Commission Nationale de l'Informatique et des Libertés du Bénin (CNIL Bénin)

Deuxième édition des Journées Nationales de l'Informatique et des Libertés

Palais des Congrès de Cotonou, 04 et 05 août 2015.

RAPPORT FINAL

PLAN

B- Recommandations aux concepteurs d'appareils électroniques et aux opérateurs de téléphonie mobile
C- Recommandations aux autorités étatiques
D- Recommandations à la CNIL

Cérémonie de clôture

Prologue

Le troisième millénaire est caractérisé par un développement fulgurant de la technologie. Il n'existe, de nos jours, aucun domaine où le génie technologique ne soit présent. Avec le développement exponentiel et incontrôlé des technologies de l'information et de la communication, il est difficile, voire impossible, de cerner toutes les implications, et surtout tous les risques auxquels se trouvent exposés les consommateurs. La chose est d'autant plus criarde qu'on se demande s'il existe encore des données de la vie privée des utilisateurs de ces technologies de l'information et de la communication qui échappent à l'emprise de ces outils.

C'est dans le but de cerner tous les contours et les enjeux de la protection des données personnelles au regard de la prééminence des technologies de l'information et de la communication, que la Commission Nationale de l'Informatique et des Libertés du Bénin (CNIL Bénin) a organisé, les 04 et 05 août 2015, au Palais des Congrès de Cotonou, la deuxième édition des Journées Nationales de l'Informatique et des Libertés. Ces deux journées ont permis aux participants de comprendre les risques qu'induisent les technologies de l'information et de la communication, mais aussi de s'informer de certains dispositifs de protection des données privées.

Ce rapport restitue les différentes activités effectuées au cours des deux journées. Il s'agit, en clair, de la synthèse des allocutions, des communications, des débats et des recommandations qui en découlent.

I- Cérémonie d'ouverture du colloque

La cérémonie d'ouverture est marquée par deux allocutions, présentées par Nicolas Benon, président de la CNIL ; et Thomas Yombo, ministre chargé des Relations avec les Institutions, représentant le chef de l'Etat.

A- Allocution de bienvenue du président de la CNIL

Le président, au début de ses propos, a souhaité la bienvenue aux autorités politico-administratives venues rehausser de leur présence la cérémonie d'ouverture, aux participants, à madame la présidente de la CIL Burkina Faso et à madame Marie Georges, Experte indépendante Informatique et Libertés. Il a, par la suite, rappelé la tenue de la première édition des Journées Nationales de l'Informatique et des Libertés, le 12 novembre 2012, autour du thème « Informatique : Comment protéger ses données ». La question reste d'actualité. Elle se pose de plus en plus,

avec acuité, d'où le thème retenu pour ces deuxièmes journées : « Protection de la vie privée : enjeux et défis ». Monsieur Benon n'a pas manqué, dans son allocution, de rappeler l'historique de la CNIL Bénin et d'énumérer les difficultés auxquelles elle est confrontée, avant d'annoncer le programme du colloque.

B- Allocution du représentant du chef de l'Etat

Dans son allocution, le ministre a jugé de l'opportunité de la création de la CNIL Bénin, par la loi N° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel. Il a salué le président et tous les membres de la CNIL pour le travail d'information et de sensibilisation aussi bien à l'endroit des populations que des responsables des traitements des données personnelles, sur leurs droits et leurs devoirs. Il a, par la suite, souhaité la bienvenue à madame Marguerite Ouédraogo, présidente de la CIL Burkina Faso et vice-présidente de l'Association Francophone des Autorités de Protection des Données personnelles, et madame Marie Georges, consultante auprès du Conseil de l'Europe. En réponse aux doléances formulées par le président de la CNIL, le représentant du chef de l'Etat a promis l'appui conséquent du gouvernement afin que la prochaine mandature de la CNIL ait les ressources nécessaires pour mener à bien sa mission républicaine, car, à l'en croire, « le droit à la protection des données à caractère personnel constitue un droit fondamental ». Le ministre a, pour finir, invité les différents acteurs, ainsi que les populations, à plus de responsabilités dans la protection des données personnelles.

II- Communications sur divers thèmes

Il s'agit, ici, de rappeler les communications qui ont été présentées pendant les deux journées. Elles sont appuyées par l'expérience du Burkina Faso en matière de protection des données privées.

