



LE REVEIL DE LA VIE PRIVEE

PRIVACY TECH

GARANTIR LE FUTUR VISAGE DU MONDE NUMERIQUE

Nous devons prendre position pour concevoir un univers numérique respectueux des droits et des libertés.

Ce mémoire a été présenté pour le Prix du Meilleur Mémoire AFCDP 2016
par Alessandro FIORENTINO
Ambassadeur du Privacy by Design et Vice-Président de la Privacy Tech

Préface de Gérard PELIKS
Président de l'association CyberEdu
Lieutenant-colonel de gendarmerie dans la Réserve Citoyenne de Cyberdéfense
(DGGN) et membre du Conseil d'Administration de l'Association des Réservistes du
Chiffre et de la Sécurité de l'Information (ARCSI)

PRÉFACE

Le nécessaire besoin de sécurité doit-il restreindre l'aspiration légitime à la liberté ? Vaste et difficile question ! La liberté d'un citoyen doit-elle s'arrêter là où la sécurité d'un autre citoyen commence ? Gros dilemme !

Nous allons vers de plus en plus de dépendance au numérique avec les technologies qui émergent. Citons par exemple les algorithmes qui traitent l'information que nous donnons sur nous-mêmes et le plus souvent à notre insu. Citons les objets connectés intelligents qui diffuseront nos moindres faits et gestes, et parfois entre eux, dans un temps pas très lointain. Il devient évident que se posera la question : comment puis-je garder pour moi l'information que je ne souhaite pas diffuser ?

Pour assurer, autant que faire se peut, la confidentialité de son information sensible, autrement dit pour avoir la garantie que son information sensible ne pourra être lue que par les personnes autorisées, et même parfois seulement par soi-même, il est une technique incontournable : le chiffrement. Cette technique peut également garantir l'intégrité de son information chiffrée, autrement dit que seuls ceux qui sont autorisés à modifier cette information puissent le faire. L'intégrité peut également établir l'authenticité de l'auteur de cette information.

Avec les directives et les règlements européens, en particulier le Règlement Général sur la Protection des Données, qui sont applicables, ou le seront à très court terme, pour établir ou rétablir la confiance que les citoyens peuvent accorder aux prestataires, l'ensemble des entreprises de part le monde qui traitent de données personnelles de citoyens résidant dans les pays membres de l'Union Européenne devra se conformer aux décisions de l'Europe, sous peine de lourdes sanctions. Les utilisateurs auront ainsi l'assurance que leurs données resteront dans un espace de confiance, protégées par le cadre juridique européen.

Cet ouvrage de M. Alessandro Fiorentino a le mérite, dans sa première partie, d'exposer clairement les menaces qui pèsent sur la vie privée des personnes qui résident sur le sol européen et les contre-mesures que les organisations doivent mettre en place pour protéger les données à caractère personnel qui leur sont confiées, ne serait-ce que pour se mettre en conformité avec le Règlement Général sur la Protection des Données.

Pour protéger les données sensibles, une solution acceptable est donc de les chiffrer. La deuxième partie de l'ouvrage décrit de manière très compréhensible, même si on ne possède pas déjà les bases de la cryptologie, différentes techniques de chiffrement et d'échanges de clés. Ainsi sont expliqués le chiffrement à clé symétrique utilisé pour chiffrer et déchiffrer les fichiers sensibles et le chiffrement asymétrique, dit encore chiffrement à clé publique qui permet de faire transiter la clé de chiffrement symétrique, de manière

sécurisée même sur un réseau public qui ne l'est pas, comme l'Internet. Les données sensibles doivent également conserver leur intégrité. Le calcul d'empreinte et le chiffrement à clé publique permettent de signer un document ou une donnée. Sans entrer dans des détails trop techniques, ni décrire les algorithmes qui nécessitent, pour être compris, des bases mathématiques très poussées, cet ouvrage nous donne les clés indispensables pour appréhender cette discipline si mystérieuse, si complexe mais si indispensable qu'est la cryptologie.

La dernière partie aborde des innovations qui s'ajouteront, quand elles sortiront des laboratoires de recherche, aux technologies décrites et dès maintenant utilisables. Ainsi le chiffrement homomorphe permettra d'utiliser le Cloud quand on y met des données sensibles, donc qu'il faut chiffrer, non seulement comme un espace de stockage mais aussi comme un espace de calcul. Effectuer des calculs sur des données chiffrées et obtenir un résultat qui déchiffré est le même que celui qu'on aurait obtenu si le calcul avait été effectué sur des données en clair ... est-ce un rêve ? Non, c'est une réalité grâce aux mathématiques et au chiffrement homomorphe. Mais aujourd'hui des améliorations restent à faire pour que cette technologie soit applicable dans tous les cas.

Merci à Alessandro Fiorentino pour avoir évoqué ces technologies complexes avec des mots simples, et bravo pour cet ouvrage qui a le mérite d'évoquer des solutions aux bouleversements qu'on peut attendre du Règlement Général sur la Protection des Données. Ce règlement sera garant de la confiance des utilisateurs envers leurs prestataires mais aussi impliquera de gros travaux pour les prestataires qui font des traitements sur les données à caractères personnel de leurs clients. Ces prestataires devront impérativement se mettre en conformité avec ce règlement. C'est ce que cet ouvrage a le mérite d'avoir décrit.

Gérard PELIKS
Expert sécurité de l'Information
Président de l'association CyberEdu

RÉSUMÉ

Le règlement général sur la protection des données personnelles du 27 avril 2016 a pour objectif le renforcement des droits des citoyens et la modernisation du cadre juridique existant permettant à l'Europe de faire face à l'essor du numérique et à la mondialisation. Il a été publié le 4 mai 2016 et sera applicable le 25 mai 2018 dans tous les pays de l'Union Européenne (UE).

L'article 34 du règlement impose que toute violation de données à caractère personnel fasse l'objet d'une communication aux personnes concernées. Ce même article introduit toutefois plusieurs exceptions, notamment si le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées aux données affectées par ladite violation, telles que le chiffrement.

La problématique principale de ce mémoire repose sur une seconde lecture de l'article 34 du règlement : Dans quelle mesure l'article 34 al. 3a du règlement introduit-il une incitation au chiffrement, en tant qu'exonération privilégiée à l'obligation d'information des personnes concernées par une violation de données ?

REMERCIEMENTS

Pour commencer nous souhaitons remercier **Madame Armande BRU-FRANCOIS**, Secrétaire Générale de l'Association PRIVACY TECH pour ses remarques et relectures avisées ainsi que le soutien qu'elle porte à notre démarche.

Nous remercions particulièrement **Monsieur Gérard PELIKS** pour son soutien et sa contribution dans la rédaction de la préface de ce mémoire.

Nous adressons nos sincères remerciements à **Monsieur Jan Philipp ALBRECHT**, Vice-Président de la Commission des libertés civiles de la justice et des affaires intérieures et rapporteur du Parlement européen sur la réglementation de la protection des données, pour sa disponibilité, son soutien, le temps qu'il a consacré pour répondre à nos questions nous permettant d'obtenir sa vision sur notre lecture de l'article 34.

Nous tenons également à remercier **Monsieur Christian HARTZ**, Directeur Technique et Associé du Cabinet Infhotep pour son investissement à travers nos différents échanges.

Sans oublier **Monsieur Christian DES LAURIERS**, Fondateur du Cabinet Infhotep pour son soutien et son engagement dans la mise en place de l'offre Informatique et Libertés du cabinet et **Monsieur David BESSOT**, Associé du Cabinet Infhotep pour avoir initié cette belle aventure.

TABLE DES MATIERES

PRÉFACE	2
INTRODUCTION	7
CHAPITRE 1 - LE REVEIL DE LA VIE PRIVEE	10
1. CITOYENS SOUS SURVEILLANCE	11
1.1. Le panoptique numérique	11
1.2. Un monde post-Snowden	12
1.3. Les attentats au service de la surveillance	12
1.4. Quis custodiet ipsos custodes ?	13
2. LE CHIFFREMENT AU COEUR DU DEBAT	14
2.1. Apple et Google généralisent le chiffrement par défaut	14
2.2. Poker menteur à Cupertino	15
2.3. Schizophrénie du gouvernement français	16
2.4. La Commission Nationale Informatique et Libertés prend position	17
2.5. Syndrome d'Asperger Place Beauvau	17
3. ADOPTION DU REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES	18
3.1. L'article 34 du règlement européen	19
3.2. Les nouvelles obligations à prendre en compte	22
3.3. Le rôle du Data Protection Officer	24
CHAPITRE 2 - LE RETOUR DU CHIFFREMENT	25
1. LA CRYPTOLOGIE	25
1.1. La cryptographie, un élément clé	25
1.2. Le contrôle d'intégrité	29
1.3. Le chiffrement symétrique	31
1.4. Le chiffrement asymétrique	33
1.5. La tokenisation	34
1.6. L'obfuscation du code	35
2. MISE EN ŒUVRE DES DISPOSITIFS TECHNIQUES	36
2.1. Activer un compte utilisateur ou modifier un mot de passe oublié.	36
2.2. Chiffrement symétrique ou asymétrique lequel choisir ?	37
2.3. Assurer la réversibilité d'un document chiffré.	37
2.4. L'authentification forte	38
3. UN PARADIGME A SOMME POSITIVE	44
3.1. L'impact sur l'expérience utilisateur	44
3.2. Une dichotomie pour le business ?	45
4. INNOVATIONS ET PROSPECTIVES	46
4.1. Le chiffrement homomorphe	46
4.2. L'informatique ubiquitaire, le dernier défi	48
CONCLUSION	50

INTRODUCTION

Tout a commencé le 5 juin 2013. Une longue série d'articles de presse a mis la lumière sur plusieurs programmes de surveillance mis en place par la NSA. Ces articles reposaient sur un grand nombre de documents, fournis par Edward Snowden, un ancien sous-traitant de l'agence choqué par l'étendue de la surveillance diligentée par son pays au détriment du droit à la vie privée.

La confiance que les 2,749 milliards de personnes connectées¹ en 2013 avaient placée dans la toile suite à l'avènement de l'internet et des réseaux sociaux s'envola, réduisant les grandes firmes américaines impliquées à de simples informateurs de la NSA lui permettant d'aspirer de nombreuses données et propulsant au cœur du débat la question de la protection des données à caractère personnel.

Plongés dans l'ère post-Snowden, les géants du net ont alors changé leur politique de protection des données introduisant la généralisation du chiffrement par défaut pour combattre les programmes de surveillance mis en place par les États-Unis afin de regagner la confiance des utilisateurs et ne plus être en mesure de répondre aux demandes des autorités américaines.

Ces initiatives n'ont pas été accueillies avec enthousiasme par la NSA et le FBI privilégiant des impératifs de sécurité nationale dans un contexte de menaces terroristes.

