meilleure compréhension. Et quand on leur demande ce qu'est le RGPD, 47% d'entre eux disent ne pas savoir. Pour le fondateur de l'entreprise, cela s'explique par le fait que les entreprises n'ont pas suffisamment œuvré à expliquer aux consommateurs l'enjeu de cette directive et à obtenir leur consentement pour utiliser leurs données. C'est pourtant le seul moyen pour qu'elles les rassurent et continuent en parallèle de développer leurs ventes via du marketing digital ciblé [40].

Concernant les banques, il m'a été difficile de d'obtenir les éléments permettant de faire un constat un an après l'entrée en vigueur du RGPD. D'après Thomas Hirtzig, manager au sein du cabinet de conseil Alpha FMC, les banques ont anticipé la protection des données personnelles de leurs clients bien avant la mise en place de la RGPD. « En matière de sécurité, on fait difficilement mieux qu'elles » [34]. Pourtant, même si de nombreuses procédures ont été mises en place, comme je l'ai montré dans la partie précédente de ce mémoire, j'ai été surprise d'apprendre par le directeur d'agence que j'ai interrogé que son équipe n'avait à ce jour suivi aucune formation interne sur le sujet du RGPD. Lors de l'ouverture d'un compte, ce sujet n'est pas non plus abordé avec le client. Il y a sans doute encore du travail à faire ....

II. L'EPINEUX PROBLEME DES DOSSIERS PAPIERS

J'ai été surprise lorsque je travaillais en back-office bancaire, qu'aucune directive n'ait été fournie quant au traitement des données papier, et les documents papier non archivés finissaient tout bonnement à la poubelle. Pas de destructeur de papier ! C'était avant l'ère RGPD, certes, mais les choses ont-elles évoluées ? Les données papier sont en effet tout autant concernées par le RGPD que les autres et les banques, comme toutes les entreprises ne doivent focaliser leurs processus uniquement sur la sécurisation des données numériques. Si les clients fournissent de plus en plus leurs données par e-mail ou par voie numérique, les documents papier sont encore présents. Une fois numérisés, qu'advient-il ensuite de ces documents papier ? Sont-ils détruits correctement ? Ils peuvent être archivés durant une durée légale, mais après ? Un sujet sur lequel je n'ai pas trouvé

d'informations. Gageons que la prise de conscience a eu lieu. En tout cas, les banques semblent ne pas chercher à communiquer sur le sujet.

CHAPITRE 2 – DES INNOVATIONS POUR MIEUX CONNAITRE LE CLIENT

I. UNE MINE D'OR DE DONNEES A EXPLOITER

Les données que possèdent les banques sur leurs clients, tels l'état-civil, l'adresse, le numéro de téléphone, le mail, le montant des revenus, du patrimoine, l'IBAN, mais aussi et surtout les données de paiement, constituent une mine d'or. Les banques peuvent étudier et exploiter les habitudes de consommation de leurs clients à des fins de développement commercial afin de leur proposer des offres ciblées qui permettront de les fidéliser.

L'analyse de l'utilisation des opérations effectuées avec les cartes de paiements permet par exemple d'obtenir des informations sur les habitudes d'achats des clients et la plupart des établissements bancaires pensent aujourd'hui qu'elles sont stratégiques et devraient être mieux exploitées [29].

Le directeur d'agence que j'ai interrogé m'a confirmé que les comptes des clients n'étaient pas encore correctement exploités à ses yeux. Dans sa banque, une liste de contacts prioritaires a néanmoins été éditée pour proposer des assurances et des crédits à la consommation à des clients ciblés en amont.

L'exploitation limitée de ces données peut s'expliquer. Difficile de créer des parcours clients numériques avec des étapes de démarchage, de vente et de suivi des relations à distance et en parallèle respecter les obligations du RGPD relatives à la communication des informations, au recueil du consentement et au devoir de conseil [29]. Néanmoins, d'après une étude du Cabinet Deloitte, même si la question des données personnelles reste une préoccupation des Français, « 58% accepteraient de fournir davantage de données personnelles à leur banque en échange d'un conseil plus personnalisé » [41].

