Sécurité et hygiène numérique des professionnels

François Pellegrini

Sécurité et hygiène numérique des professionnels

François Pellegrini

Université de Bordeaux, LaBRI & Inria Bordeaux - Sud-Ouest, 351 cours de la Libération, 33405 Talence cedex, France. francois.pellegrini@labri.fr

I.– Une obligation ancienne : la sécurité des données

Sur le plan de la sécurité, le Règlement général sur la protection des données (RGPD), entré en vigueur le 25 mai dernier, ne constitue pas une révolution. En effet, dès sa version initiale du 6 janvier 1978, la loi « Informatique et Libertés » (LIL) disposait que : « Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage [...] à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés ». Au fil du temps, ces dispositions n'ont été amendées qu'à la marge [1].

La démarche de contrôle de la conformité mise en œuvre par la Commission nationale de l'informatique et des libertés (CNIL) possède deux versants : un versant juridique, portant sur la vérification du respect des dispositions applicables (information des personnes, « opt-in », encadrement des activités des sous-traitants, etc.), et un versant technique, portant sur la vérification de la mise en œuvre effective de ces procédures et du traitement. De par la portée des dispositions précitées, cette vérification ne se restreint pas au traitement proprement dit, mais également à son environnement, et notamment à la sécurité bâtimentaire et des sécurité des systèmes d'information servant de supports aux traitements.

La vérification de la conformité s'effectue donc dans le cadre d'une analyse de proportionnalité, mesurant l'écart entre les pratiques du responsable de traitement et les différents niveaux de sécurité offerts par l'état de l'art, et considérant les moyens nécessaires à l'atteinte du niveau de sécurité adéquat vis-à-vis des caractéristiques du traitement (dont notamment le volume et la sensibilité des données).

Cet état de l'art est déterminé à l'aune des connaissances et bonnes pratiques des communautés de la sécurité informatique et du secteur considéré. Ces connaissances incluent celle des risques et des menaces déjà identifiés, correspondant à des comportements à proscrire. C'est par exemple le cas du « top 10 » des risques informatiques et défauts de conception des applications web [2], publié par l'OWASP (« *Open Web Application Security Project* »), une association professionnelle internationale destinée à l'amélioration de la sécurité des logiciels. Les bonnes pratiques incluent la mise en œuvre de méthodologies d'analyse, telles que la méthode EBIOS [3] (« Expression des Besoins et Identification des Objectifs de Sécurité ») d'audit de sécurité informatique. Le « G29 », groupe de travail des autorités de protection des données de l'Union européenne institué en vertu de l'article 29 de la directive 95/46/CE, prédécesseur du Contrôleur européen de la protection des données (CEPD), s'en est très fortement inspiré pour définir ses lignes directrices relatives à la méthodologie de réalisation des AIDP (« Analyse d'impact sur les données personnelles ») [4]. Ceci constitue un état de l'art « communautaire », auquel peuvent être adjoints les états de l'art plus officiels, telles que les recommandations de bonnes pratiques et référentiels d'exigences de sécurité de l'ANSSI (« Agence nationale de la sécurité des systèmes d'information ») [5]. La CNIL a pour sa part édicté ses propres référentiels, tels celui relatif à la robustesse des mots de passe [6].

Pour construire cet état de l'art, la CNIL dispose également d'outils normatifs plus rigides. Ainsi l'article 34 de la LIL, dans sa version antérieure au RGPD, disposait-il que des décrets, pris après avis de la CNIL, pussent fixer les prescriptions techniques auxquelles devaient se conformer certaines catégories de traitements de données sensibles [7].

1. Les dispositions de l'article 29 de la loi de 1978 initiale étant par la suite reprises au sein de l'article 34 en les termes suivants : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

2. Voir : https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project .

3. Voir pour référence : https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ .

4. Voir : G29, « Lignes directrices sur l'analyse d'impact relative à la protection des données » adoptées le 4 octobre 2017 : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf .

5. Voir : https://www.ssi.gouv.fr/administration/bonnes-pratiques/ .

6. Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, modifiée par la délibération n° 2017-190 du 22 juin 2017. Voir : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033928007 .

7. Il s'agissait de ceux mentionnés aux 2° et 6° du II de l'article 8, à savoir, d'une part, ceux nécessaires à la sauvegarde de la vie humaine sans le consentement de la personne et, d'autre part, les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un professionnel astreint au secret médical.