En France, la loi relative au renseignement promulguée en juillet 2015 a considérablement renforcé les pouvoirs de surveillance. L'équilibre entre protection des données personnelles et surveillance est au centre de nombreuses préoccupations. Face aux attentats de janvier et novembre 2015, de nombreuses mesures ont été mises en place réduisant un peu plus les libertés fondamentales des citoyens et remettant en question le droit au chiffrement.

¹ Selon les derniers chiffres communiqués par l'UIT (Union Internationale des Télécommunications), le monde comptait 2,749 milliards d'internautes au premier trimestre 2013 soit 38,8 % de la population mondiale.

Le règlement général sur la protection des données du 27 avril 2016² a quant à lui pour objectif le renforcement des droits des citoyens et la modernisation du cadre juridique existant permettant à l'Europe de faire face à l'essor du numérique et à la mondialisation. Il a été publié le 4 mai 2016 et sera applicable le 25 mai 2018 dans tous les pays membres de l'Union Européenne.

L'article 34 du règlement impose que toute violation de données à caractère personnel fasse l'objet d'une communication aux personnes concernées. Ce même article introduit toutefois plusieurs exceptions, notamment si le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées aux données affectées par ladite violation, telles que le chiffrement.

La problématique principale de ce mémoire repose sur une seconde lecture de l'article 34 al.3a du règlement, à savoir, dans quelle mesure introduit-il une incitation au chiffrement, en tant qu'exonération privilégiée à l'obligation d'information des personnes concernées par une violation de données. Ainsi, l'obligation de communication aux personnes concernées ne serait qu'un premier degré de lecture de l'article 34 al 3a, favorisant en réalité la position de l'UE vers davantage de chiffrement.

Dans une première partie, nous présenterons le contexte actuel confrontant la sécurité aux libertés fondamentales des citoyens. Nous analyserons les différentes lectures qui peuvent en découler, les événements liés à ce contexte, les solutions permettant aux citoyens d'optimiser leur droit à la vie privée, les différentes positions prises concernant le chiffrement, ainsi que les nouvelles obligations pour les entreprises et les Data Protection Officers introduites par les dispositions du règlement général sur la protection des données.

Dans un second temps nous procèderons à une revue de l'ensemble des différents types de chiffrement, nous verrons comment les mettre en place en nous appuyant sur des exemples de notre propre expérience professionnelle et analyserons les impacts liés à ces dispositifs techniques.

² 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

<http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR>

In fine, nous étudierons les innovations et les perspectives à venir dans les années futures. Cela nous permettra d'imaginer des mises en œuvre possibles à l'horizon 2020.

CHAPITRE 1 - LE REVEIL DE LA VIE PRIVEE

La protection de la vie privée fait partie des droits fondamentaux. Le droit à la vie privée a été adopté et proclamé par l'Assemblée générale des Nations-Unies dans sa résolution 217 (III) du 10 décembre 1948 dans l'article 12 de la Déclaration universelle des droits de l'homme³.

«Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes»

Ce droit aujourd'hui inquiété par le contexte ambiant lié au développement permanent des nouvelles technologies et à la menace terroriste, conditionne également d'autres droits et libertés telles que la liberté d'association et d'expression eux-mêmes considérés comme des fondements de la démocratie⁴.

La faculté d'un peuple à exercer son droit à la vie privée est un indicateur mesurant le degré de liberté dans une société.

³ Le 10 décembre 1948, les 58 États Membres qui constituaient alors l'Assemblée générale ont adopté la Déclaration universelle des droits de l'homme à Paris au Palais de Chaillot ([résolution 217 A \(III\)](http://www.un.org/fr/documents/udhr/)).
<http://www.un.org/fr/documents/udhr/>

⁴ Le terme démocratie (du grec ancien δημοκρατία / dēmokratía, aujourd'hui souvent interprété comme « souveraineté du peuple », combinaison de δῆμος / dêmos, « peuple » et κράτος / krátos, « pouvoir », ou encore kratein, « commander ») désigne le régime politique dans lequel le peuple a le pouvoir. Selon la célèbre formule d'Abraham Lincoln (16e président des États-Unis de 1860 à 1865) prononcée lors du discours de Gettysburg, la démocratie est « le gouvernement du peuple, par le peuple, pour le peuple ». C'est l'une des définitions canoniques couramment reprise, ainsi qu'en témoigne l'introduction de la Constitution de 1958 de la Cinquième République française.
<https://fr.wikipedia.org/wiki/Démocratie>

1. CITOYENS SOUS SURVEILLANCE

La surveillance de masse a une influence sur le comportement des individus. En effet le fait de se penser surveillé, même si ce n'est pas le cas, entraîne à se conformer à une conduite prédéterminée, à l'autocensure, à l'obéissance et à la soumission.

Selon l'avocat Glenn Greenwald⁵ : « *La surveillance de masse crée une prison dans l'esprit qui est bien plus subtile mais bien plus efficace pour favoriser la conformité aux normes sociales, bien plus effective que la force physique ne pourra jamais l'être*⁶ »

Nous étudierons dans cette première partie la déclinaison du panoptique dans un monde numérique, les impacts liés aux révélations d'Edward Snowden, les relations entre le terrorisme et la surveillance ainsi que les éléments garantissant le respect d'un cadre juridique.

1.1. Le panoptique numérique

Créé à la fin du XVIII^e siècle par le philosophe Jeremy Bentham et son frère, Samuel Bentham, le panoptique est un modèle d'architecture carcérale. Ce dispositif consiste à placer un surveillant dans une tour centrale lui permettant d'observer chaque prisonnier. Ces derniers enfermés dans des cellules individuelles autour de la tour, ignorent s'ils sont surveillés ou non. L'effet du panoptique est d'induire chez le détenu un sentiment d'omniscience invisible.

Les programmes de surveillance électronique par la collecte de renseignements à partir d'Internet constituent un panoptique numérique fondé sur le modèle de Bentham. Placés au cœur du réseau, ils offrent aux gouvernements un pouvoir de contrôle et de surveillance à l'échelle mondiale jamais atteint dans l'histoire. La généralisation de cette surveillance a une influence sur l'ensemble de la population entraînant une normalisation des comportements.

⁵ Glenn Greenwald (né le 6 mars 1967) est un journaliste politique, avocat, blogueur et écrivain américain. À partir de 2013, il commence à publier les révélations d'Edward Snowden sur les programmes de surveillance de masse (PRISM, XKeyscore) des citoyens, entreprises et États du monde entier par la NSA

https://fr.wikipedia.org/wiki/Glenn_Greenwald

⁶ L'importance de la vie privée :

https://www.ted.com/talks/glenn_greenwald_why_privacy_matters?language=fr

1.2. Un monde post-Snowden

Suite aux révélations d'Edward Snowden sur les programmes de surveillance utilisés par le gouvernement américain, nous avons pu constater un changement de posture des géants du web. Conscients de l'image renvoyée auprès de l'ensemble des utilisateurs et des incidences économiques possibles en cas de boycott, Apple et Google ont donc changé leur politique de protection des données personnelles intégrant le chiffrement par défaut.

Considérée jusque-là comme une contrainte légale faisant obstacle à la fonction mercatique et au développement de l'offre, la protection des données est devenue une priorité dans l'optique de regagner la confiance des utilisateurs perdue au fil des révélations.

Ces pratiques ont bouleversé la perception de la sécurité et de la vie privée sur le web et ont soulevé des questions majeures liées à l'architecture et la gouvernance mondiale de l'Internet.

1.3. Les attentats au service de la surveillance

Sous l'impulsion des inquiétudes légitimes des citoyens sur la protection de données, l'utilisation du chiffrement n'a pas été accueillie avec enthousiasme par l'ensemble des agences de renseignement occidentales justifiant leur position par l'importance actuelle de la menace terroriste. La possibilité de déjouer d'éventuels projets d'attentats justifierait la surveillance de millions de citoyens et de nombreux dirigeants à travers le monde.

Initialement introduits à la suite des attentats du 11 septembre 2001, ces dispositifs de surveillance sont omniprésents. En France les lois sur le renseignement se multiplient élargissant au fur et à mesure le spectre d'écoute et de captation des données particulièrement attentatoires aux libertés fondamentales.

Il convient de garder à l'esprit que le problème se trouve aujourd'hui dans la grande difficulté d'analyse de l'information de masse. Dès juillet 2009, un rapport de l'ensemble des inspections générales des services de renseignement américain avait conclu sur le rôle limité de la surveillance de masse dans le succès des opérations contre-terroriste.

« Il est difficile de citer des cas précis dans lesquels ces dispositifs ont directement contribué à des succès contre-terroristes⁷ ».

A la lecture de ces conclusions nous pouvons nous demander si ces programmes de surveillance visent réellement à prévenir les actes de terrorisme. Giorgio Agamben dans son article « De l'Etat de droit à l'Etat de sécurité⁸ » publié le 23 décembre 2015 souligne un risque de relation systémique entre le terrorisme et les Etats sécuritaires appliquant une politique de surveillance *« si l'Etat a besoin de la peur pour se légitimer, il faut alors, à la limite, produire la terreur ou, au moins, ne pas empêcher qu'elle se produise ».*

1.4. Quis custodiet ipsos custodes ?

Une des questions que de nombreux défenseurs des libertés fondamentales se posent est de savoir qui surveille ceux qui nous surveillent ?

Aux Etats-Unis c'est la Foreign Intelligence Surveillance Court qui a pour mission de superviser les demandes de mandats autorisant une opération de surveillance. Cette cour s'appuie sur la loi FISA (Foreign Intelligence Surveillance Act) pour instruire les demandes. De 1979 à 2012, la cour a reçu 33 949 demandes de mandats et en a accepté 99,97% (soit 11 rejets en 33 ans)⁹¹⁰.

En France, depuis 1991 la Commission nationale de contrôle des interceptions de sécurité (CNCIS) doit s'assurer de la légalité des autorisations d'interception. Cette autorité administrative indépendante a été présidée par Jean-Marie Delarue de 2014 à septembre 2015. Reprochant au gouvernement de n'avoir pas réussi à trouver l'équilibre entre exigence de sécurité et libertés individuelles, Jean-Marie Delarue a confirmé qu'il ne souhaitait pas être désigné à la présidence de la nouvelle Commission nationale de contrôle des techniques

⁷ Unclassified Report on the Resident's Surveillance Program, 10 July 2009 : <https://fas.org/irp/eprint/psp.pdf>

⁸ Giorgio Agamben : « De l'Etat de droit à l'Etat de sécurité » : http://www.lemonde.fr/idees/article/2015/12/23/de-l-etat-de-droit-a-l-etat-de-securite_4836816_3232.html

⁹ Perez Evan, « Secret Court's Oversight Gets Scrutiny », The Wall Street Journal, 9 juin 2013

¹⁰ « Foreign Intelligence Surveillance Act Court Orders 1979–2012 », Electronic Privacy Information Center, 4 mai 2012 (consulté le 12 juillet 2013)

de renseignement (CNCTR) lors de son audition par la commission d'enquête du 16 septembre 2015¹¹.

