CIBA Conférence Information Bibliothèques Archives

2ème édition | 26-28 août 2022 |

Evénement virtuel

Gouvernance de l'information et du numérique

Communication

La protection des données personnelles : quelle pratique au Bénin ?

Randolphe H. Aglikpo
Université de Toulouse Jean Jaurès, Toulouse, France

Randolphe Hildebert Aglikpo est titulaire d'une Licence professionnelle en Archivistique obtenue en 2018 à l'École Nationale d'Administration (Université d'Abomey-Calavi, Bénin). Il est étudiant en Master Ingénierie de l'information numérique à l'Université Jean-Jaurès de Toulouse en France. Il peut être joint à l'adresse randolphehild@gmail.com.

La protection des données personnelles : quelle pratique au Bénin ?

Randolphe H. Aglikpo
Université de Toulouse Jean Jaurès, Toulouse, France

Résumé

Avec le développement de l'internet et des services numériques, la sécurité des données est devenue un enjeu de plus en plus important tant pour les personnes physiques que morales. Diverses organisations et même État ont été victime d'une cyberattaque, mettant hors service tout ou une partie de leur système informatique. Les réseaux sociaux sont devenus aujourd'hui un moyen, des mines d'or de collecte de données. Clic sur un lien malveillant, piratage d'ordinateur… plusieurs moyens peuvent permettre aux personnes malveillantes d'avoir accès à des données. Ces cinq dernières ont particulièrement été marquées par la circulation de vidéos de "Sexetape" sur les réseaux sociaux entraînant diverses conséquences pour les victimes.

Pour se libérer de l'attaque ou encore des chantages, les hameçonnés, sont parfois obligés de payer une rançon ou de céder aux chantages en offrant des services. Pour les entreprises, les cyberattaques peuvent permettre aux pirates d'accéder au système informatique, mais également aux bases de données et aux éléments internes à ce système. Ainsi, noms, prénoms, adresses, numéros de téléphone, de cartes bancaires, documents comptables et financiers se retrouveraient livrés à des pirates informatiques. Toute cette liste de données est regroupée dans ce que l'on appelle les données personnelles.

Mots clés : *Protection des données à caractère personnel ; Code du numérique ; cyberattaque ; piratage ; réseaux sociaux*

Introduction

Avec le développement de l'internet et des services numériques, la sécurité des données est devenue un enjeu de plus en plus important tant pour les personnes physiques que morales. Diverses organisations et même États ont été victime d'une cyberattaque, mettant hors service tout ou une partie de leur système informatique. Les réseaux sociaux sont devenus aujourd'hui un moyen, des mines d'or de collecte de données.

Clic sur un lien malveillant, piratage d'ordinateur… plusieurs méthodes peuvent permettre aux personnes malveillantes d'avoir accès à des données. Ces cinq dernières années ont particulièrement été marquées par la circulation de vidéos de "Sexetape" sur les réseaux sociaux entraînant diverses conséquences pour les victimes. Pour se libérer de l'attaque ou encore des chantages, les hameçonnés, sont parfois obligés de payer une rançon ou d'offrir des services.

Dans les entreprises, les cyberattaques peuvent permettre aux pirates d'accéder au système informatique, mais également aux bases de données et aux éléments internes à ces systèmes. Ainsi, noms, prénoms, adresses, numéros de téléphone, de cartes bancaires, documents comptables et financiers se retrouveraient livrés à des pirates informatiques. Toute cette liste de données est regroupée dans ce que l'on appelle les données personnelles. On entend par "donnée personnelle " : « toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, ci-après dénommée personne concernée.

Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel un prénom ou un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».(Loi portant code du numérique en République du Bénin., 2018) La protection des données à caractère personnel est enclin dans le dispositif juridique béninois, d'abord par la (Loi portant protection des données à caractère personnel en République du Bénin, 2009) et depuis 2018 par la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin. Cette dernière pose un cadre juridique en matière de protection des données personnelles au Bénin et répond également aux évolutions du numérique.

Cadre institutionnel et réglementaire de la protection des données personnelles au Bénin

Comme expliqué plus haut, la loi n° 2017-20 du 20 avril 2018 portant code du numérique est celle qui régit la question de la protection des données à caractère personnel en République du Bénin. Elle s'applique à toutes les entreprises et collectivités établies sur le territoire de la République du Bénin, mais également aux entreprises qui ne sont pas établies en République du Bénin, mais dans un lieu où le droit de la République du Bénin s'applique en vertu du droit international public. Article 381, livre V code du numérique. Le code du numérique constitue donc une réglementation de grande ampleur, tous les secteurs d'activités, publics comme privés, sont visés.