Cet outil n'a jamais été utilisé. Le nouvel article 11 de la LIL prévoit pour sa part la possibilité pour la CNIL d'édicter de son propre chef des règlements types contraignants relatifs à la sécurité de toutes catégories de traitements, ainsi qu'au traitement de certaines catégories de données sensibles : « En concertation avec les organismes publics et privés représentatifs des acteurs concernés, elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé. À ce titre, sauf pour les traitements mis en œuvre pour le compte de l'État agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures, notamment techniques et organisationnelles, supplémentaires pour le traitement des données biométriques, génétiques et de santé en application du 4 de l'article 9 du [RGPD] [...] ». Cette possibilité sera sûrement exploitée.

Ces exigences de sécurité constituent une obligation de moyens, éventuellement renforcée selon la sensibilité et le volume des données à caractère personnel concernées. Il ne s'agit cependant pas d'une obligation de résultat. En dépit de recherches toujours plus élaborées dans le domaine de l'analyse des logiciels et de la sécurité informatique, il est impossible de certifier le comportement d'un logiciel donné. L'activité de conception logicielle est fondamentalement de nature artisanale [8], et de ce fait soumise aux erreurs humaines. Il n'est donc pas attendu qu'un logiciel soit exempt de bogues. En revanche, la négligence des professionnels sera de plus en plus durement sanctionnée, à la mesure du rehaussement de l'état de l'art en matière de génie et de qualité logiciels, en particulier sur le versant sécuritaire.

II.– Relations avec les sous-traitants

Une des évolutions significatives du RGPD par raport à la LIL est la clarification des relations avec les sous-traitants, et l'émergence du principe de « co-responsabilité » du traitement. Ces dispositions ont été conçues dans le but de responsabiliser l'ensemble de la chaîne de traitement, et de susciter une collaboration réelle entre ses acteurs. Antérieurement, le sous-traitant ne pouvait être impliqué directement en cas de manquement à la LIL. Le responsable de traitement pouvait éventuellement se retourner contre lui après coup, afin d'espérer une compensation pour la sanction infligée, mais le dommage de la publicité de ladite sanction était supporté seul. Le risque d'une telle séparation était que des prestataires déresponsabilisés offrent à des responsables de traitement peu au fait de la technique, des solutions financièrement moins-disantes mais dont la qualité n'était pas suffisante.

Le RGPD consacre le rôle de conseil du sous-traitant, voué à accompagner ses clients responsables de traitement dans la mise en œuvre de processus conformes à la loi. Le respect du RGPD par les sous-traitants, les garanties qu'ils peuvent apporter sur ce point, et les services à valeur ajoutée relatifs à la mise en conformité qu'ils peuvent apporter, constitueront des critères déterminants pour leur sélection par les clients responsables de traitements. Les services fournis par les sous-traitants peuvent être techniques, mais aussi juridiques et méthodologiques, tels que la mise en œuvre de procédures formelles encadrant les actes contractuels relatifs à la fourniture de solutions informatiques : recette, audits de sécurité, etc.

À l'inverse de ce que prétendent certains, le RGPD n'institue pas un renversement de la charge de la preuve de conformité du responsable de traitement, mais acte le passage à une obligation de moyens renforcée. Celle-ci impose la formalisation et la documentation des procédures relatives à la sécurité des données à caractère personnel. Il sera d'autant plus facile à un responsable de traitement de monter sa bonne foi qu'il disposera d'éléments matériels attestant de sa volonté de conformité, avec l'appui de ses sous-traitants.

III.– Apprentissage de l'hygiène numérique

En dépit du fait que les enfants et la majorité des adultes ne sont pas experts en virologie et bactériologie, un certain nombre de principes d'hygiène corporelle sont enseignés dans les écoles et rappelés sur les lieux de travail : se laver les mains avant les repas et après être allé aux toilettes, traiter ses déchets alimentaires et domestiques de façon adéquate, etc. Ces mesures peuvent être renforcées dans le cadre d'environnements professionnels spécifiques : on impose ainsi aux cuisiniers des collectivités des obligations d'hygiène renforcées, tout comme aux personnels médicaux ou travaillant dans des environnements à régimes restrictifs : port de vêtements spéciaux, prise de douches et autres procédures de décontamination, etc.

Les mêmes principes d'hygiène numérique doivent être enseignés aux personnes quant à l'usage des outils numériques, au sein de leur environnement professionnel comme personnel. En effet, la mode du « BYOD » (pour « *Bring Your Own Device* »), consistant à utiliser sur son lieu de travail les mêmes équipements que pour ses usages domestiques), ainsi que la généralisation du télétravail, accroît la porosité entre ces deux environnements. De fait, maintenir un niveau de sécurité suffisant de l'environnement professionnel nécessite le respect de bonnes pratiques de sécurité également dans l'environnement personnel et domestique.