« Le mois dernier, j'ai demandé à ne pas figurer parmi les membres proposés par le vice-président du Conseil d'État. Disons que s'il avait voulu penser à moi, je l'en ai dissuadé, parce que je pense que la loi sur le renseignement d'une part, et les techniques de saisine des données d'autre part, ne me donnent pas les garanties d'un contrôle suffisant. Par conséquent, je ne souhaite pas m'y associer »

Nous vous laissons tirer seuls les conclusions de cette décision prise par Jean-Marie Delarue.

2. LE CHIFFREMENT AU COEUR DU DEBAT

L'ensemble des faits et des éléments présentés précédemment ont propulsé au cœur du débat le chiffrement. Serait-il le dernier recours garantissant aux citoyens ce droit à la vie privée proclamé dans l'article 12 de la Déclaration universelle des droits de l'homme ?

Dans cette seconde partie, nous reviendrons sur les mesures mises en œuvre par Apple et Google pour regagner la confiance des utilisateurs, nous analyserons les dessous du bras de fer qu'a mené Apple face au FBI, les divergences au sein du gouvernement français concernant le chiffrement ainsi que la position de la CNIL sur ce sujet.

2.1. Apple et Google généralisent le chiffrement par défaut

L'intégration du chiffrement par défaut dans l'iOS 8 et Android Lollipop suite aux révélations de l'été 2013 fut une prise de position inédite par les géants du web. Considérés jusque-là comme des firmes peu respectueuses de la vie privée de leurs clients et régulièrement mises en cause par la Commission Nationale Informatique et Libertés (CNIL), Apple et Google se sont improvisés défenseurs des libertés fondamentales. Représentant 95% du marché des mobiles, l'évolution de leur politique de protection des données personnelles a

¹¹ Audition de Jean Marie Delarue de la Commission nationale consultative des interceptions de sécurité : <https://www.youtube.com/watch?v=dutUxYNAG2I>

profondément changé le décor du monde du renseignement. Suite à la généralisation du chiffrement, Apple et Google ne sont parfois plus en mesure de répondre aux nombreux mandats de perquisition de données des autorités. Cette situation déclencha de multiples propositions d'intégration de portes dérobées dans les systèmes de chiffrement mis à disposition des citoyens.

2.2. Poker menteur à Cupertino

Dans le cadre de l'enquête sur l'attaque terroriste du 2 décembre 2015 de San Bernardino, faisant 14 victimes et 21 blessés en Californie, les policiers ont demandé en février 2016, à Apple l'accès à une partie du contenu chiffré de l'iPhone 5C d'un des terroristes.

Suite au refus d'Apple d'aider la police, la justice californienne a finalement demandé à la firme, dans une décision du 16 février 2016, de fournir au FBI un logiciel pour déverrouiller le téléphone du suspect, sans risque d'effacement des données qu'il contient après 10 tentatives erronées de saisie du code.

Ce dispositif impliquait inévitablement l'intégration d'une porte dérobée « backdoor » au sein du système de chiffrement mis en place par Apple.

Mais Tim Cook, le PDG d'Apple, resta sur sa position mettant en avant le Premier Amendement, le droit à la vie privée et les risques de dérives d'une telle atteinte au chiffrement. Il qualifia la décision de la cour de justice californienne de « mesure sans précédent » menaçant la sécurité des clients d'Apple¹², engageant un bras de fer médiatique avec le gouvernement américain en refusant publiquement de se plier à la demande du FBI.

Après le ralliement à la cause d'Apple de la majorité des géants du web et de l'Union américaine pour les libertés civiles, les autorités américaines ont finalement annoncé quelques heures avant l'audience du lundi 28 mars 2016, que le FBI était désormais capable d'accéder au contenu de l'iPhone d'un des terroristes de San Bernardino.

¹² Lettre du 16 février 2016 de Tim Cook destinée aux clients d'Apple
<http://www.apple.com/customer-letter/>

Ce retournement inattendu est considéré par beaucoup de spécialistes comme un abandon stratégique du ministère de la justice ne souhaitant pas créer une jurisprudence en faveur de la sécurité et de la protection de la vie privée des clients d'Apple.

2.3. Schizophrénie du gouvernement français

En France, la Ministre de la Justice Christiane Taubira et le Ministre de l'Intérieur Bernard Cazeneuve estimaient dès septembre 2015 que le chiffrement systématique n'apportait qu'un « gain minime » aux citoyens, mais qu'il mettait en péril leur sécurité.

Le 10 mars 2015, le Ministre de l'Intérieur Bernard Cazeneuve avait également donné son soutien au FBI dans l'affaire qui l'opposait à Apple.

Une seule voix dissonante en la personne d'Axelle Lemaire, secrétaire d'Etat au numérique, avait retenti défendant le droit au chiffrement et la position de l'ONU, formalisée dans un rapport¹³ de mai 2015 s'opposant aux portes dérobées « backdoors » et demandant une nouvelle fois de garantir le droit au chiffrement.

Malgré une large contribution citoyenne lors de la consultation publique organisée en préparation du projet de loi pour une République Numérique, le gouvernement s'est opposé au chiffrement intégral. Toutefois plusieurs amendements dont l'objectif était d'encadrer les portes dérobées et d'imposer de fortes amendes pour les firmes comme Apple et Google en cas de refus d'accès aux données stockées ont été rejetées.

Le 3 mars 2016, le nouveau garde des Sceaux Jean-Jacques Urvoas estimait lors de la Commission des lois à l'Assemblée nationale que la réponse devait être européenne et qu'une loi nationale n'était pas une réponse adaptée pour faire plier les géants du web.

« La réponse doit être européenne, sinon internationale. La loi nationale ne nous paraît être pas le mode opératoire le plus efficace pour faire plier des structures aussi influentes qu'Apple et Google »

¹³ Rapport annuel, le chiffrement des communications et le respect des droits de l'homme
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

2.4. La Commission Nationale Informatique et Libertés prend position

Le 8 avril 2016, la CNIL pris également position pour le droit au chiffrement estimant qu'il contribuait à « la résilience de nos sociétés numériques et de notre patrimoine informationnel¹⁴ ».

La CNIL s'est, par la même occasion, opposée à la mise en place de portes dérobées ou de clés maîtres qui fragiliserait l'avenir de l'écosystème du numérique.

Concernant le rôle du chiffrement dans le cadre des procédures judiciaires, l'autorité administrative indépendante rappelle que plusieurs solutions existent pour accéder aux données lors d'une enquête et que les personnes mises en cause ont l'obligation de coopérer en particulier de fournir les clés de déchiffrement sur demande des autorités.

La CNIL a également souligné que la protection de données personnelles était garantie par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, et que le chiffrement apparaissait donc comme un élément majeur permettant de faire face à la révolution numérique et l'étendue de la surveillance internationale.

2.5. Syndrome d'Asperger Place Beauvau

A l'issue du conseil de défense du 11 août 2016, Bernard Cazeneuve a annoncé vouloir lancer une initiative européenne visant à limiter le chiffrement des communications.

Cette actualité a entraîné la publication d'une tribune dans le journal le Monde « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible¹⁵ » signée par une vingtaine de personnalités, dont Isabelle Falque-Pierrotin, présidente de la CNIL, et plusieurs membres du Conseil national du numérique.

Néanmoins, le 23 août 2016, Bernard Cazeneuve a rencontré son homologue allemand Thomas de Maiziére afin d'adopter une position commune.

¹⁴ Quelle position de la CNIL en matière de chiffrement ?

<https://www.cnil.fr/fr/les-enjeux-de-2016-3-quelle-position-de-la-cnil-en-matiere-de-chiffrement>

¹⁵ « Chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible »

<http://cnnumerique.fr/tribune-chiffrement/>

Comment notre Ministre de l'Intérieur peut-il faire abstraction de la position de la CNIL, du Conseil national du numérique, de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)¹⁶ ? Il semble ignorer qu'un règlement européen sur la protection des données a été adopté récemment. Axelle Lemaire, Secrétaire d'État au Numérique lui a-t-elle expliqué que la loi pour une République numérique adoptée en juillet 2016, confie à la CNIL la promotion de « l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données » ?

3. ADOPTION DU REGLEMENT EUROPEEN SUR LA PROTECTION DES DONNEES

L'adoption du règlement général sur la protection des données¹⁷ du 27 avril 2016 par le Conseil et le Parlement européen est l'aboutissement d'un projet de règlement publié le 25 janvier 2012 par la Commission Européenne.

Le règlement 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, abrogeant la directive 95/46/CE sera applicable à partir du 25 mai 2018 dans tous les pays membres de l'Union européenne. Pour les entreprises, le compte à rebours a commencé. Une prise de conscience à la hauteur de l'importance que représente le sujet de la protection des données personnelles paraît aujourd'hui inévitable. Il conviendra d'être en mesure de faire face au cadre juridique européen introduit par le règlement avant la date d'application.

Pour beaucoup d'experts de la profession, l'apparition de nombreux nouveaux principes et la présence dans le règlement d'une multitude de principes déjà existant dans des textes fondamentaux pourrait être le signe qu'un réveil est déjà en cours.

¹⁶ Cyberdéfense : interdire le chiffrement est "irréaliste"

http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/cyberdefense-interdire-le-chiffrement-est-irrealiste-23-01-2015-1899054_506.php

¹⁷ Règlement Général sur la Protection des Données

<http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR>

3.1. L'article 34 du règlement européen

L'article 34 du règlement intitulé « Communication à la personne concernée d'une violation de données à caractère personnel », indique que, « lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation à la personne concernée dans les meilleurs délais »

Voici l'article 34 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 dans son intégralité :

Article 34 - Communication à la personne concernée d'une violation de données à caractère personnel

1. *Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.*
2. *La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).*
3. *La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:*

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. *Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.*

Extrait du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Comme nous pouvons le constater, l'alinéa 3 introduit plusieurs exceptions, notamment lorsque le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement.

Nous étudierons donc l'ensemble des dispositifs existant et les différents cas d'usage dont leur mise en œuvre sera développée dans le second chapitre : « LE RETOUR DU CHIFFREMENT ».

Nous considérons que l'élément principal de cet alinéa 3a repose sur son orientation pour le chiffrement. En effet, comme nous avons pu le constater précédemment, le sujet du chiffrement est au cœur du débat, confrontant les partisans, la plupart défenseurs de libertés fondamentales et leurs détracteurs représentés par les gouvernements ou les agences de renseignement considérant le chiffrement comme un obstacle à la surveillance généralisée mise en place sur le web.

Or, le législateur européen, en prenant cet article 34 al.3a semble s'être déclaré en faveur du chiffrement. Cette position, si elle était publique et formalisée explicitement ne provoquerait-elle pas un froid diplomatique entre l'Europe et les Etats-Unis ?