L'une des grandes révolutions du nouveau code du numérique, est la question de la responsabilisation des entreprises ou de leurs sous-traitants sur la sécurité des données personnelles qu'ils ont collectées. Dorénavant, les entreprises doivent à tout moment pouvoir prouver que leur traitement des données personnelles est correctement effectué. L'Autorité de protection des données personnelles (APDP) du Bénin, nommée jusqu'en 2018 Commission nationale de l'informatique et des libertés (CNIL) veille à la protection des données personnelles.

L'APDP est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle contrôle et sanctionne en cas de manquement à la sécurité des données et pour avoir certaines données personnelles, il faut se référer à l'APDP qui délivre une autorisation après une étude minutieuse et pertinente des raisons qui fondent la demande. C'est d'ailleurs cette responsabilisation pénale qui a pu pousser de nombreuses entreprises réticentes à faire évoluer leurs pratiques, notamment en se déclarant et en mettant en place des mesures nécessaires signifiant le but du traitement des données à caractère personnel collectées. Mais, de quelles données à caractère personnel s'agit-il?

Les données à caractère personnel qui doivent être protégées

Dans le cadre de leur activité, les entreprises sont amenées à traiter un certain nombre de données internes, qu'elles portent sur leurs employés ou collaborateurs qui entrent dans la catégorie des données personnelles. Mais ces données, qui font partie du « patrimoine informationnel » d'une entreprise, sont nécessaires à son bon fonctionnement (ou comment procéder à la paie des salaires et cachets sans les informations bancaires de la personne ?).

Ce patrimoine informationnel est constitué d'informations relatives aux collaborateurs, aux clients, mais aussi aux décisions stratégiques de l'entreprise ou aux informations sur son état financier. Ces données sont particulièrement sensibles. En effet, une personne malveillante ayant trouvé un accès à ce type d'information sur un employé ou un collaborateur pourra plus facilement tenter une usurpation d'identité sur un de ses collègues par exemple.

Selon les pratiques de chaque entreprise, le volume de données sensibles à protéger va être très variable ; la vente en ligne, sur le site de l'entreprise, demande une attention particulière afin que les données bancaires des clients soient bien sécurisées. Il ne faut pas non plus oublier les échanges de données personnelles entre l'entreprise et des personnes extérieures, qu'ils se fassent par courriel, ou même sur les messageries instantanées des réseaux sociaux.

Les entreprises possèdent de plus en plus des sites internet très développés sur lesquels, il est possible de créer un compte client, d'acheter leurs produits et services, de s'inscrire à leur newsletter, ou encore de s'abonner à leurs comptes sociaux Facebook, YouTube et Instagram). La collecte d'informations personnelles se fait sur tous ces services. La création d'un compte client, le service de contact, la gestion des commentaires, tout comme la newsletter, récoltent des données comme le courriel des utilisateurs, les noms, prénoms et adresses des abonnés etc.

Globalement, le code du numérique demande aux entreprises une réelle clarté sur les données personnelles qu'elles collectent, le but de cette collecte, ce qui est fait de ces données sur le long terme et les mesures de sécurité prises par elles pour limiter les risques d'atteintes aux droits des individus. La loi fait aussi normalement obligation aux entreprises de mettre sur leur site internet une charte de confidentialité dès qu'elles sont en possession de données à caractère personnel des clients ou visiteurs de leur site, que le traitement des données est mis en œuvre et que le responsable et/ou les moyens de traitement sont situés sur le territoire béninois. La violation de l'une de ces prédispositions du code du numérique peut entrainer des sanctions.

Les chapitres VI et VII du livre V de la loi n° 2017-20 portant code du numérique en République du Bénin abordent les sanctions encourues en cas de violation de données à caractère personnel. Le code du numérique prévoit trois types de sanctions. Il s'agit des sanctions administratives, des sanctions civiles et des sanctions pénales qui peuvent aller de cinq à dix ans d'emprisonnement et d'une amende de 10 millions à 50 millions de francs CFA. L'APDP peut prononcer un avertissement à l'encontre du responsable de traitement qui ne respecte pas les obligations découlant de la loi en ce qui concerne les sanctions administratives.

