**ETAT DE L’ART**

**Parenthèse sur la sécurité informatique**

La sécurité peut être définie comme étant une situation, un état dans laquelle quelqu’un ou quelque chose n’est exposé à aucun danger, à aucun risque d’agression, de détérioration ou encore par le long processus visant à atteindre cet état.

Lorsqu’on parle de sécurité dans le domaine des technologies de l’information et de la communication, on fait très souvent allusion à la sécurité de l’information. La sécurité de l'information, en anglais *Information Security* abrégé *Infosec* consiste en la mise en place d’un ensemble de stratégies pour gérer les processus, les outils et les politiques nécessaires pour prévenir, détecter, documenter et contrer les menaces à l'information. La sécurité de l’information recouvre donc toutes les techniques permettant d’assurer la protection de l’information. La sécurité de l’information se fonde sur 3 principes fondamentaux :

* la confidentialité : c’est le fait d’assurer que l’information ne puisse être accessible qu’à ceux qui ont l’autorisation de la consulter. Cela sous-entend le fait de rendre inintelligible cette information aux personnes non autorisées ;
* l’intégrité : assurer que l’information n’est pas modifiable par un tiers non autorisé. Elle consiste à certifier que les données n’ont pas été détruites ou altérées tant de façon intentionnelle qu’accidentelle ;
* la disponibilité : assurer que l’information est accessible en temps voulu par ceux qui en ont l’autorisation. Ne pas pouvoir accéder à une information en temps voulu est semblable à la non-possession de celle-ci.

Comme principes supplémentaire, nous notons :’

* l’authentification : elle consiste à assurer l’identité d’un tiers et permet de garantir qu’un tiers est bien celui qu’il prétend être ;
* la non-répudiation : le fait de ne pas pouvoir nier une action faite sur le système.

**Parenthèse sur Cryptographie**

La sécurité informatique est un domaine pluridisciplinaire. En effet, pour arriver à ses buts, elle a, tout au cours utilisé, entre autres, la cryptographie. La cryptographie peut être définie comme un art et une science permettant de concevoir des techniques pour garder le secret des messages transmis. Voici les problèmes que doit résoudre la cryptographie :

* la confidentialité
* l’intégrité
* l’authentification

On voit ainsi que la sécurité informatique et la cryptographie partagent des objectifs similaires. Et c’est pour cette raison que tout au long de l’histoire, elle a été utilisée dans le domaine de la sécurité informatique. De même, les évolutions dans le domaine de la sécurité informatique ont souvent été rendus possibles grâce aux avancées de la cryptographie.

On distingue :

* la cryptographie classique qui décrit la période d’avant les ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d’une langue naturelle. Dans cette famille, on retrouve le chiffrement par substitution qui consiste, à remplacer, sans en bouleverser l’ordre les symboles d’un texte clair par d’autres symboles [1] et le chiffrement par transposition qui repose sur le bouleversement de l’ordre des symboles du message clair. Les techniques de chiffrement les plus connues dans cette famille sont le chiffrement de César et le chiffrement de Vigenère.
* la cryptographie moderne qui utilise la puissance de calcul des ordinateurs pour affiner ces techniques de chiffrement. Dans cette famille, nous avons le chiffrement symétrique qui utilise une même clé pour le chiffrement et le déchiffrement (DES en est la technique la plus connue) et le chiffrement asymétrique qui utilise des clés différentes pour le chiffrement et le déchiffrement. RSA est l’algorithme de chiffrement asymétrique le plus utilisé

**Histoire sur sécurité informatique**

**Temps Anciens**

Garder des informations secrètes n’est pas une préoccupation nouvelle. Le domaine de la sécurité des informations est très ancien. Déjà, dans l’antiquité des techniques de chiffrement de l’information ont été utilisées. Vers 1900 av JC, le scribe de Khnumhotep II retraçait la vie de son maître dans sa tombe en utilisant un certain nombre de symboles inhabituels pour masquer le sens des inscriptions avec les hiéroglyphes qu’il dessinait. Vers 500 av. J.-C., les Spartiates ont développé un dispositif appelé Scytale, qui a été utilisé pour envoyer et recevoir des messages secrets. Plus récemment dans l’histoire, l’empereur romain Jules César utilisa la technique de chiffrement qui porte son nom (Chiffrement de César) afin de crypter ses messages personnels. Ces Expériences, Bien Que Ne Couvrant Que Le Principe De La Confidentialité, Sont Les Ancêtres De La Sécurité De L’information.

A cette époque, assurer la sécurité de l’information se résumait en un problème de cryptage de données. On utilisait alors la cryptographie classique avec le chiffrement par substitution d’abord [1] puis plus tard le chiffrement par transposition.