Pour autant, en plus de l'exploitation des données issues des transactions réalisées sur les comptes de leurs clients, certaines banques étudient l'idée d'élargir encore la collecte de leurs données : données socio-économiques, données de conjoncture ou encore données issues des réseaux sociaux [29]. Elles souhaitent ainsi affiner encore davantage leur ciblage client et « leur offrir des services sur-mesure (ajustement de crédit, location d'appartement…) » [36]. Ainsi, comme d'autres banques, BNP Paribas envisage à terme de proposer des offres non bancaires « dans le shopping, la mobilité, le logement ou encore la santé » [42].

II. COMMENT ?

Pour encore mieux tirer profit de la masse exponentielle de données sur leurs clients, que l'on exprime aujourd'hui sous le terme « Big Data », les banques investissent dans de nouveaux outils technologiques tout en gardant toujours à l'esprit leur sécurisation.

Ces nouveaux outils sont basés sur le développement d'algorithmes innovants comme « la reconnaissance optique de caractères », « le traitement automatique du langage naturel » ou « la reconnaissance de formes » [29]. On en parle souvent sous le nom d'intelligence artificielle, car ces algorithmes « permettent la réalisation par des machines de tâches qui font appel à l'intelligence lorsque celles-ci sont réalisées par des humains » [29].

L'algorithme reproduit un modèle. Ainsi il fera une prédiction en fonction de ce modèle. En étudiant le comportement d'achat du client, il en déduira ainsi quel type de produit il faut lui proposer. Le paramétrage de l'algorithme aura préalablement été fait par des équipes informatiques.

Un autre exemple d'application de ce type d'algorithme est le « chatbot » ou agent conversationnel : son intérêt pour l'activité commerciale bancaire est de pouvoir réaliser des échanges avec les clients allant de la simple prise de contact au diagnostic de leurs besoins et à l'apport de conseils ou de solutions. Là encore, un paramétrage humain en amont est nécessaire.

CHAPITRE 3 – NE RIEN LACHER SUR LA CYBERSECURITE

I. LES ALGORITHMES

Un autre intérêt de l'exploitation des données clients est paradoxalement la lutte contre la fraude. Ces mêmes algorithmes, qui en ayant besoin d'une quantité toujours plus importante de données personnelles, accentuent les risques de fraude, peuvent se révéler être un meilleur moyen de lutter contre la cybercriminalité [25]. La détection des fraudes est désormais automatisée et il est possible d'analyser 60 millions de données quotidiennement pour y détecter une anomalie [30].

Les algorithmes permettant simplement de faire des prédictions se cantonnent aux techniques de fraude connues [30]. Par contre, d'autres algorithmes type « machine learning », pour apprentissage automatisé des machines, pourraient s'utiliser pour la détection de schémas de fraude encore inconnus [30]. En se basant sur l'analyse de ce qui a déjà été fait, cet algorithme pourrait en tirer des conclusions et prendre des décisions en autonomie [29].

II. INTEGRER LES START-UP

Alors que les consommateurs continueront d'être en attente de nouveaux services digitalisés, le risque cybercriminel ne cessera de croître. Les banques sont donc obligées de sans cesse développer de nouveaux moyens de détection des fraudes. Certaines d'entre elles ont choisi de miser sur un travail conjoint avec des start-up spécialisées en cybersécurité. Plus souples que les banques en matière de gouvernance et de prise de décision, plus réactives, moins couteuses en frais de fonctionnement, elles apportent des méthodes d''innovation nouvelles.

Comme d'autres banques, la Banque Postale a misé sur les start-up pour qu'elles conçoivent de nouveaux produits innovants, notamment dans le domaine de la cybersécurité, qu'elle espère pouvoir utiliser par la suite. Elle les accueille au sein de son incubateur Platform58 [43].

Société Générale a créé le concours du Banking Cybersecurity Innovation Awards qui met en compétition des start-up et des PME qui recherchent des solutions de cybersécurité dédiées au secteur bancaire. Les lauréats peuvent tester leurs solutions chez Société Générale. [44].