Comment pouvons-nous encore cautionner cette hypocrisie ? L'ensemble des dirigeants qui ont été espionnés sont-ils toujours sous le choc, prostrés par les révélations de l'été 2013 ? Cette inertie est-elle uniquement réservée aux citoyens ? Nous sommes en droit de nous

demander si l'Union Européenne, elle-même espionnée, ne nous aurait pas discrètement envoyé un message.

Si notre lecture s'avérait juste, où pourrions-nous placer le niveau de la souveraineté européenne ? Ce silence actuel sur le droit au chiffrement, cet élément clé dans la protection de données personnelles, donc dans la garantie de nos droits fondamentaux, serait-il un aveu de faiblesse ?

Cet alinéa serait-il une tentative discrète de résistance ou pire de désobéissance ? Cette lecture justifierait l'ensemble de toutes ces positions très consensuelles que nous pouvons observer au fil du temps concernant la surveillance de masse mise en place par les Etats-Unis.

L'Union Européenne nous chuchoterait-elle à l'oreille que le chiffrement est notre dernière chance de reprendre le contrôle de nos données à caractère personnel, introduisant cet alinéa à destination de l'ensemble des entreprises qui finalement pourraient être les seules assez nombreuses et assez puissantes pour généraliser la résistance ?

Les révélations d'Edward Snowden n'étaient-elles pas un appel au réveil de la vie privée ?
L'alinéa 3a de l'article 34 ne serait-il pas quant à lui un appel au retour du chiffrement ?

Face à toutes nos interrogations, nous avons pris contact le 30 mai 2016 avec Jan Philipp Albrecht¹⁸, le Vice-Président de la Commission des libertés civiles de la justice et des affaires intérieures et rapporteur du Parlement européen sur la réglementation de la protection des données, afin d'obtenir sa vision sur notre lecture de l'article 34.

Nous lui avons donc demandé dans quelle mesure la communication aux personnes concernées par une violation de données à caractère personnel ne serait pas qu'un premier degré de lecture de l'article 34 introduisant implicitement la position de l'Union Européenne encourageant le droit au chiffrement ?

¹⁸ Jan Philipp Albrecht : http://www.europarl.europa.eu/meps/fr/96736/JAN+PHILIPP_ALBRECHT_home.html

Voici ce qu'il nous a répondu : « Effectivement, l'alinéa 3a de l'article 34 encourage l'utilisation de techniques de chiffrement appropriées. »

Il nous précise que cela n'est toutefois pas nouveau, « en effet la directive 2002/58 sur la vie privée et les communications électroniques contenait déjà une approche de ce type à l'alinéa 3 de l'article 4 depuis sa dernière modification en 2009¹⁹.

Le contenu de l'article 34 du Règlement Général sur la Protection des Données est basé sur ce texte.

Dans le Règlement Général sur la Protection des Données, Il a été ajouté "telles que le chiffrement" pour le rendre encore plus claire sur ce que l'on entend par cela. »

3.2. Les nouvelles obligations à prendre en compte

Le règlement fait du Data Protection Officer une pierre angulaire de la protection des données personnelles dans l'entreprise. En plus de ce qui a été précisé précédemment concernant l'article 34, de nouvelles obligations incomberont aux responsables de traitements.

Le DPO devra accompagner l'entreprise qui l'a désigné à appréhender de nouveaux principes dont les principaux sont présentés ci-dessous :

La protection des données dès la conception (Privacy by Design) recommande d'intégrer à toute technologie exploitant des données à caractère personnel des dispositifs techniques de protection de la vie privée dès sa conception et des mesures organisationnelles permettant d'anticiper en amont des projets informatiques, la problématique de protection des données personnelles.

Le principe d'« accountability » impose aux entreprises d'être en mesure de justifier l'ensemble des dispositifs de contrôle et d'encadrement mis en place pour assurer la conformité Informatique et Libertés au sein de l'organisme.

¹⁹ Directive 2002/58 sur la vie privée et les communications électroniques modifiée en 2009
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:FR:HTML>

Les entreprises seront dans l'obligation de notifier toute violation de données à caractère personnel aux autorités de contrôle. Les « Privacy Impact Assessments » traduits par la CNIL en « études d'impacts sur la vie privée », devront être réalisées sur l'ensemble des traitements considérés comme sensibles. L'étude d'impact sur la vie privée a vocation à évaluer les risques d'atteinte à la vie privée et leur impact sur les personnes concernées. Elle devra décrire toutes les mesures mises en œuvre par l'organisme pour y faire face. Elles représentent aussi pour le DPO un outil performant pour exprimer ses recommandations dès la conception d'un projet.

Dès 2015 la CNIL a publié plusieurs guides concernant les études d'impact : « *PIA, la méthode : Comment mener une étude d'impact sur la vie privée*²⁰ », « *PIA, l'outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée*²¹ » et « *PIA n°3 Bonnes Pratiques, mesures pour traiter les risques sur les libertés et la vie privée*²² » ces guides permettent d'obtenir une présentation générale de la méthodologie européenne afin de répondre aux attentes de la Commission européenne et de la CNIL.

Les prestataires et les éditeurs de logiciel ne seront pas épargnés, en effet le règlement introduit un principe de coresponsabilité, ils pourront donc être amenés à réaliser directement les études d'impacts nécessaires à la mise en place de leurs solutions et seront, par la même occasion, responsables de la sécurité des données de leurs clients.

Ce nouveau règlement devrait être considéré par chaque entreprise comme une opportunité d'optimiser sa sécurité juridique. Il ne doit pas se traduire comme une contrainte réglementaire de plus, mais comme un cadre permettant d'affronter la transformation numérique en respectant le droit à la vie privée des clients.

²⁰ Comment mener une étude d'impact sur la vie privée
<https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf>

²¹ PIA, l'outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée
<https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Outillage.pdf>

²² PIA n°3 Bonnes Pratiques, mesures pour traiter les risques sur les libertés et la vie privée
<https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-BonnesPratiques.pdf>

Présenté jusqu'à maintenant par beaucoup comme un avantage concurrentiel, la protection des données personnelles sera sans aucun doute un facteur de confiance dont les entreprises ne pourront plus se dispenser.

3.3. Le rôle du Data Protection Officer

Le « Data Protection Officer » tiendra un rôle majeur dans les années à venir, garant du respect de la vie privée, son implication est maintenant imposée.

Il a vocation à devenir un élément central dans les entreprises qui gèrent ou dont l'activité repose sur des données à caractère personnel.

Il devra être consulté en amont de l'ensemble des projets afin d'établir la place de protection des données personnelles au sein de ces derniers. En effet, il devra comme toujours assurer la licéité des traitements mis en place en termes de finalité, de proportionnalité du traitement, de pertinence des données au regard de la finalité, de durée de conservation, du nombre de destinataires, d'encadrement des relations avec les sous-traitants, d'information claire et préalable, d'exercice des droits des personnes et le cas échéant d'encadrement des transferts hors Union Européenne, effectuer les formalités adaptées et réaliser comme nous le disions précédemment une étude d'impact dans le cas où le traitement en question est considéré comme sensible.

Afin de respecter l'article 25 concernant la protection des données dès la conception, il devra également élaborer avec l'ensemble des services impliqués de l'organisme, l'intégration du concept de Privacy by Design. Le DPO devra donc avoir une réelle maîtrise des dispositifs techniques et des mesures organisationnelles.

Beaucoup de ces dispositifs techniques reposeront sur différents types de chiffrement, la maîtrise de ces dispositifs et l'adéquation de leur mise en place en fonction des cas d'usage seront fondamentaux pour répondre à l'article 24 « accountability » afin d'être en mesure de démontrer l'ensemble des éléments mis en œuvre. Ces compétences seront également nécessaires pour éviter la notification des violations de données aux personnes concernées.

CHAPITRE 2 - LE RETOUR DU CHIFFREMENT

Dans ce second chapitre nous présenterons de façon opérationnelle, les apports de techniques telles que le chiffrement, le hachage et la tokenisation pour éviter la notification des violations de données aux personnes concernées.

Nous étudierons l'ensemble de ces dispositifs et les différents cas d'usage dans lesquels ils pourront être mis en œuvre.

Comme nous l'expliquions précédemment, la maîtrise de ces dispositifs techniques permettra également d'être en mesure de répondre à plusieurs principes fondamentaux comme la confidentialité, l'intégrité ou la protection des données dès la conception.

Ce chapitre ne fera pas du lecteur, un développeur ou un cryptologue, toutefois il lui permettra d'avoir les bases nécessaires afin d'appréhender l'ensemble des points de contrôle pour encadrer convenablement la protection des données sensibles ou à caractère personnel.

1. LA CRYPTOLOGIE

Dans cette partie, nous verrons la place de la cryptographie dans le futur de la protection des données à caractère personnel ainsi que les différents cas d'usage dans lesquels il pourront être mis en place en fonction des différents types de chiffrement.

1.1. La cryptographie, un élément clé

Étymologiquement, on traduit le terme "cryptologie" comme la science du secret. Cette pratique fut utilisée au cours des différents siècles de l'histoire. Déjà en 2000 av. J.-C. les égyptiens cryptaient leurs hiéroglyphes, et par la suite Jules César lui-même communiquait

avec ses généraux grâce à un chiffrement par décalage connu aujourd'hui comme "le Chiffre de César"²³.

Ce besoin de limiter l'accessibilité d'une information stratégique à une personne ou encore à un groupe restreint d'individus n'est pas nouveau.

Aujourd'hui lorsque l'on parle de cryptologie, cela regroupe la cryptographie et la cryptanalyse.

La cryptographie, ou « chiffre de défense » permet de chiffrer une information, pour la protéger des regards, en la brouillant par le biais d'un algorithme et d'une clé, et permet, à qui est autorisé de la lire, de la déchiffrer en utilisant le même algorithme et une clé.

La cryptanalyse, ou « chiffre d'attaque » quant à elle, consiste sans être en possession de la clé de retrouver un message en clair en le décryptant avec d'autres méthodes.

La cryptographie se subdivise également en deux types bien distincts : la cryptographie symétrique et la cryptographie asymétrique.

La cryptologie ne concernait au début qu'une minorité d'individus, ou d'organisations gouvernementales, comme l'armée ou les services secrets.

C'est pour cette raison qu'il y a encore peu de temps la cryptologie était considérée comme une arme de guerre dans beaucoup de pays y compris aux Etats-Unis et en France.

Suite à l'avènement de l'internet, du web dit 2.0, des réseaux sociaux et des smartphones, la cryptographie a aujourd'hui une place fondamentale dans l'économie ainsi que dans notre vie quotidienne. Ces nouvelles technologies ont entraîné une augmentation non négligeable du volume des collectes et des échanges de données à caractère personnel. Ce phénomène a créé un besoin massif de sécurité, de confidentialité et d'intégrité des données des utilisateurs comme conséquence collatérale.