Elle peut ainsi prononcer : une sanction pécuniaire, à l'exception des cas où les traitements sont mis en œuvre par l'État ; une injonction de cesser le traitement des données à caractère personnel ; un retrait de l'autorisation accordée en application des dispositions de la loi et un verrouillage de certaines données à caractère personnel. S'agissant des sanctions civiles, en cas d'atteintes graves ou immédiates aux droits et libertés suivant la loi, l'APDP ou la personne dont les droits et libertés ont été violés, peut demander, par voie de référé, à la juridiction compétente, d'ordonner le cas échéant, sous astreinte, toute mesure nécessaire à la sauvegarde de ses droits et libertés. La complicité et la tentative sont punies des mêmes peines.

Il est important de rappeler que constituent des manquements graves : la collecte déloyale des données personnelles, la communication à un tiers non autorisé des données personnelles (photos, vidéos, numéros de téléphone, etc.) ; la collecte des données sensibles, des données relatives à des infractions ou à un numéro national d'identification sans respecter les conditions légales. Aussi, le fait de procéder à la collecte et à l'utilisation des données personnelles ayant pour conséquence de provoquer une atteinte aux droits fondamentaux ou à l'intimité de la vie privée physique concernée est un manquement grave, puni par la loi. Ces différents textes punissent aussi toutes formes de dérapages sur les réseaux sociaux.

N’étant jamais à l’abri d’une cyberattaque ou encore d’un hameçonnage, il existe des outils qui peuvent permettre de prévenir les tentatives de piratage et ainsi protéger ses données. « L'hameçonnage » (ou phishing en anglais), est un type d’attaque informatique utilisant un courriel frauduleux (l’attaquant se fait passer pour un organisme officiel, une entreprise, voire un individu proche du destinataire) afin de tenter de récupérer des informations personnelles, ou même directement de l’argent.

Outils pour protéger les données personnelles

En l’absence de contrôles informatiques stricts, le risque d’erreur humaine, expose toute organisation à de la perte de données. Les causes de cyberattaques proviennent généralement d’une faille interne. La communication quotidienne est faite par courriel ou par les réseaux sociaux. Une compromission de la sécurité des communications, amènerait donc à une mise en danger des échanges d’informations personnelles ou financières ayant pu avoir lieu, mais aussi à celle des projets commerciaux de l’organisation, ce qui peut avoir des conséquences économiques et sociales importantes.

Vu l’importance de l’utilisation des courriels dans la communication des entreprises, mais aussi bien sûr, des collectivités ou individus, il est peu étonnant que ces mêmes messageries électroniques soient ciblées dans des attaques informatiques. Ce type d’attaque n’est ni rare, ni récent, mais reste efficace ; 43% des violations de données analysées dans le rapport de Verizon ont été initiées par hameçonnage, et on estime également à 4% le nombre de destinataires de ces tentatives se rendant vulnérables à une intrusion ou une usurpation de leur identité. (Widup et al., 2021).

Certaines de ces attaques sont directes : le destinataire du courriel a cliqué sur un lien frauduleux menant vers une imitation d’un site officiel ou marchand et rentre lui-même des données personnelles. C’est le cas des pratiques qualifiées de « gayman » au Bénin. D’autres sont indirectes, le courriel peut en effet contenir un virus ou un logiciel malveillant dissimulé en tant que pièce jointe, ou dans un lien, et cliquer sur un de ces éléments va alors pouvoir infecter le système informatique, l’ordinateur ou le téléphone portable si celui-ci n’est pas suffisamment protégé. De là, des documents sensibles pourront être récupérés par la personne à l’origine de l’attaque. Un type d’attaque simple en apparence donc, mais qui peut avoir des conséquences très importantes, et qui est en perfectionnement constant : un courriel dangereux pouvant aussi bien provenir d’une adresse connue ayant été piratée.