III. LA BLOCKCHAIN

Les banques explorent également de nouvelles innovations technologiques. La blockchain est sans doute l'une des plus disruptives. La blockchain, pour chaine de blocs, repose sur le principe du stockage de données de manière décentralisée, car réparti sur plusieurs serveurs, et infalsifiable car cryptée. Les banques travaillant sur des blockchains privées auxquelles seules les personnes autorisées peuvent accéder, contrairement aux blockchains publiques accessibles à tous, « elles ne posent pas de question particulière de conformité au RGPD » [45]. L'un des usages de la blockchain pour le secteur bancaire serait donc le stockage et la sécurisation des données de leurs clients [29]. Elles pourraient se les échanger avec d'autres banques qui auraient accès à la blockchain sans risque de pertes ou de falsification. Un exemple concret serait la lutte contre le blanchiment et le financement du terrorisme plus performant grâce aux partages des informations entre les banques. Les processus KYC, dont j'ai parlé en partie I, souvent longs et fastidieux pourraient être accélérés avec le stockage de données accessibles à tous les acteurs en charge des contrôles sans risques d'altérations ni de divulgation des données.

IV. LE CLOUD COMPUTING

Certaines banques voient des opportunités dans le cloud computing par rapport à leurs propres datacenters. Si certaines pensent que les conditions de sécurité sont désormais obtenues avec le cloud et qu'il est désormais nécessaire à leur transformation, d'autres sont, au contrainte, plus réticentes à l'utiliser [29]. BNP Paribas est parmi l'une des seules banques en Europe à avoir fait le choix du cloud [46].

V. INVESTIR DAVANTAGE

Pour Emmanuel Germain, directeur adjoint de l'ANSSI, « 5 à 10% du budget informatique d'une organisation doivent être consacrés à la cybersécurité. » [25]. Et l'investissement doit continuer de grossir. Sur 6 milliards d'euros que BNP Paribas investit annuellement en informatique, 400 millions sont dédiés à la cybersécurité, soit 6,6% [46].

CONCLUSION

De par leur activité, les banques sont fortement exposées à la fraude. Elles possèdent des données sensibles sur leurs clients et leurs systèmes d'informations sont victimes régulièrement d'attaques. Un vol de données clients a un impact désastreux sur l'image de marque d'une enseigne bancaire. A mes yeux, le maître mot d'une relation réussie et pérenne est donc la confiance. Les banques n'ont pas le choix, elles doivent assurer la sécurité des opérations de leurs clients et la protection de leurs données stockées.

Mais, bien que la pression ait été mise sur les banques, comme sur les autres entreprises dès 1978 avec la loi « informatique et libertés » et que le RGPD ait encore dernièrement renforcé les droits des clients, il ne s'agit pas seulement pour les banques de respecter les règlementations en vigueur. Les études ont d'ailleurs montré qu'elles avaient pris très tôt ce sujet au sérieux. Elles doivent également démontrer aux clients l'intérêt qu'elles portent à leurs données. Aujourd'hui les clients font confiance à leurs banques à plus de 50% [36]. Conserver cette confiance est donc un chantier primordial pour les banques, d'autant qu'à contrario les ¾ de ces mêmes clients disent qu'ils n'hésiteront pas à aller à la concurrence en cas de problèmes de sécurité impactant leurs données [36].

Dans un secteur où l'attrition est donc forte, ce chantier doit se mener sur deux fronts. Tout d'abord, il faut continuer le dialogue permanent entre le réseau commercial, le back office et les clients afin de conserver cette « connaissance clients ». Ensuite, la stratégie doit être de positionner la cybersécurité au centre même de tous les process d'interactions informatiques entre les banques, les clients qui utilisent les outils digitaux et les acteurs tiers que la directive DSP2 autorise désormais à accéder aux systèmes d'informations des banques.