Ces bonnes pratiques comprennent le fait d'utiliser des supports de données chiffrés (disques durs et supports amovibles), et de ne pas recourir inconsidérément à des services « gratuits », à l'ergonomie parfois bien plus plaisante que celle de services équivalents offerts dans l'environnement professionnel, mais qui sont susceptibles de porter préjudice à la confidentialité et à la sécurité des données.

8. F. Pellegrini, « L'originalité des œuvres logicielles », Revue internationale du droit d'auteur, n° 252, avril 2017, pp. 45-105, https://www.la-rida.com/fr/article-rida/3382 .

En particulier, nombre de ces services « gratuits » hébergent en dehors de l'Union européenne les données qui leurs sont fournies, ou sont opérés par des sociétés de droit non-communautaire qui sont susceptibles de faire l'objet, de la part d'États tiers, de mesures judiciaires [9] ou extra-judiciaires [10] d'accès aux données qu'ils gèrent. C'est pour se prémunir contre de tels problèmes que l'Allemagne est intervenue afin que les hébergeurs des silos de données installés en Allemagne soient tous de droit communautaire [11]. En France, une circulaire a rappelé aux collectivités locales l'obligation d'héberger leurs données sur le sol national [12]. D'autres pays, tels que la Russie, ont pris des mesures similaires de « territorialisation » des hébergements et traitements de données, qui participent à la mise en œuvre d'une politique de souveraineté informationnelle.

Il est également nécessaire de sensibiliser le personnel des entreprises et administrations vis-à-vis des techniques d'intrusion par ingénierie sociale. On désigne par ce terme les méthodes recourant à la psychologie ou à l'astuce pour obtenir des personnes visées les informations recherchées. Par exemple, cela peut consister à se faire passer pour un technicien du prestataire de service informatique afin de solliciter d'une personne la communication de son mot de passe, au prétexte de problèmes de configuration informatique à résoudre. Ces méthodes fonctionnant mieux sur les personnels étrangers et/ou nouvellement arrivés, car souvent peu au fait des procédures et ne sachant pas quels sont les usages ni les risques à s'opposer à une personne se réclamant d'une autorité supérieure, des sessions de formation doivent être dispensées à tout nouvel entrant, incluant ces risques et les procédures de signalement à mettre en œuvre. L'ANSSI a édité un « Guide d'hygiène informatique », qui peut aider les responsables de traitements à mettre en œuvre et suivre l'application de ces mesures [13].

La sécurité des données à caractère personnel n'est donc pas un processus figé, aux résultats acquis. Il s'agit d'un processus dynamique, dont les procédures doivent être réévaluées en permanence à l'aune de l'évolution des menaces. Dans le cadre du RGPD, les autorités de protection des données s'attacheront donc, en cas d'incident, à étudier la trajectoire et l'implication du responsable de traitement et de ses sous-traitants dans la sécurisation de ses données, objectif partagé par l'ensemble des acteurs concernés.

9. C'est ainsi qu'un juge étasunien a pu exiger de Microsoft la remise par ce dernier de données personnelles pourtant hébergées sur l'un de ses serveurs situés au sein de l'Union européenne. Voir : Samuel Gibbs, « *US court forces Microsoft to hand over personal data from Irish server* », The Guardian, 29 avril 2014, https://www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server .

10. Edward Snowden a ainsi révélé comment la NSA étasunienne et le GCHQ britannique accédéaient aux flux de données transfrontaliers des grands silos de données étasuniens dans le cadre du projet MUSCULAR ; voir : Iain Thomson, « *NSA, UK hacked Yahoo! and Google data center interconnects – report* », The Register UK, 31 octobre 2013, https://www.theregister.co.uk/2013/10/31/nsa_and_uk_hacked_yahoo_and_google_data_center_interconnects_report/ . L'accès direct aux datacentres de ces grands silos est pour sa part mis en œuvre dans le cadre du programme PRISM ; voir : Glenn Greenwald et Ewen MacAskill, « *NSA Prism program taps in to user data of Apple, Google and others* », The Guardian, 7 juin 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data .

11. Voir par exemple : Jean Kaminsky, « Un "Cloud allemand" imposé à Microsoft », Solutions numériques, 17 mars 2016, https://www.solutions-numeriques.com/un-cloud-germanique-impose-a-microsoft/ .

12. Note d'information n° 2016/004 du 5 avril 2016 relative à l'informatique en nuage, B.O. du ministère de la culture et de la communication n° 258, mai 2016, pp. 43-45, http://www.culture.gouv.fr/content/download/145167/1566564/version/1/file/BO%20n%C2%B0%20258%20(mai%202016).pdf .

13. Voir : https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/ .