²³ Chiffrement par décalage : [http://fr.wikipedia.org/wiki/Chiffrement_par_décalage](http://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage)

La cryptographie a longtemps été interdite en France car elle était considérée jusqu'en 1996 comme une arme de guerre de deuxième catégorie. La législation française s'est par la suite assouplie autorisant la cryptographie symétrique avec des clés ne dépassant pas 128 bits (longueur de la clé sur laquelle repose le chiffrement). Suite à l'apparition des sites de commerce en ligne, la loi pour la confiance dans l'économie numérique du 21 juin 2004²⁴ a totalement libéré l'utilisation des moyens de cryptographie quelle que soit la longueur de la clé utilisée, en revanche, leur importation ou exportation restent soumises à déclaration ou autorisation.

La cryptographie a un rôle central dans les différents dispositifs techniques à mettre en place afin de protéger des données à caractère personnel.

Comme nous l'expliquions précédemment, il existe deux systèmes cryptographiques, le système de chiffrement symétrique et le système de chiffrement asymétrique dit aussi "chiffrement à clé publique".

Le système de chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer alors que le système de chiffrement asymétrique repose sur une paire de clés, une clé publique liée mathématiquement à une clé privée. Un message chiffré par une des deux clés ne pourra être déchiffré que par l'autre clé.

Nous verrons que nous utilisons déjà l'ensemble de ces différents systèmes de chiffrement au quotidien afin de répondre souvent à ce besoin d'anticiper toutes les dérives potentielles et les risques d'exploitations abusives de nos données personnelles.

Les données les plus sensibles comme les coordonnées bancaires d'un client ont l'obligation d'être stockées via un chiffrement symétrique dans les bases de données. En effet, la CNIL

²⁴ Loi pour la confiance dans l'économie numérique
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=i>
[d](#)

exige que les données bancaires soient chiffrées par l'intermédiaire d'un algorithme de chiffrement dit "fort"²⁵.

Il y a différentes méthodes de chiffrement symétrique, les trois principales sont le DES, le triple DES et l'AES. Suite aux révélations de l'été 2013, nous recommandons donc de mettre en place un chiffrement symétrique avec la méthode AES avec une clé de 256 bits à minima.

Le système de chiffrement asymétrique quant à lui est un dispositif technique qui est utilisé pour transmettre une clé de chiffrement symétrique, d'une manière sûre. Il a un rôle primordial dans la sécurité liée aux navigations sur le web : on le rencontre principalement où il y a chiffrement symétrique, pour protéger la clé de chiffrement symétrique notamment dans le protocole https.

Naviguer sur le web via un protocole http non sécurisé revient à se promener nu sur la voie publique : dans le monde numérique, une quantité non négligeable d'individus ont la faculté d'espionner n'importe qui en temps réel.

Le chiffrement asymétrique peut être également utilisé de manière plus basique dans le monde de l'entreprise pour permettre d'envoyer à un contact une clé symétrique qui servira ensuite à déchiffrer un message chiffré en s'assurant qu'il ne pourra être déchiffré que par une seule personne. Cette pratique ne pourra être mise en place sans mesure organisationnelle. Il convient donc d'inviter les contacts potentiels à utiliser la clé publique de l'organisme pour s'assurer que seul l'organisme puisse déchiffrer la clé pour ensuite ouvrir un message envoyé.

Ce principe de clé privée et clé publique permet d'assurer la non-répudiation. La non-répudiation est une exigence en cas de transactions financières en ligne. Il permet d'identifier de manière irréfutable l'émetteur débiteur d'un paiement.

²⁵ Fiche pratique : Un site marchand peut-il conserver mes données bancaires ? Publié par la CNIL le 21 juin 2011 <http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/un-site-marchand-peut-il-conserver-mes-donnees-bancaires/>

Dans la cryptographie il existe également le hashage. Ce n'est pas un système, il s'agit de fonctions de calcul d'empreinte, le hashage converti une chaîne de caractères de longueur quelconque en une chaîne de caractères de longueur fixe, qui caractérise la chaîne de longueur quelconque. Ces fonctions permettent un contrôle d'intégrité.

Le hashage permet par exemple de conserver l'empreinte générée par un mot de passe d'un utilisateur sans jamais en être en possession.

Ce principe est appliqué également dans le secteur de la biométrie grâce auquel il est possible de stocker l'empreinte générée par une donnée biométrique (empreintes digitales, iris, réseaux veineux etc..) sans jamais la conserver en clair.

Le hashage peut également se retrouver dans les "computer forensics", en cas de saisie informatique dans le cadre d'une enquête policière, les officiers de police judiciaire ont l'obligation de générer une empreinte de l'ensemble des fichiers saisis pour assurer qu'aucune altération ou modification ait lieu entre le moment de la saisie et le jugement²⁶.

1.2. Le contrôle d'intégrité

Le contrôle d'intégrité est une méthode utilisée pour calculer l'empreinte d'un mot de passe. Cette méthode donne la possibilité au système de stocker l'empreinte du mot de passe sans jamais en avoir connaissance, nous pourrions donc comparer l'empreinte calculée avec l'empreinte stockée pour vérifier qu'elles sont bien identiques.

Nous recommandons vivement de mettre en place un contrôle d'intégrité en utilisant la fonction SHA512.

Les fonctions de hash sont des fonctions irréversibles, aucun algorithme ne permet de retrouver la chaîne d'origine. La seule solution pour retrouver la chaîne d'origine est d'utiliser le déchiffrement par comparaison.

²⁶ Informatique légale : http://fr.wikipedia.org/wiki/Informatique_légale

Ainsi, chaque chaîne dont on calcul l'empreinte est comparée à l'empreinte recherchée jusqu'à trouver la correspondance.

Il existe principalement trois méthodes de déchiffrement par comparaison :

- Le brut force, qui consiste à générer toutes les combinaisons possibles d'une chaîne pour une longueur donnée.
- L'attaque par dictionnaire, qui consiste à utiliser les mots d'un dictionnaire stockés sur un fichier texte.
- Le rainbow table ou table arc-en-ciel qui est en cryptanalyse une structure de données qui a pour vocation de retrouver un mot de passe à partir de son empreinte. L'intérêt de stocker un dictionnaire en base de données est d'augmenter les performances du temps de réponse des requêtes lors d'une attaque. La constitution d'un tel dictionnaire prend du temps et doit être faite à l'avance. Toutefois elle est envisageable.

Il existe également des phénomènes de collisions. On peut parfois constater qu'un couple de données dans son ensemble de départ est tel que leur empreinte est identique. C'est le calcul dit en seconde pré image

Afin de répondre à ces différentes problématiques, on utilise la technique du grain de sel qui consiste à introduire un grain de sel qui va déformer le hash attendu. Ce grain de sel est en fait un très grand nombre que l'on concatène au mot de passe avant de calculer l'empreinte.

Cette technique est une déclinaison de la méthode "Shamir"²⁷, une méthode incontournable dans la gestion du secret²⁸.

Il convient donc d'ajouter une valeur au mot de passe avant de le hasher pour s'assurer que le même mot de passe ne donne pas le même hash et limiter les potentielles possibilités de collisions tout en augmentant la protection face à d'éventuelles attaques.

²⁷ Cette méthode repose sur l'atomisation d'une clé secrète en plusieurs éléments imposant la présence de plusieurs personnes pour déchiffrer. On peut retrouver l'utilisation de cette méthode dans les dispositifs de vote électronique ou encore dans le secteur bancaire pour accéder à des coffres-forts. En effet, un client ne peut accéder à son coffre sans la présence de la clé détenue par la banque.

²⁸ Secret réparti : http://fr.wikipedia.org/wiki/Secret_réparti

Ainsi au lieu d'enregistrer le hash du mot de passe seul, on peut enregistrer le hash du mot de passe suivi de l'adresse e-mail de la personne ou encore de son login. L'objectif est juste d'augmenter la complexité du hashage.

Prenons un exemple concret :

Le mot de passe de l'utilisateur "alex" est le suivant : "adequacy"
le hash est égal à : sha512("adequacy")

Le hash contient alors
183c92bb0e1bc9f7434a9a205bc9334b3a1eb8665f7392acd362354aa6ade639717b03ae29a4dbaac91666694c0b5bebfeedf40af2a0c65243425f47ba4df236 qui est le hash du terme : adequacy.

Si l'on avait un dictionnaire avec tous les hashes possibles, on pourrait alors associer

183c92bb0e1bc9f7434a9a205bc9334b3a1eb8665f7392acd362354aa6ade639717b03ae29a4dbaac91666694c0b5bebfeedf40af2a0c65243425f47ba4df236 à adequacy et donc obtenir le mot de passe.

Nous recommandons donc de rassembler le login et le mot de passe pour effectuer le contrôle d'intégrité : le hash sera alors égal à : sha512("alexadequacy") qui sera plus difficilement retrouvé dans un dictionnaire et générera également deux chaînes de caractères différentes pour deux utilisateurs utilisant le même mot de passe.

Il faut cependant souligner que ce paragraphe a pour but d'expliquer la technique du grain de sel et rappeler que l'état de l'art consiste à choisir un mot de passe ne correspondant à rien de connu.

1.3. Le chiffrement symétrique

Le chiffrement symétrique est un système reposant sur une même clé qui permet de chiffrer et de déchiffrer une donnée. Cette clé est le plus souvent appelée "secrète" car toute la sécurité de l'ensemble est directement liée au fait que cette clé n'est connue que par l'expéditeur et le destinataire.

Concernant les données et les fichiers à chiffrer, il convient de privilégier l'utilisation d'un système de chiffrement symétrique de type AES 256 à minima, afin d'optimiser la sécurité et les performances. 256 correspondant à 256 bits c'est-à-dire la longueur de clé utilisée.

Exemple : Si Alex souhaite envoyer un message chiffré à Alice, ils devront tous les deux être en possession de la clé secrète. Alex pour chiffrer le message et Alice pour le déchiffrer.

Pour rappel le chiffrement symétrique est bien plus rapide à exécuter que le chiffrement asymétrique. C'est pour cette raison qu'il est privilégié pour le chiffrement des données.

Dans le cadre de la mise en place d'un chiffrement symétrique AES 256, il convient également de choisir un mode opératoire nous assurant d'aboutir à un chiffrement probabiliste.

Un chiffrement probabiliste assure qu'un même message chiffré avec une même clé plusieurs fois donne un message chiffré différent à chaque fois. Le mode opératoire CBC (Cipher Bloc Chaining) assure un chiffrement probabiliste. C'est d'ailleurs le mode le plus courant.

Actuellement le système de chiffrement utilisé par Apple pour chiffrer les données contenues dans les iPhones est l'AES256. La clé est générée avec un hash du mot de passe secret concaténé avec l'identifiant du téléphone de l'utilisateur pour qu'Apple ne soit pas en mesure de le déchiffrer.