Conserver cette confiance est d'autant plus important pour les banques que l'environnement concurrentiel est fort et que les clients sont en attente de nouvelles offres et fonctionnalités plus dédiées, et veulent pouvoir accéder à leurs comptes ou traiter des opérations avec leurs banques à partir de leurs ordinateurs, tablettes ou mobiles à n'importe quel moment. Il y a donc également un enjeu commercial important lié aux données. L'offre de nouvelles expériences clients repose désormais sur des outils technologiques qui vont devoir compiler toujours plus de données et demanderont donc toujours plus de cybersécurité et de budget.

Outre les axes d'amélioration sur la partie réglementaire, les banques devront donc prouver leur capacité à s'adapter aux différents enjeux liés à la protection des données personnelles avec des moyens humains, technologiques et financiers.

BIBLIOGRAPHIE ET SITOGRAPHIE

[1]. Ludwig, Hervé (mis à jour le 2 janvier 2019). « Les 50 chiffres à connaître sur les médias sociaux en 2019 », sur le site *BDM*. Consulté le 15 juin 2019. https://www.blogdumoderateur.com/50-chiffres-medias-sociaux-2019/

[2]. Hoadley C.M., Heng X., Joey J.L., Rosson M.B. (2009). "Privacy as information access and illusory control : The case of the Facebook News Feed privacy outcry", ***Electronic Commerce Research and Applications***, vol. 9, n° 1, p. 50-60.

[3]. Barnes S.B. (2006). "A privacy paradox : Social networking in the United States", ***First Monday,*** vol. 11, n° 9, Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312.

[4]. Entreprise et vie privée, Le « privacy paradox » et comment le dépasser ? Bernard Pras, dans Revue française de gestion 2012/5 (N° 224), pages 87 à 94, Cairn.

[5]. Champeau, Guillaume (17 septembre 2014). « 75% des applis mobiles collectent les données personnelles », sur le site *BDM*. Consulté le 12 juin 2019. https://www.numerama.com/magazine/30595-75-des-applis-mobiles-collectent-des-donnees-personnelles.html

[6]. « Bilan 2018 du e-commerce en France » sur le site https://www.fevad.com/bilan-e-commerce-ventes-internet/ Consulté le 16 juin 2019.

[7]. Terré, (2000) « Vie privée, travaux du groupe d'études société de l'information et vie privée », Académie des sciences morales et politiques, rapport final, chapitre 7.

[8]. De Kerautem, Virginie (20 février 2017). « Data centers : mais où se trouvent vos données ?», sur le site *Le Parisien*. Consulté le 23 juin 2019. http://www.leparisien.fr/economie/business/data-centers-mais-ou-se-trouvent-vos-donnees-20-02-2017-6694767.php

[9]. L., Bastien (16 avril 2018). « Les vols de données Cloud ont déjà touché 26% des entreprises ?», sur le site *Le Big data*. Consulté le 23 juin 2019. https://www.lebigdata.fr/mcafee-vols-donnees-cloud

[10]. Karayan, Raphaële (07 juin 2016). « Le cloud computing expliqué aux nuls», sur le site *L'express, l'Expansion*. Consulté le 23 juin 2019. https://lexpansion.lexpress.fr/high-tech/le-cloud-computing-explique-aux-nuls_1384009.html

[11]. « Mobiles : Le nombre d'attaques de malware a doublé en 2018 » sur le site *Kaspersky.* https://www.kaspersky.fr/blog/mobile-malware-report/11503/ Consulté le 16 juin 2019

[12]. « Le piratage d'Equifax dû à une faille informatique non corrigée » sur le site *Le Monde*. Consulté le 20 juin 2019.
https://www.lemonde.fr/pixels/article/2017/10/03/le-piratage-d-equifax-du-a-une-faille-informatique-non-corrigee_5195179_4408996.

[13]. « La réforme de la cybersécurité en Europe » sur le site *Conseil de l'Union Européenne*. Consulté le 21 juin 2019. https://www.consilium.europa.eu/fr/policies/cyber-security/

[14]. Lemoine P. (2000). « Commerce électronique, marketing et liberté », Travaux du groupe d'études société de l'information et vie privée, Académie des Sciences Morales et Politiques, Rapport final (2), chapitre 7.