A- Communication sur le thème : « Technologie, usages, droit informatique et libertés : les enjeux quotidiens, locaux, régionaux et mondiaux », par Mme Marie Georges

Madame Marie Georges a commencé sa communication par l'histoire de l'ordinateur, son évolution dans le temps et les multiples traitements que les concepteurs en font, souvent à l'insu de l'utilisateur. Elle a ensuite abordé la nature des données personnelles, qui sont « l'expression de notre identité, de notre personnalité, de nos choix ». Selon la nature, l'origine et la portée des innovations, certains principes peuvent être mis à mal, telles la centralisation des fichiers, la

biométrie, etc. De la même façon, la nature, l'origine et la portée des données peuvent engendrer d'autres problèmes. C'est le cas des réseaux sociaux qui ne garantissent aucune intimité, mais aussi des paiements par smartphone, etc. Ces smartphones, en effet, permettent des enregistrements de renseignements personnels dans la base de données dont seul le concepteur a la maîtrise et l'utilisation.

Il n'existe, actuellement, aucune procédure de certification de l'absence de back door dans le logiciel de base. De même, il n'existe pas de procédure systématique d'information, y compris pour la durée de conservation, et de consentement préalable pour l'accès d'une application Smartphone à toute donnée personnelle interne à l'équipement. C'est le cas de l'accès invisible à la géolocalisation, et au répertoire des noms, des numéros de téléphone, etc.

Madame Marie Georges a également abordé la question du Cloud, des Big Data et de l'Internet des objets, qui ont aussi des enjeux d'ordre technique et juridique en ce sens qu'ils ne garantissent pas la vie privée du consommateur ou de l'utilisateur. En conclusion, la communicatrice a formulé des recommandations pour garantir un tant soi peu la vie privée des personnes. Nous y reviendrons dans la suite du rapport.

B- Communication sur le thème : « Les réseaux sociaux et le flou de la vie privée : Cas de Facebook », par M. Emmanuel Zossou

Le deuxième communicateur est parti d'un constat : « Avec l'avènement de Internet et de web 2.0, tout le monde est producteur de contenu ». Et ce contenu que tout le monde peut produire, est également accessible à tout le monde, avec ou sans le consentement du "producteur". Et cela s'accentue avec les réseaux sociaux qui s'imposent comme des réalités incontournables. Or ceux-ci enregistrent au fur et à mesure les données personnelles qui sont, par la suite, exploitées à des fins inconnues.

Monsieur Zossou a expliqué que toutes les données enregistrées par exemple sur le serveur de Facebook sont récupérées et abondamment vendues, par tous les moyens, que ce soit aux annonceurs ou autres. Facebook n'est donc pas aussi gratuit que le pensent les internautes. Ils doivent savoir que c'est le prix à payer. Voilà, selon lui, « la face cachée de Facebook ». Il a illustré ses propos par des exemples.

Le communicateur s'est aussi indigné de l'accès incontrôlé des enfants à Facebook. Ils y mettent tout et visualisent tout, sans se rendre compte des dangers auxquels ils s'exposent ainsi. Les réseaux sociaux ne sont donc pas aussi merveilleux qu'on le pense, puisque toute notre vie privée est enregistrée.

Heureusement, s'est réjoui le communicateur, il existe des organismes de protection des données personnelles. Néanmoins, cela ne suffit pas tout de même à résoudre définitivement le problème de fuite de données personnelles, car les réseaux sociaux continuent toujours leur piratage.

Monsieur Zosou, à l'issue de sa communication, a formulé des recommandations.

C- Communication sur le thème : « Etat de droit, vie privée et technologie de surveillance », par Mme Marie Georges

La seconde communication de madame Marie Georges a été présentée en trois parties. D'abord le rappel des principes de la protection des personnes à l'égard du traitement numérique de données, ensuite les cas de dérogations aux principes, et enfin les préconisations.

La loi sur l'informatique et les libertés a clairement énuméré les principes de la protection des personnes à l'égard du traitement numérique de données. Chacun de ces principes répond aux risques d'abus et nécessite alors des garanties telles que la légitimité, la proportionnalité, la sécurité, etc. Toutefois, des dérogations peuvent être constatées. Ce sont, par exemple, les traitements liés aux enquêtes de la police judiciaire, et les traitements de surveillance effectués par les services de renseignements. Mais que ce soit pour l'une ou l'autre dérogation, la législation prévoit des garde-fous pour éviter les abus, les dérives.