AES ou Advanced Encryption Standard aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il est actuellement l'un des algorithmes le plus utilisé et le plus sécurisé.

1.4. Le chiffrement asymétrique

Le chiffrement asymétrique quant à lui repose sur deux clés, une clé privée et une clé publique.

Voici trois exemples pour bien comprendre son utilité :

Chaque personne dispose d'un couple de clés, une privée que seule cette personne connaît et une clé publique qu'elle communique aux personnes qui souhaitent lui envoyer des messages.

Exemple n°1 : Un employé souhaite envoyer un message chiffré à son dirigeant.

L'employé chiffrera son message avec la clé publique du dirigeant pour s'assurer qu'il soit le seul à être en mesure de le déchiffrer avec sa clé privée. Ce cas d'usage assure donc à l'employé que son message ne sera lu que par son dirigeant.

Exemple n°2 : Le dirigeant souhaite répondre à son employé en assurant à son employé que la réponse provient bien de lui afin d'assurer la non-répudiation du message.

Le dirigeant utilise sa clé privée pour chiffrer le message et l'employé pourra déchiffrer le message à l'aide de la clé publique du dirigeant.

Exemple n° 3 : Le dirigeant souhaite répondre à son employé en s'assurant que seul son employé sera en mesure de déchiffrer le message envoyé.

Le dirigeant utilisera alors la clé publique de l'employé pour chiffrer son message pour que l'employé soit le seul à pouvoir le déchiffrer avec sa clé privée personnelle.

Ce que nous venons de vous présenter est exactement ce qui est mis en place lorsque que deux serveurs échangent entre eux de manière sécurisée. En effet chaque serveur est muni de deux clés, une privée et une publique.

Lors d'un échange chiffré entre deux serveurs, le serveur A utilise la clé publique du serveur B pour envoyer son message et le serveur B utilise sa clé privée pour déchiffrer le message.

De la même manière, le serveur B utilisera la clé publique du serveur A pour répondre et le serveur A utilisera sa clé privée pour prendre connaissance de la réponse.

Toutefois si le serveur A souhaite assurer la non-répudiation d'une information qu'il envoie, il effectuera la démarche inverse. Il chiffrera le message avec sa clé privée pour assurer au serveur B que le message a été chiffré par le serveur A.

Encore une fois ces différents exemples ont pour objectif d'expliquer la théorie du chiffrement asymétrique, mais en pratique, il est utilisé pour chiffrer une clé symétrique qui chiffrera le message.

Le protocole asymétrique recommandé actuellement est le RSA 2048. Afin de naviguer sur internet de façon sécurisée on utilise le protocole https. Ce protocole utilise comme nous l'évoquions précédemment un protocole de transfert de fichiers avec une couche de chiffrement TLS qui repose sur un chiffrement asymétrique de type RSA 2048 entre le client et le serveur.

Nous recommandons lorsque c'est possible d'utiliser des librairies de type PHPSeclib PURE PHP²⁹ pour générer vous-même vos clés en évitant d'avoir recours à un tiers de confiance dont nous nous méfions.

Nous ne sommes jamais mieux sécurisés que par nous-même par le biais d'un chiffrement open source sans lien avec un système d'information sur lequel nous n'avons pas de contrôle.

1.5. La tokenisation

Cette technologie a pour objectif de remplacer des données sensibles par des tokens ou des jetons qui sont alors des données sans signification ou valeur intrinsèque en dehors du système d'information dans lequel elles ont été produites.

²⁹pure PHP implementations of SSH, SFTP, RSA and X.509
<http://phpseclib.sourceforge.net/>

L'utilisation de cette technologie limite les risques de compromission des données critiques au travers des applications, des processus, ou des intervenants sur le système.

C'est alors les tokens qui sont utilisés remplaçant les informations originales. En cas de divulgation, les données subtilisées ne peuvent pas être réutilisées et perdent ainsi toute valeur.

Pour comprendre le principe, voici un exemple concret :

Imaginons qu'Alex souhaite payer un achat en ligne, lorsqu'il validera son paiement il enverra au vendeur un token correspondant à ses coordonnées bancaires qu'un tiers de confiance, lui aura généré. Le vendeur demandera par la suite au tiers de confiance de valider le paiement. Dans ce type de transaction, le tiers de confiance est inévitable.

Ce processus permet à l'acheteur de ne pas donner ses coordonnées bancaires à tous les vendeurs avec qui il souhaite faire une transaction. Seul le tiers de confiance a en sa possession les coordonnées bancaires d'Alex afin de valider les paiements.

1.6. L'obfuscation du code

Pour augmenter la sécurité des développements informatiques mis en ligne, il peut également être opportun d'obfusquer certains fichiers dans le serveur comme les fonctions de chiffrements ou le fichier de configuration dans lequel on retrouve les informations permettant de se connecter à la base de données.

Certains développeurs utilisent cette technique pour protéger le code source qu'il considère comme leur propriété intellectuelle. Pour un développement en langage PHP nous recommandons des solutions telles que "IONCUBE³⁰" pour l'encodage des fichiers.

L'obfuscation permet d'éviter l'analyse des algorithmes en cas de vol des codes sources du système.

³⁰ ioncube est un encodeur de fichiers PHP.

L'obfuscation de certaines librairies contenant des fonctions stratégiques d'un logiciel ou d'une plateforme permettra à l'architecte du système d'information d'être le seul détenteur de la librairie originale encore en clair et d'offrir la possibilité aux développeurs d'utiliser ces fonctions sans en connaître les mécanismes. Cette pratique permet d'effectuer des développements informatiques atomisés reprenant les principes de la méthode « Shamir » sur le partage du secret.

Le principe d'atomisation consiste à faire développer à différents développeurs une partie du code sans qu'aucun n'ait de vision globale sur le projet réalisé.

2. MISE EN ŒUVRE DES DISPOSITIFS TECHNIQUES

Dans cette seconde partie, nous présenterons les mises en œuvre possibles des dispositifs techniques de chiffrement sur différent cas d'usage comme l'activation d'un compte utilisateur, la modification d'un mot de passe oublié, le chiffrement d'un document en assurant sa réversibilité et l'authentification forte.

2.1. Activer un compte utilisateur ou modifier un mot de passe oublié.

Afin d'activer un compte utilisateur ou donner à un utilisateur la possibilité de modifier son mot de passe en toute sécurité, la pratique recommandée consiste à envoyer un mail à l'adresse correspondante au compte.

Ce courriel contient généralement un lien avec le hash d'une variable aléatoire permettant de s'assurer que cette procédure est initiée par la personne qui a reçu le lien.

Cette variable aléatoire est un token généré et stocké à la volée dans la base de données pour être comparé au moment où l'utilisateur effectue la procédure d'activation de compte ou de modification de mot de passe. Voici un exemple de résultat du hash d'une variable aléatoire qui peut-être considéré comme un token : 5728683c2f844c4b51e90e5b8a49d0dd.

Cette comparaison utilise le principe le contrôle d'intégrité : le token utilisé dans le lien est-il identique à celui généré dans le compte de l'utilisateur précédemment ?

Voici un exemple pour générer un token en fonction de l'heure. Cette variable aléatoire sera différente en fonction de l'heure à laquelle elle est générée.

```
$token = md5(microtime(TRUE)*100000);
```

2.2. Chiffrement symétrique ou asymétrique lequel choisir ?

Comme nous l'expliquions précédemment dans le cadre de la mise en place d'un système de chiffrement pour un système d'information, on cumule les deux types de chiffrement.

Le chiffrement asymétrique est généralement utilisé pour l'échange sécurisé de clé symétrique. On assure la non-répudiation des échanges de clés grâce au chiffrement asymétrique et on assure un niveau de performance grâce au chiffrement symétrique.

Il faut garder à l'esprit que le chiffrement asymétrique est plus robuste que le chiffrement symétrique mais plus gourmand en ressource donc moins performant au niveau du temps de calcul. C'est pour cela qu'il faut utiliser le chiffrement asymétrique pour chiffrer des clés symétriques qui sont des chaînes de caractères dont la longueur est limitée.

Les données sensibles ou les fichiers quant à eux devront être chiffrés par un système de chiffrement symétrique de type AES 256.

2.3. Assurer la réversibilité d'un document chiffré.

Lorsque l'on met en place un système de chiffrement pour chiffrer des fichiers, il faut assurer la réversibilité intégrale lors du déchiffrement.

Pour chiffrer un fichier PDF par exemple il faudra ajouter une étape préalable au chiffrement, en effet il convient de « sérialiser » le fichier en amont afin de le convertir en données brutes.

Ce sont ces données brutes qui devront être chiffrées, une fois déchiffrées ces données devront être « dé-sérialisées » pour reprendre la forme d'un fichier.

Ces fonctions sont parfois intégrées dans les fonctions de chiffrement, néanmoins il faut vérifier ce paramètre lors de la mise en place d'un système de chiffrement afin de s'assurer de la réversibilité intégrale et effective de l'ensemble des fichiers.

Nous mettons à votre disposition en téléchargement gratuit³¹, deux fonctions en PHP intégrant la procédure de sérialisation et dé-sérialisation, une fonction pour chiffrer en AES256 avec un mode opératoire probabiliste et la fonction de déchiffrement correspondante.

Pour rappel une clé de 64 caractères permet d'assurer un niveau de chiffrement AES sur 256 bits. Afin de générer une chaîne de caractère de 64 caractères la pratique la plus courante est de générer cette clé grâce au SHA256 d'un mot de passe par exemple.

NB : Nous recommandons le hash SHA512 pour faire du contrôle d'intégrité sur des mots de passe, toutefois pour transformer un mot de passe en clé de 64 caractères pour du chiffrement symétrique AES 256, il faudra utiliser le hash SHA256.

Exemple : `$key=hash('sha256', 'alex', false);`

Le résultat de ce hash donnera une chaîne de 64 caractères. :
4135aa9dc1b842a653dea846903ddb95bfb8c5a10c504a7fa16e10bc31d1fdf0

2.4. L'authentification forte

Pour l'identification d'un utilisateur, comme nous l'expliquions précédemment, il convient de comparer l'empreinte du mot de passe saisi avec l'empreinte du mot de passe conservée en base de données.

³¹ Fonctions de chiffrement et de déchiffrement AES 256 en PHP
https://www.fiorentino-consulting.com/Fonctions_de_chiffrement_et_de_dechiffrement_AES_256_en_PHP.txt

Afin d'optimiser la sécurité des plateformes web permettant à l'utilisateur d'accéder à son profil ou à son compte personnel, un grand nombre d'entreprises souhaite mettre en œuvre une authentification forte pour certaines fonctions mises à disposition de leurs utilisateurs.