[15]. « Le baromètre de l'intrusion, 6ème édition 2016 » sur le site *Publicis Eto*. Consulté le 21 juin 2019. http://www.publicis-eto.fr/media/PUBLICIS-ETO_Barometre_2016.pdf

[16]. Entreprise et respect de la vie privée du consommateur. De l'usage autorisé à l'utilisation souhaitable des données personnelles, Régis Dumoulin et Caroline Lancelot Miltgen. Dans Revue française de gestion 2012/5 (N° 224), pages 95 à 109, Cairn.

[17]. Simson Garfinkel, 2000. **«** Database nation: The death of privacy in the 21st century »**.** Sebastopol, Calif.: O'Reilly.

[18]. « Donnée personnelle » sur le site *La CNIL*. Consulté le 19 juin 2019. https://www.cnil.fr/fr/definition/donnee-personnelle

[19]. Wang H., Lee M. et Wang C. (1998), Consumer privacy concerns about Internet marketing, Communications of the ACM, 41, 3, 63-70

[20]. Gurau C., Ranchhod A. et Gauzente C. (2003), To legislate or not to legislate : a comparative exploratory study of privacy-personalisation factors affecting French, UK and US web sites, Journal of Consumer Marketing, 20, 7, 652-654

[21]. Croigier, J.Charles (21 novembre 2016). « La protection des données personnelles : un enjeu critique pour les banque**s**», sur le site *Revue banque*. Consulté le 10 juin 2019 http://www.revue-banque.fr/management-fonctions-supports/article/protection-des-donnees-personnelles-un-enjeu-criti

[22]. « Les français parés pour le RGPD ? » sur le site *Affinion*. Consulté le 19 juin 2019. https://affinion.fr/actualites/les-francais-pares-pour-le-rgpd/

[23]. Rolland, Sylvain (20 septembre 2017). «Cyberattaques : que contient le "paquet cyber" que l'Europe veut voter en 2018 ?», sur le site *La tribune*. Consulté le 21 juin 2019. https://www.latribune.fr/technos-medias/cyberattaques-que-contient-le-paquet-cyber-que-l-europe-veut-voter-en-2018-751009.html ex11'

[24]. « Protection des OIV » sur le site de *l'ANSSI*. Consulté le 21 juin 2019. https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/

[25]. Germain Emmanuel (15 janvier 2018). « Le risque augmente et est à la fois très fort et sous-évalué » sur le site *Revue banque*. Consulté le 20 juin 2019. http://m.revue-banque.fr/risques-reglementations/article/risque-augmente-est-fois-tres-fort-sous-evalue#desc-puce-nbp-1

[26] « La lutte contre le blanchiment de capitaux et le financement du terrorisme », hors-série Les mini-guides bancaires, Les clés de la banque, Fédération bancaire française oct. 2018
https://lesclesdelabanque.com/web/Cdb/Particuliers/Content.nsf/MiniGuideFeuilletableWeb?ReadForm&DocId=7QMFYE

[27]. Ferron, Aurélien (07 juin 2019). « Pourquoi les banques veulent-elles en savoir autant sur vous ? » sur le site *Le Figaro*. Consulté le 07/06/2019 http://www.lefigaro.fr/argent/pourquoi-les-banques-veulent-elles-en-savoir-autant-sur-vous-20190607

[28]. « Cybersécurité : l'innovation par essence » sur le site *Société Générale*. Consulté le 04 juin 2019. https://www.societegenerale.com/fr/cybersecurite-innovation-par-essence

[29]. « Étude sur la révolution numérique dans le secteur bancaire français ». Consulté le 04 juin 2019.https://acpr.banque-france.fr/sites/default/files/medias/documents/as_88_etude_revolution_numerique_secteur_bancaire_francais.pdf

[30]. Lejoux Christine (20 avril 2016) « Les banques face au défi de la cyber criminalité » sur le site *La tribune*. Consulté le 16 juin 2019. https://www.latribune.fr/entreprises-finance/banques-finance/banque/les-banques-face-au-defi-de-la-cybercriminalite-565132.html