Par ailleurs, des doutes sont à émettre quant à l'efficacité de ces dérogations.

Pour finir, la communicatrice a fourni un certain nombre de préconisations internationales pour réglementer la technologie de surveillance. Il s'agit de la même garantie pour les personnes, sans considération de nationalité ou de résidence. Mais en vérité, cela n'existe nulle part.

D- Communication sur le thème : « Téléphonie mobile et vie privée », par Me Yvon Détchénou

Pour Me Détchénou, le développement technologique a fait entrer le téléphone portable dans nos vies. Or ce que les utilisateurs ignorent, les téléphones portables

ne sont plus un simple moyen de communication, mais des terminaux mobiles, devenus, à notre insu, de vrais condensés de technologies, des outils informatiques avec des capacités surprenantes. Ces appareils sont dotés de services à distance qui gèrent des paramètres de notre vie quotidienne. Ils mémorisent nos moindres données personnelles, que ce soient nos activités, nos conversations, nos goûts, nos centres d'intérêt, ou nos habitudes. Et toutes ces données, ils les transmettent à des centres de stockage qui les utilisent selon leur bon vouloir. Ceci pose la problématique de l'intrusion dans les téléphones portables.

Parlant d'intrusion, Me Détchénou distingue les données volontairement transmises des données acquises à l'insu de l'utilisateur. L'utilisateur introduit dans son téléphone portable certaines de ses données personnelles, et ceci volontairement, juste pour activer le fonctionnement de son appareil, sans savoir que ces renseignements sont stockées dans une base de données et peuvent être à tout moment utilisées à d'autres fins. Ces données sont transmises par l'utilisateur même, certes ; mais de façon presque inconsciente, ignorante. D'un autre côté, il y des données personnelles de l'utilisateur qui sont enregistrées par le téléphone même, seulement par son activité propre, aussi bien par les interfaces qui y sont installées que par les équipements qui le composent.

Mais que ce soit dans l'un ou l'autre cas, la problématique autour du caractère intrusif du téléphone portable dans la vie privée du consommateur pose un double problème : d'abord la question de la protection juridique de la vie privée, ensuite la question de la propriété des données personnelles.

Face à la difficulté de protection des données personnelles avec l'avènement des technologies de l'information et de la communication, la question que se pose le conférencier est : « Est-ce la vie privée qu'on va devoir réduire ? Ou est-ce la possibilité d'accès qu'on va devoir élargir ? ». La question reste en suspens et mérite qu'on y réfléchisse sérieusement.

III- Poursuite des communications

A- Communication sur le thème : « L'usage de la biométrie au Bénin et ses enjeux vis-à-vis de la protection des libertés fondamentales », par M. Emmanuel Zossou

L'intervention de monsieur Zossou a été faite en deux parties : Les généralités et les enjeux. Après une définition claire de la biométrie, le communicateur a énuméré les diverses possibilités d'identification, que sont : Ce que l'on possède, Ce que l'on sait, et Ce que nous sommes ; c'est-à-dire notre corps. L'usage de la biométrie

répond, à l'en croire, à plusieurs besoins : le besoin de confort et le besoin de sécurité. Les avantages et inconvénients de la biométrie ont mis un terme à la première partie de la communication.

La seconde partie, quant à elle, est relative aux enjeux que présente la biométrie. Ce sont, en premier lieu, la problématique de l'introduction de la biométrie dans les listes électorales au Bénin, et en second lieu, la pertinence du choix et des moyens mis en œuvre au regard de la protection de la vie privée, sans en mesurer les conséquences sur la vie privée ; et aussi sans un cadre juridique approprié.

D'un autre côté, il y a inquiétude quant à l'utilisation faite des données biométriques. Ces données ainsi collectées exposent les citoyens à des vols permanents d'identité, à un risque de sécurité lié à la centralisation des bases de données, de sécurité des réseaux, de discrimination des personnes, de piratage des technologies, des limites de la technologie utilisée, entre autres.

Le communicateur a terminé son intervention en formulant des questionnements sur le respect des données personnelles par l'utilisation des données biométriques à des fins électorales.