**Temps modernes**

Avec le temps, les techniques permettant d’assurer la sécurité de l’information deviennent de plus en plus pointues. La seconde guerre mondiale a marqué un tournant dans l’histoire de nombreuses technologies, y compris celles qui ont façonné l’industrie de la sécurité de l’information. De nouveaux moyens de communication apparaissent : la radio et le cinéma étaient les principaux vecteurs de l’information. Sur le champ de bataille, les différentes unités devaient coordonner leurs actions et pour ce faire des informations étaient échangées entre elles. Toutes ces communications étaient diffusées par radio et pouvaient être interceptées par l’ennemi. Il était d’une importance cruciale de rendre l’information inintelligible à l’ennemi puisqu’il s’agissait de communiquer sur les stratégies d’actions à mener. Pour protéger ces communications militaires, des systèmes très sophistiquées furent mises en place. Il s’agissait surtout de machines permettant de chiffrer l’information. Enigma était la machine de chiffrement la plus avancée de l’époque : elle sécurisait les communications des flottes et des troupes nazis en leur permettant de chiffrer leurs messages par un chiffrement par substitution. Elle utilisait des algorithmes de chiffrement par substitution très poussés à l’époque. Elle avait la réputation d'être inviolable. Cependant, des experts en chiffrement polonais et britanniques ont réussi à trouver le moyen de casser Enigma en créant une machine connue sous le nom de « Bombe cryptographique » permettant de déchiffrer ses messages, donnant ainsi à la coalition antihitlérienne un avantage significatif ou « l’avantage définitif » selon Churchill et Eisenhower lors de la seconde guerre mondiale et soulignant du même pied l’importance capitale qu’a revêtu la sécurité de l’information lors de cette époque.

Puis, la seconde guerre mondiale laissa place à la guerre froide, une guerre d’opinion opposant deux blocs : d’un côté les états unis démocrates et de l’autre les russes, communistes. Ce fut la naissance d’une course à l’armement et à l’avancée technologique pour dominer le camp adverse.

Durant cette période les premiers ordinateurs sont créés. A cette époque, ils ont beaucoup plus utilisés comme outils de calcul pour des applications scientifiques et n’étaient pas très répandus. C’était des systèmes mono-utilisateurs logés dans de grande salle et il n’y avait pas communication entre ces différentes machines. La sécurité n’était pas une priorité et même dans ce cas n’impliquait que le fait de sécuriser les salles où étaient installées ces machines.

Du fait de leur puissance et de leurs nombreux avantages, de plus en plus d’ordinateurs et de systèmes d’exploitation furent créés. De même, la cryptographie entre dans une nouvelle ère. En effet, des techniques de chiffrement plus avancées sont mises en place grâce à la puissance de calcul des ordinateurs. C’est la naissance de la cryptographie moderne [1].

Avec la prolifération des terminaux distants sur les ordinateurs commerciaux, le contrôle physique de l'accès à la salle informatique n'était plus suffisant. En réponse aux nouvelles vulnérabilités, des systèmes de contrôle d'accès logique ont été développés. Un système de contrôle d'accès maintient une table en ligne des utilisateurs autorisés. Un enregistrement d'utilisateur type stocke le nom de l'utilisateur, son numéro de téléphone, son numéro d'employé et des informations sur les données auxquelles l'utilisateur était autorisé à accéder et les programmes qu'il était autorisé à exécuter. Un utilisateur peut être autorisé à afficher, ajouter, modifier et supprimer des enregistrements de données dans différentes combinaisons pour différents programmes. Dans le même temps, les gestionnaires de système ont reconnu l'importance de pouvoir se remettre de catastrophes pouvant détruire le matériel et les données. Les centres de données ont commencé à faire régulièrement des copies sur bande de fichiers pour le stockage hors site. Les gestionnaires de centre de données ont également commencé à élaborer et à mettre en œuvre des plans de reprise après sinistre. Ce sont les premières politiques de sécurité entreprises. Cependant, même avec un tel système en place, de nouvelles vulnérabilités ont été reconnues au cours des années suivantes. Il fallait des systèmes plus fiables.