[31]. Danton, Benoît (05 septembre 2016) « L'image des banques est à son meilleur niveau depuis 10 ans » sur le site *Fédération française bancaire*. Consulté le 21 juin 2019. http://www.fbf.fr/fr/espace-presse/communiques/l'image-des-banques-francaises-est-a-son-meilleur-niveau-depuis-10-ans

[32]. Delille Gil (15 janvier 2018). « Banque, menaces cyber et évolutions fonctionnelles : la recherche d'un équilibre permanent » sur le site *Revue banque*. http://m.revue-banque.fr/risques-reglementations/article/banques-menaces-cyber-evolutions-fonctionnelles-re

[33]. « RGPD, quel impact pour le secteur bancaire ? » sur le site *BforBank*. Consulté le 26 juin 2019. https://www.bforbank.com/mag/tendances/rgpd-impact-secteur-bancaire.html

[34]. Mignot, Vincent (5 juin 2018). « Banque, que change le RGPD pour vous » sur le site *CBanque*. Consulté le 21 juin 2019. (https://www.cbanque.com/banque/actualites/68389/banque-que-change-le-rgpd-pour-vous

[35]. Mignot, Vincent (29 mai 2018). « RGPD : Arkéa ouvre un département dédié aux données personnelles ». Sur le site *CBanque*. Consulté le 21 juin 2019. https://www.cbanque.com/banque/actualites/68271/rgpd-arkea-ouvre-un-departement-dedie-aux-donnees-personnelles

[36]. Garin, Matthieu et Coulomban, Amaury (15 janvier 2018). « La confiance : levier essentiel pour la transformation numérique ». Sur le site *Revue banque*. Consulté le 21 juin 2019. http://m.revue-banque.fr/risques-reglementations/article/confiance-levier-essentiel-pour-transformation-num

[37]. « Ouverture d'un compte à distance grâce à la biométrie » sur le site *Société Générale*. Consulté le 19 juin. https://www.societegenerale.com/fr/innovation-et-digital/services-innovants/ouverture-compte-distance-biometrie.

[38]. « Société Générale première banque en France à expérimenter la carte biométrique » sur le site *Société Générale*. Consulté le 19 juin. https://www.societegenerale.com/fr/newsroom/societe-generale-experimentation-carte-biometric

[39]. « Report on innovative uses of consumer data by financial institutions » sur le site *European banking authority.* Consulté le 19 juin 2019.
https://eba.europa.eu/documents/10180/1720738/Report+on+Innovative+uses+of+data+2017.pdf

[40]. « RGPD : les consommateurs restent dans le flou » sur le site *Comarketing news*. Consulté le 21 juin. https://comarketing-news.fr/rgpd-les-consommateurs-restent-dans-le-flou/

[41]. « Relation banques et clients – 8ème édition » sur le site *Deloitte*. Consulté le 26 juin 2019. https://www2.deloitte.com/fr/fr/pages/services-financier/articles/relations-banques-clients.html

[42]. Lederer, Edouard (20 juin 2019). « Comment BNP Paribas s'inspire des géants du Net pour mieux leur résister ». Les Echos, p. 28.

[43]. Guinot, Danièle (mis à jour le 07/02/2019). « La Banque Postale mise sur les start-up ». sur le site *Le Figaro.* Consulté le 16 juin. http://www.lefigaro.fr/societes/2019/02/07/20005-20190207ARTFIG00007-la-banque-postale-mise-sur-les-start-up.php

[44]. « Quatre startups lauréates des « Banking Cybersecurity Innovation Awards « sur le site Société Générale». Consulté le 21 juin. https://www.societegenerale.com/fr/newsroom/Quatre-startups-laureates-Banking-Cybersecurity-Innovation-Awards

[45]. « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? » sur le site de La CNIL. Consulté le 21 juin 2019.
https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles

[46]. Bonnafe, J.Laurent (13 mai 2019) « Notre budget IT dépasse les 6 milliards d'euros à l'année », Jean-Laurent Bonnafé - Les Echos » sur le site BNP Paribas **»**. Consulté le 26 juin 2019. https://group.bnpparibas/actualite/budget-it-depasse-6-milliards-euros-annee-jean-laurent-bonnafe-echos

TABLES DES FIGURES