La sensibilisation et la formation des employés ou individus aux bonnes pratiques à avoir en cas de courriel ou de messages douteux est essentielle. L’APDP a à cet

effet un rôle important à jouer. Même si cela semble encore insuffisant eu égard des dérives constatées, l'APDP a mis en place divers dispositifs pouvant permettre à chaque citoyen de se renseigner sur la protection des données à caractère personnel. Sur son site internet, elle a publié des textes, décisions et lois réglementant la protection des données. Elle a également mis en place des dispositifs de conseil, d'outils de conformité, de protection des cookies, de veilles informationnelles (à travers la rubrique l'arnaque du mois), droits et devoirs destinés à renseigner, prévenir et aider chaque citoyen à comprendre et à prendre les mesures idoines en matière de protection de données à caractère personnel.

L'APDP a mis en ligne divers formulaires ayant rapport à la protection des données : déclaration des données à caractère personnel sur un site web, demande de déclaration, demande d'autorisation, déclaration de système de vidéosurveillance ainsi que les procédures de saisie de l'APDP, les formalités préalables à la mise en œuvre des traitements, les plaintes, réclamations et pétitions. Même si, elle a eu à organiser des formations notamment à l'égard des acteurs du secteur public ou encore des collectivités territoriales sur la mise en conformité en matière de protection des données personnelles, celles-ci restent moindre face à l'enjeu et l'importance que représentent les données à caractère personnel.

On remarque encore qu'une masse importante de la population béninoise ne connait pas ce que signifie données à caractère personnel, n'est pas encore outillée ou encore n'a pas connaissance de l'existence du code du numérique et des dispositions à prendre pour ne pas enfreindre à ses règles. Cela s'explique par les dérives notamment sur les réseaux sociaux où des entreprises ou « influenceurs web » demandent à leurs internautes de fournir leur numéro téléphone et autres informations sans prendre les dispositions nécessaires pouvant permettre de protéger ces données mises à la connaissance de tous. Une vraie politique de vulgarisation de la loi portant code du numérique devra être mise en place.

L'APDP peut également travailler dans le sens de mettre en place une formation MOOC en ligne sur la protection des données à caractère personnel à destination de tous. Si la sensibilisation et la formation des employés ou individus aux bonnes pratiques à avoir en cas de courriel ou de messages douteux est essentielle, il existe d'autres technologies ou astuces simples qui peuvent permettre d'assurer la sécurité du système d'information, de l'ordinateur ou du téléphone portable. Pour les organisations, cela se traduira par la mise en place de technologies de : contrôle d'accès, ad hoc, surveillance de réseau, sauvegarde et récupération et de cryptographie.

Messagerie chiffrée, mot de passe, lecteur de proximité, pare-feu, antivirus, il existe diverses technologies qui permettent de protéger les systèmes

d'informations, de détecter très tôt les intrusions et de les supprimer. Il existe aussi des outils qui peuvent permettre de protéger aussi son téléphone. Internet, le smartphone, les objets connectés nous relient au vaste monde, pour le meilleur et pour le pire. Ils font continuellement partie de nos vies. En permanence et en continu, nous surfons sur le net avec des alter ego numériques construits à partir de nos données personnelles. Sites, applications, moteurs de recherche, serveurs, pour la plupart gratuits, offrent une valeur ajoutée non négligeable à notre quotidien.

Néanmoins, en contrepartie, nous donnons en échange des informations nous concernant, des informations qui nous décrivent, qui sont ensuite revendues à toutes les entreprises qui cherchent à nous connaître. C'est le principe de la publicité ciblée qui inonde le web d'aujourd'hui. Sans pour autant garantir la sécurité des données, de petites astuces sur le web peuvent permettre de limiter la collecte des données par les sites marchands ou encore pour se protéger.

Il est conseillé de lire les conditions générales d'utilisation afin de déterminer l'usage qui sera fait des données collectées sur le site. Il faut également penser à sécuriser son mail en utilisant un mot de passe de plus de 12 caractères minimums, sans que ce soit son prénom, sa date de naissance ou ceux d'un parent proche. L'usage d'une suite de lettres et de chiffres aléatoires et les caractères spéciaux est plutôt recommandé. En cas de difficultés, il existe des générateurs de mots de passe. Ce mot de passe devra être changé régulièrement et ne doit pas non plus être utilisé pour tous les sites.