L'objectif est de s'assurer que les actions ou les modifications effectuées via la plateforme web sur des données considérées comme sensibles ne pourront être effectuées qu'une fois que l'utilisateur se sera authentifié avec un niveau de sécurité supérieur à celui lui permettant d'accéder à son compte.

Il y a différentes mises en œuvre possibles, chacune de ses mises œuvres a des avantages et des inconvénients.

La notion d'authentification s'oppose à celle de l'identification d'une personne physique ou morale. Une certaine ambivalence s'est installée par abus de langage. En effet on parle souvent d'authentification lorsqu'il s'agit d'identification. La présentation d'une pièce d'identité lors d'un contrôle, identifie par le biais d'un document officiel, toutefois cette présentation ne permet pas une authentification formelle, en effet le lien entre la pièce d'identité et la personne n'est alors pas établie de façon indiscutable, irrévocable et reconnue par les tribunaux comme non répudiable en cas de litige.

En effet une authentification réelle doit-être apportée par un tiers de confiance et par une preuve au sens juridique reconnue devant les tribunaux. Par exemple : la signature électronique de la carte bancaire assure le principe de non-répudiation.

Juridiquement, la charge de la preuve émanant d'un tiers de confiance distingue l'identification de l'authentification en cas de litige ou de contestation.

Les systèmes d'authentification courants utilisent un seul facteur, en général un mot de passe.

L'authentification forte consiste à utiliser plusieurs facteurs de différentes natures afin de réduire les risques d'une éventuelle attaque. On présente généralement les différents facteurs d'authentification comme suit³² :

« Ce que l'entité connaît : un mot de passe, une phrase secrète, un code PIN.

Ce que l'entité détient : une carte magnétique, RFID, une clé USB, une carte à puce, un smartphone, etc... Soit un élément physique appelé jeton d'authentification, le token.

Ce que l'entité est : soit une personne physique par le biais d'une empreinte digitale, une empreinte rétinienne, la structure de la main, la structure osseuse du visage ou tout autre élément biométrique.

Ce que l'entité sait faire ou fait : soit une personne physique par le biais de biométrie comportementale tel que signature manuscrite, la reconnaissance de la voix, un type de calcul connu de lui seul ou un comportement.

Où l'entité se trouve : suite à une identification et authentification réussie, elle est autorisée à accéder à un système logique depuis un endroit défini. »

Pour une authentification forte, il faut combiner au moins deux des facteurs ci-dessus.

L'authentification forte est une des fondations essentielles pour garantir :

- L'autorisation ou le contrôle d'accès qui garantit qui peut y avoir accès.
- La confidentialité qui garantit qui peut le voir.
- L'intégrité qui garantit qui peut le modifier.
- La traçabilité qui garantit qui l'a fait.
- L'irrévocabilité qui garantit que la personne puisse le prouver.

³² Authentification forte

<http://www.techno-science.net/glossaire-definition/Authentification-forte.html>

Nous considérons qu'il existe trois familles technologiques pour l'authentification forte :

- Certificat numérique
- Biométrie multimodale (deux facteurs biométriques minimum)
- One Time Password (OTP) / Mot de passe à usage unique.

Certificat Numérique

Cette technologie est basée sur l'utilisation d'un système de chiffrement asymétrique et l'utilisation d'un « challenge » garantissant alors la non-répudiation de l'utilisateur du certificat utilisé.

Exemple :

- Infrastructure à clés publiques (PKI)
- Chiffrement asymétrique de type chiffrement RSA 2048 avec clé privée et clé publique.

Biométrie

Cette technologie repose sur la reconnaissance d'une caractéristique ou d'un comportement unique.

Exemple :

- Biométrie
- Technologie Match on Card

One Time Password (OTP) / Mot de passe à usage unique

Voici la définition de Wikipédia³³ : « *Un mot de passe à usage unique ou OTP (One-time password) est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaques par rejeu. Cela signifie que, si un intrus potentiel parvient à enregistrer un OTP qui était déjà utilisé pour se connecter à un service ou pour effectuer une opération, il ne sera pas en mesure de l'utiliser car il ne sera plus valide. En revanche, les OTP ne peuvent pas être mémorisés par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir.*

Cette technologie permet de s'authentifier avec un mot de passe à usage unique. Elle est fondée sur l'utilisation d'un secret partagé (cryptographie symétrique) ou l'utilisation d'une carte d'authentification. Il n'est donc pas possible de garantir une véritable non-répudiation. »

Intéressons-nous à la famille des One Time Password (OTP) qui est la technologie la plus répandue sur le web et dont le coût de mise en place est le plus faible. Il existe deux algorithmes possibles :

- HMAC-based one-time password (HOTP) : l'algorithme est basé sur un compteur.
- Time-based One-time Password (TOTP) : l'algorithme est basé sur le temps permettant de choisir la durée de validité du mot de passe.

L'intérêt d'utiliser l'algorithme basé sur le temps est de choisir une durée de validité inférieure à celle d'une attaque par dictionnaire en fonction de la longueur du mot de passe ciblé.

L'algorithme TOTP est également la technologie utilisée par GOOGLE pour l'application GOOGLE AUTHENTICATOR qui permet d'obtenir une authentification forte pour les

³³ Mot de passe à usage unique :
https://fr.wikipedia.org/wiki/Mot_de_passe_à_usage_unique

adresses Gmail. Ce qui sous-entend qu'il sera possible d'utiliser l'application GOOGLE AUTHENTICATOR si on le souhaite. La librairie PHP permettant la mise en place d'un TOTP compatible avec la technologie GOOGLE AUTHENTICATOR est disponible en téléchargement gratuit sur l'adresse url³⁴ en bas de page.

Pour encore plus de détail voici une page web³⁵ explicative à transmettre au développeur en charge la mise en place d'un tel dispositif.

La mise en place d'un algorithme TOTP peut se traduire de différentes manières.

Un utilisateur peut recevoir un mot de passe de 6 chiffres valable 30 secondes par SMS, par mail, ou en utilisant une application OTP type GOOGLE AUTHENTICATOR.

Si l'on privilégie l'expérience utilisateur, l'envoi d'un SMS ou d'un mail seront les solutions les plus adaptées.

Si l'on privilégie la sécurité on exclura l'envoi du mail au profit de l'envoi SMS utilisant un canal différent et limitant la réception du mot de passe à un seul périphérique (le téléphone).

Cette solution mettra donc l'utilisateur dans l'obligation de prouver :

- Ce qu'il connaît : le mot de passe de son compte.
- Et ce qu'il détient : le téléphone sur lequel il recevra le mot passe unique par SMS.

Pour pallier au vol du smartphone de l'utilisateur, il est possible d'ajouter une réponse à une question secrète liée à l'utilisateur, cela ajoutera un facteur « ce qu'il connaît » de plus qui n'a pas vocation à être reçu dans une boîte mail ou enregistré dans un navigateur.

L'ensemble de ce dispositif est une forme de tokenisation utilisée pour l'authentification.

³⁴ Librairie PHP Google two-factor authentication

https://www.fiorentino-consulting.com/Librairie_PHP_Google_two-factor_authentication.txt

³⁵ Page d'intégration d'un TOTP compatible Google Authenticator

<https://www.idontplaydarts.com/2011/07/google-totp-two-factor-authentication-for-php/>

3. UN PARADIGME A SOMME POSITIVE

Dans cette troisième partie nous verrons l'ensemble des facteurs permettant de s'assurer que le principe de chiffrement des données est bien un paradigme à somme positive.

Nous présenterons l'impact sur l'expérience utilisateur que peut entraîner le chiffrement, les avantages qu'il pourra apporter à une entreprise malgré l'existence d'une forme de dichotomie pour le business ainsi que l'impact que pourrait engendrer une utilisation généralisée du chiffrement sur l'économie numérique.

3.1. L'impact sur l'expérience utilisateur

L'impact de l'implémentation d'un système de chiffrement sur l'expérience utilisateur ne sera pas sans conséquence, en effet malgré les performances actuelles des serveurs informatiques, la mise en place d'un système de chiffrement ralentira l'ensemble des processus.

Il mettra également l'utilisateur dans l'obligation de répondre à des questions secrètes qui lui permettront de ne pas perdre l'ensemble des données chiffrées en cas d'oubli de son mot de passe.

Néanmoins, l'implémentation d'un système de chiffrement pour protéger les données sensibles comme des données à caractère personnel ou des données de santé augmentera incontestablement le facteur confiance de l'utilisateur face aux services numériques mis à disposition sur des plateformes web.

La révolution numérique a engendré un grand nombre de nouvelles pratiques, ces phénomènes ont provoqué et continueront de provoquer une augmentation non négligeable des volumes de données circulant sur la toile, le risque de violation de données à caractère personnel est proportionnel. En effet plus il y aura de données à caractère personnel sur le web plus le risque d'atteinte à la vie privée des utilisateurs sera important.

Avec le temps, la maîtrise et la sensibilisation des internautes sont de plus en plus importantes, dans l'avenir le chiffrement des données deviendra une exigence attendue par l'ensemble des utilisateurs.

Présenté jusqu'à maintenant par beaucoup comme un avantage concurrentiel, le chiffrement des données sera sans aucun doute un nouveau facteur dont les entreprises ne pourront plus se dispenser pour faire face à la concurrence, notamment celle des grands acteurs du web qui ont déjà pris ce virage dès septembre 2013.

3.2. Une dichotomie pour le business ?

Les bases de données représentent aujourd'hui des actifs stratégiques pour les organismes qu'ils soient publics ou privés. Elles jouent un rôle majeur dans la fonction commerciale. Un grand nombre d'informations liées aux clients y sont stockées. On peut aussi y retrouver les informations inhérentes aux différents produits ou services. Elles représentent une véritable valeur économique au sein du patrimoine des entreprises et sont une composante clé de leur compétitivité.

Le chiffrement des données provoquera sans aucun doute des impacts sur la fonction mercatique des entreprises, les données jusque-là utilisées pour créer des besoins et des services en fonction des informations captées sur la situation personnelle de l'utilisateur ne seront plus automatiquement disponibles.

Pour un dirigeant d'entreprise cette stratégie présente à première vue un manque à gagner, mais ce raisonnement n'est pas forcément fondé. En effet le recueil de consentement permettra toujours d'effectuer des campagnes publicitaires destinées aux utilisateurs qui se seront inscrits sur des listes de diffusion, les achats des clients permettront toujours d'envoyer des offres complémentaires pour effectuer du marketing croisé. Certes les champs de diffusion seront moins larges mais forcément plus ciblés.

Le chiffrement des données imposera aux développeurs d'application d'intégrer des nouveaux types de fonctionnalités de recherche au sein des systèmes d'information sur lesquels les données sont chiffrées comme des recherches phonétiques par exemple³⁶.

Nous mettons également à votre disposition une librairie PHP open source³⁷ développée par l'école Polytechnique adaptée aux recherches phonétiques en français.