B- L'expérience du Burkina Faso en matière de protection des données à caractère personnel, par Mme Marguerite Ouédraogo Bonane

Madame Marguerite Ouédraogo Bonane, présidente de la CIL Burkina Faso et vice-présidente de l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP), a commencé son intervention par la projection d'un film présentant la CIL Burkina et ses diverses interventions et activités pour la sécurisation des données privées dans le pays. Elle a ensuite fait l'historique de la structure qu'elle dirige depuis des années.

La communicatrice a ensuite présenté les grandes activités menées par la CIL Burkina, avant d'émettre des perspectives sur plusieurs plans.

IV- Les grandes recommandations

Les travaux ont permis aux participants de se rendre compte que la situation est assez alarmante. Tout nous échappe, plus rien ne nous appartient. Que faire alors ?

Accepter les outils modernes, ou plutôt ne pas en adopter du tout et mener une vie d'homme des cavernes ? Toute la question est là. Des travaux de cet atelier, plusieurs recommandations ont été formulées pour lutter contre ce qu'on peut appeler l'espionnage de la vie privée. Ces recommandations concernent les consommateurs eux-mêmes individuellement, les concepteurs, les opérateurs de téléphonie mobile, les autorités étatiques et la CIL.

A- Recommandations à l'endroit des utilisateurs

En tant que premiers concernés, les utilisateurs de technologies doivent prendre des mesures pour sécuriser leurs données personnelles, afin de ne pas se faire espionner. Il s'agit, entre autres, de :

- Lire les conditions d'utilisation d'un service avant de l'installer. Les avis des autres utilisateurs peuvent également être utiles ;

- Verrouiller l'écran de son appareil pour ne pas en permettre l'accès à d'autres personnes ;

- Ne pas partager son mot de passe avec des amis ;
- Se méfier des réseaux Wi-Fi accessibles gratuitement ou ouverts à tous ;

- Avant de s'inscrire sur un site, se renseigner sur les conditions de protection de la vie privée ;
- Configurer les paramètres de confidentialité en toute connaissance de cause.
- Ne pas divulguer trop d'informations à caractère personnel sur Internet ;

- Vérifier à quelles données contenues dans son Smartphone l'application à installer va avoir accès, en fonction de ce que le téléphone permet ;
- Ne pas télécharger d'applications de source inconnue et arrêter régulièrement les applications qui continuent à tourner « en tâche de fond » alors que vous ne les utilisez pas en ce moment-là.

B- Recommandations aux concepteurs d'appareils électroniques et aux opérateurs de téléphonie mobile

Il leur est recommandé notamment, de :

- Respecter la vie privée des individus, ce qui revient à respecter les dispositions légales existant en la matière ;

- Fournir au client tous les renseignements nécessaires sur les fonctionnalités des appareils et services et y recueillir son entière adhésion avant de le mettre à sa disposition.

C- Recommandations aux autorités étatiques

L'Etat doit :

- Mettre à la disposition de la CNIL les ressources adéquates ;
- Renforcer le cadre légal ;
- Mettre à jour les recommandations ;
- S'assurer que le cadre légal est approprié en matière d'écoute et de vidéosurveillance.

D- Recommandations à la CNIL

A la Commission Nationale de l'Informatique et des Libertés, il est recommandé de :

- Informer suffisamment les populations sur la législation en vigueur, leurs droits et devoirs en matière de données à caractère personnel ;
- Suivre les nouvelles technologies et les nouveaux usages ;
- Les analyser au regard des DH et des transformations sociales en jeu ;
- Formuler des recommandations nécessaires après échanges avec les parties prenantes et avec leurs homologues.
- Interpeller les structures privées de collecte de données personnelles à des fins particulières, pour qu'elles se conforment à la législation.

Conclusion

Les deux journées qu'a duré cet atelier d'écoute et surtout d'échanges ont permis aux participants de se rendre compte que la vie privée est menacée de nos jours. Audace, Persévérance, Vigilance et Collaboration doivent être les maîtres-mots de tous les acteurs de la protection de la vie privée. Nous finirons par une recommandation du président Obama : « Attention à ce que vous postez sur Facebook, cela pourrait se retourner contre vous tôt ou tard… Quoi que vous fassiez, on vous le ressortira à un moment ou à un autre de votre vie ». Et l'autre de compléter : « Souriez toujours, on vous observe ! ».