Avant tout achat sur internet, il est important de s'assurer avant tout de la présence du petit cadenas dans la barre de recherche en haut de la page (celle qui contient l'adresse du site que vous visitez). Ce cadenas est le sésame indispensable avant toute emplette en ligne, il garantit l'existence d'un protocole HTTPS sur le site marchand, clé d'un shopping sécurisé. La règle d'or à ne pas oublier est de ne pas laisser ses coordonnées bancaires sur un site dépourvu de cette protection ! Cette règle est également applicable pour tous les liens. Sur la toile, il est également conseillé le recours à un VPN, un canal privé qui permet de sécuriser les échanges. Il permet de transiter les données numériques à travers un réseau chiffré à défaut d'avoir une technologie de messagerie privé qui est relativement coûteuse et plus adaptée aux organisations.

La cherté et la mauvaise qualité de la connexion internet amènent beaucoup de personnes à faire recours aux réseaux wifi publics non sécurisés. Ces types de réseaux sont légion : bibliothèque, restaurant, etc. Généralement appelées « hotspot », ces connexions 100 % gratuites sont pratiques, mais doivent être utilisées avec vigilance, car les informations qui y transitent ne sont pas protégées. Elles ne représentent toutefois pas la solution de choix pour consulter la balance

d'un compte bancaire, effectuer une transaction ou encore envoyer des fichiers ou données sensibles. Par ailleurs, le chapitre IV du livre V de la loi n° 2017-20 portant code du numérique en République du Bénin pose les obligations incombant aux responsables de traitement.

Avant d'engager tout projet de collecte de données à caractère personnel, le responsable du traitement doit faire une analyse sur la licéité du traitement, le fondement du traitement, la finalité du traitement, la pertinence et la proportionnalité des données, la sécurisation et la protection des données, la conservation limitée des données et la transparence des informations sur l'utilisation des données. Ce dernier point est encore plus important.

Le responsable du traitement ou son représentant a l'obligation de fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés quelques informations telles que : son identité et l'adresse de sa résidence habituelle ou de l'établissement principal et le cas échéant, les coordonnées de son représentant ; les coordonnées du délégué à la protection des données (DPO) ; les catégories de données concernées ; l'existence d'un droit de s'opposer, sur demande et gratuitement au traitement de données à caractère personnel la concernant envisagé à des fins de prospection notamment commerciale, caritative ou politique ; etc.

Il doit également garantir et faciliter notamment le droit d'information et de réponse de la personne concernée par les données à caractère personnel. Le responsable du traitement a, à cet effet, l'obligation de l'informer dans les meilleurs délais et en tout état de cause dans un délai de trente jours à compter de la réception de la demande. Il est également fait obligation au responsable du traitement et au sous-traitant de désigner un DPO. Ce dernier dispose de connaissances spécialisées du droit et des pratiques en matière de protection des données.

Il informe et conseille le responsable du traitement, le sous-traitant et les employés sur les obligations les incombant en matière de traitement et de protection de données. Il s'assure du respect des dispositions légales en la matière à travers les contrôles, les sensibilisations et formations. Il lui ait fait obligation d'assurer le respect de la durée de conservation, de garantir la pérennité des données et aussi la tenue du registre des activités de traitement par chaque responsable du traitement ou son représentant.

Conclusion

Depuis 2009 avec la création d'abord de la CNIL et la loi 2009 sur la protection des données à caractère personnel renforcée depuis 2018 par le code du numérique et l'APDP, l'État Béninois marque une certaine volonté à assurer la protection des données à caractère personnel de ses citoyens. Un important travail reste néanmoins à faire pour amener ou contraindre autant les entreprises privées que les structures étatiques sur la mise en conformité par rapport aux dispositions du code du numérique en matière de protection de données à caractère personnel.

De nombreuses solutions existent dans le but de protéger les données à caractère personnel. Le plus important aujourd'hui, reste la prévention, la formation et la vulgarisation des dispositions du code du numérique aux employés et citoyens en général sur la protection des données à caractère personnel. Cela s'avère indispensable eu égard des différentes dérives observées sur les réseaux sociaux depuis quelques années.

Références bibliographiques

Loi portant protection des données à caractère personnel en République du Bénin, Pub. L. No. Loi N° 2009-09 du 22 mai 2009 (2009). https://sgg.gouv.bj/doc/loi-2009-09/

Loi portant code du numérique en République du Bénin., Pub. L. No. Loi N° 2017-20 (2018). https://sgg.gouv.bj/doc/loi-2017-20/

Widup, S., Pinto, A., Hylender, D., Bassett, G., & langlois, philippe. (2021). 2021 Verizon Data Breach Investigations Report.