Le principe d'utilisation proportionné des données exclusivement pertinentes sera dans un premier temps considéré par beaucoup comme une contrainte mais augmentera également la précision des analyses marketing des entreprises.

De plus, en cas de piratage ou de violation de données à caractère personnel, le chiffrement augmentera également le niveau de sécurité juridique de l'entreprise ainsi que le niveau de sécurité du patrimoine informationnel. Comme tout objet de valeur, ce patrimoine informationnel suscite des convoitises. Le chiffrement des données a donc vocation à favoriser l'étanchéité de l'économie numérique.

4. INNOVATIONS ET PROSPECTIVES

Dans cette dernière partie, nous présenterons le chiffrement homomorphe, les évolutions qu'il engendrera et les nouvelles opportunités qu'il permettra d'atteindre dans un futur proche. Nous finirons par vous présenter l'informatique ubiquitaire qui pour beaucoup de spécialistes pourrait bien représenter le dernier défi pour la protection de vie privée.

4.1. Le chiffrement homomorphe

C'est une particularité qui peut s'appliquer à certains systèmes de chiffrement asymétriques, et qui permet à un tiers qui possède la clé publique de faire des calculs, « addition » et ou « multiplication » sur des messages préalablement chiffrés.

³⁶ Soundex est un algorithme phonétique d'indexation de noms par leur prononciation

<https://fr.wikipedia.org/wiki/Soundex>

³⁷ Fonction de génération de chaînes pour les recherches phonétiques

https://www.fiorentino-consulting.com/Fonction_de_generation_de_chaines_pour_les_recherches_phonétiques.txt

Le résultat du calcul de nouveaux messages est le résultat chiffré des opérations.

Prenons un exemple : avec un système de chiffrement homomorphe une application mobile peut savoir qu'Alice et Alex sont au même endroit en analysant leurs coordonnées de géolocalisation sans être en mesure de savoir où ils se trouvent.

Le problème avec les systèmes de chiffrement asymétriques homomorphes, c'est qu'ils ne sont que partiellement homomorphes. En effet, ils ne supportent qu'une seule opération : addition ou multiplication.

Et nous savons qu'en informatique, il est indispensable de pouvoir faire les deux afin d'être en mesure de faire tout type de calcul.

Le chiffrement homomorphe resta partiel jusqu'en 2009, date à laquelle Craig Gentry³⁸, de l'université de Stanford, publia sa thèse dans laquelle se trouve la toute première représentation théorique d'un système de chiffrement complètement homomorphe, fondée sur la cryptographie à base de réseaux euclidiens.

Sa théorie exclue l'ensemble des problèmes liés à la factorisation des nombres avec le chiffrement RSA ou au logarithme discret avec protocole cryptographique ElGamal³⁹. L'intérêt dans l'utilisation de la cryptographie à base de réseaux euclidiens est sa résistance face aux ordinateurs quantiques qui sont aujourd'hui encore à un niveau expérimental.

Toutefois le chiffrement homomorphe est actuellement limité. En effet il impose l'utilisation de clés de plusieurs méga-octets, alors qu'une clé RSA ne pèse qu'entre 128 et 512 octets, et les calculs, « addition » et « multiplication » peuvent être jusqu'à 1000 fois plus lents que les opérations non-homomorphes. Les travaux se poursuivent pour pousser ce système dans ses retranchements et réduire la taille des clés.

Pour beaucoup de développeurs d'application avides d'informations mais soucieux de l'image de leur entreprise, le chiffrement homomorphe est l'avenir du chiffrement car il permettra de traiter des données en respectant la vie privée des utilisateurs.

³⁸ Craig Gentry : [https://en.wikipedia.org/wiki/Craig_Gentry_\(computer_scientist\)](https://en.wikipedia.org/wiki/Craig_Gentry_(computer_scientist))

³⁹ El Gamal : https://fr.wikipedia.org/wiki/Cryptosyst%C3%A8me_de_ElGamal

Les données sensibles stockées dans un cloud public, chiffrées, pourront également faire, dans ce cloud, l'objet de calculs qui donneront des résultats chiffrés. Leur rapatriement chez l'utilisateur, puis déchiffrement donnera le même résultat que si les calculs avaient été opérés, chez l'utilisateur, sur les données en clair.

Néanmoins nous considérons que ce n'est pas une fin en soi et que cela ne règlera pas toutes les problématiques liées à la protection des données à caractère personnel.

Certes c'est une avancée mais finalement même si nous ne savons pas où Alice et Alex se trouvent, le fait de savoir qu'ils sont ensemble n'est-il pas une donnée à caractère personnel ?

4.2. L'informatique ubiquitaire, le dernier défi

Le terme d'informatique ubiquitaire fut prononcé la première fois en 1988 par Mark Weiser du Xerox PARC pour désigner sa vision du futur de l'informatique du XXI^e siècle.

Troisième ère de l'histoire de l'informatique, succédant à celles des ordinateurs personnels et celle des mainframes, l'informatique ubiquitaire repose sur une forme de réseau omniprésent. Souvenez-vous lors de l'ère des mainframes, un grand ordinateur était utilisé collectivement par plusieurs personnes. Par la suite celle des ordinateurs personnels, un ordinateur était utilisé exclusivement par une seule personne.

Dans l'ère de l'informatique ubiquitaire, l'utilisateur a à sa disposition une multitude de petits appareils comme le smartphone, les objets connectés et bientôt les nanotechnologies. Pour certains de ces appareils, leur utilisation fait déjà partie de nos vies quotidiennes.

Mark Weiser considérait que dans l'avenir l'informatique serait omniprésente dans la vie quotidienne des utilisateurs. Il décrivait cette période comme une ère de convergence qui amènerait différents périphériques à communiquer ensemble sur différents réseaux sans l'intervention de leur propriétaire. Collectant et échangeant des données liées à ce dernier dans l'optique de limiter le plus possible les interactions avec l'utilisateur, les périphériques analyseront nos besoins en fonction du contexte, nos contacts, nos habitudes, bref notre vie privée.

Selon lui « *les technologies les plus profondes sont celles qui sont devenues invisibles. Celles qui, nouées ensemble, forment le tissu de notre vie quotidienne au point d'en devenir indissociables*⁴⁰ ».

⁴⁰ Informatique ubiquitaire

https://fr.wikipedia.org/wiki/Informatique_ubiquitaire

CONCLUSION

Nous considérons que l'informatique ubiquitaire est le dernier défi auquel devra faire face la protection de la vie privée, et ce défi ou ce combat sera compliqué à mener. En effet, sans la généralisation du chiffrement, la protection des données à caractère personnel pourrait devenir de plus en plus complexe.

L'intelligence artificielle progresse, on parle aujourd'hui d'intelligence artificielle contextuelle, une intelligence qui interagit en fonction du contexte, un contexte qu'il faut donc analyser en amont.

Le « machine learning » ou apprentissage automatique devient de plus en plus performant, de grandes perspectives s'ouvriront notamment avec le « deep learning », l'apprentissage profond.

Les projets Big data évolueront également avec le temps en augmentant la précision de leurs résultats, multipliant avec eux des phénomènes de sérendipité concomitants.

La synergie de l'ensemble de ces phénomènes pourrait nous plonger dans un film de science-fiction, mais la science-fiction devient parfois bien réelle. George Orwell a publié son célèbre roman 1984 en 1949 et nous ne sommes aujourd'hui pas si loin de la société qu'il avait imaginée.

Nous, informaticiens, acteurs du numérique, Correspondant Informatique et Libertés ou futur DPO choisissons tous les jours comment le code va se comporter. Nous l'écrivons, nous l'encadrons. Nous sommes responsables du futur visage du monde numérique, nous devons prendre position pour concevoir un univers numérique respectueux des droits et des libertés. Nous devons coder pour protéger notre avenir. Le troisième chapitre de ce mémoire, c'est à vous de l'écrire, il pourrait s'appeler : « LA REVANCHE DES CILS »

Alessandro FIORENTINO

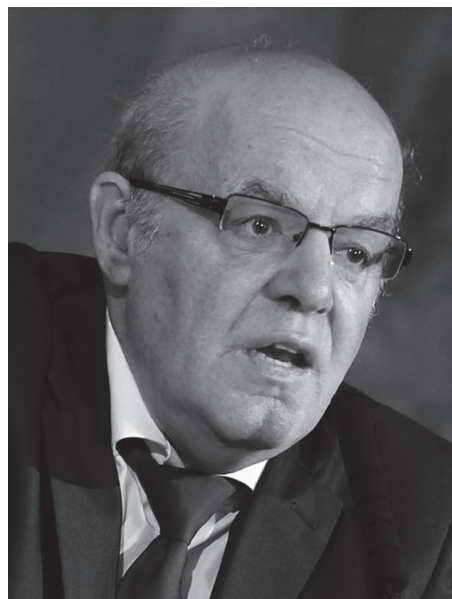


Photographie par Frédéric CAUNANT

Alessandro FIORENTINO est consultant, en charge de l'offre Informatique et Libertés au sein de la pratique SI du cabinet Infhotep. Titulaire d'un Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP), il a soutenu une thèse professionnelle relative à la mise en œuvre du Privacy by Design. Ambassadeur du Privacy by Design depuis mai 2013, il accompagne les entreprises dans le développement de projets intégrant les principes de protection de la vie privée dès la conception.

Il est également Co-fondateur de la PRIVACY TECH, une association qui vise à recenser, à promouvoir et à co-développer des solutions juridico-techniques au service de la protection de la vie privée sur Internet.

Gérard PELIKS



Photographie prise au cours d'un colloque de l'Alliance du Commerce

Gérard PELIKS travaille depuis plus de 20 ans dans le domaine de la sécurité de l'Information. Président de l'association CyberEdu (créée par l'ANSSI), président de l'atelier sécurité et VP de Forum ATENA, Ingénieur diplômé, il a travaillé pour Airbus Defence & Space Cybersecurity.

Lieutenant-colonel de gendarmerie dans la Réserve Citoyenne de Cyberdéfense (DGGN) et membre du Conseil d'Administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI), il co-organise, sur une base mensuelle, les Lundi de l'IE du Cercle d'Intelligence économique du Medef Ile-de-France.

Chargé de cours sur la cybercriminalité/cybersécurité dans des mastères d'écoles d'ingénieurs, en particulier à l'Institut Mines Télécom et à l'Institut Léonard de Vinci, son activité principale aujourd'hui est de porter l'esprit de cybersécurité / Cyberdéfense auprès du citoyen en organisant des présentations pédagogiques de tous niveaux et en écrivant des articles de vulgarisation sur les dangers du cyberspace et des contre-mesures pour en diminuer les risques.

CONTACT

email: alessandro@privacytech.fr
www.privacytech.fr



PRIVACY TECH
GARANTIR LE FUTUR VISAGE DU MONDE NUMERIQUE

ALESSANDRO FIORENTINO
LE REVEIL DE LA VIE PRIVEE