**Sécurité informatique encore plus importante avec Multics, Tiger Teams et Pentest**

Multics, un système d’exploitation multi utilisateurs fut créé en 1964. Ce fut la première fois que la problématique de la sécurité de l’information fut prise en compte en amont. En effet, dès la conception de Multics, les décisions prises (langages de programmation, architecture du noyau, etc.) prenaient en compte les exigences de sécurité. Les fonctions de sécurité de Multics comprenaient également le chiffrement des mots de passe, des audits de connexion et des procédures de maintenance logicielle. Les mots de passe dans Multics n’étaient jamais stockés en texte clair. Lorsqu'un utilisateur entrait son mot de passe, ce mot de passe était chiffré, puis comparé au mot de passe stocké sur le système. Cela permit de garder les mots de passes des utilisateurs en cas de dump système. De même, un journal d'audit de connexion enregistrait l'heure, la date et le terminal de chaque tentative de connexion, et notifiait à l'utilisateur le nombre de tentatives de mot de passe incorrectes sur son compte depuis la dernière connexion réussie. Enfin, des procédures de maintenance logicielle, telles que la vérification du nouveau logiciel permettaient de maintenir le système sûr et épargné des régressions de sécurité.   
Au début des années 1970, alors que l’armée américaine était à la recherche de systèmes informatiques multi utilisateurs capables de protéger les informations classifiées, un rapport, connu sous le nom du rapport Anderson, nommé ainsi après le notable James Anderson, recommanda le système Multics pour un développement ultérieur, en raison des caractéristiques de sécurité incluses dès la conception dans Multics.

Pour éprouver la sécurité des systèmes en place, il était très courant de faire appel à des Tiger Team. Il s’agissait d’x rassemblés pour gérer des situations spéciales, régler des problèmes spécifiques le plus rapidement possible. La plus connue de ces équipes est celle rassemblée lors de la mission Apollo 13 qui connut un problème d’atterrissage. Au début, leur travail consistait surtout en des revues manuelles de code pour détecter la source des bugs. Un peu plus tard, s’appuyant sur James Anderson, ils utilisaient le «  pentest » ou test d’intrusion. C’est une méthode permettant d’évaluer la sécurité d’un système informatique à travers des tentatives d’intrusion à la manière d’un attaquant.

* MITRE //

Bien que le rapport de la Tiger Team, mise en place conjointement par l’armée américaine et l’organisme MITRE, chargée de tester Multics ait conclu que ce dernier n'était pas un système totalement sécurisé, les fonctions de sécurité intégrées à Multics le rendaient beaucoup plus sûr que les autres systèmes commerciaux, formant une base à partir de laquelle un système sécurisé peut être dével oppé.

Conscients de cela, deux membres de l’équipe de développement de Multics vont créer un système inspiré de Multics mais moins lourd : UNIX vit le jour. C’est de ce même UNIX que dériva la plupart des systèmes d’exploitation connus de nos jours (Linux, iOS, MacOs, etc.) dont on vante la sécurité.

**Premiers ordinateurs, outils d’analyse de code source**

La décennie 1970 vit également l’apparition des premiers micro-ordinateurs. Cependant, parce qu’ils étaient entièrement autonomes et généralement sous le contrôle d'un seul individu, il y avait peu de problèmes de sécurité. En 1978, le tableur Visicalc a été développé. Visicalc était le premier programme informatique de feuille de calcul, initialement publié pour l’Apple II. Il est souvent considéré comme l'application qui a transformé l’ordinateur personnel d'un passe-temps pour les passionnés d'informatique en un sérieux outil de travail. A partir de ce moment, des logiciels commencent à être créés pour les ordinateurs. L’on sait que pour cela, il fallait écrire du code source parfois enclin à des bugs et à des vulnérabilités de sécurité.

Dès 1969, l’ARPA (Advanced Research Project Agency), une agence dédiée aux projets de recherche avancée renommée plus tard en DARPA (Defense Advanced Research Project Agency) arriva à interconnecter les ordinateurs de quatre universités en un réseau afin de leur permettre de partager leurs résultats de recherche : ce réseau fut nommé l’Arpanet. Dans Arpanet, les utilisateurs se connaissaient plus ou moins et étaient pour la majorité des académiciens : la sécurité n’était pas un problème majeur dans ce « réseau d’amis ». C’est ce simple réseau de quatre nœuds sans aucune préoccupation de sécurité qui conduisit plus tard à la naissance d’Internet et du World Wide Web.

Vers la fin des années 1970, l’analyse de codes source, qui était faite manuellement, vit une révolution. Lint, le premier outil d’analyse de codes source automatisée apparut. Initialement, il était destiné aux codes sources écrits en langage C. Lint était pratique pour trouver des bugs potentiels, mais était très lent et n'était pas équipé de la vue complète du programme. Il ne pouvait analyser qu'un seul fichier à la fois. Lint a ouvert la voie à la première génération d’outils destinés à la sécurité des applications informatiques qui, bien qu'ils aient été utiles pour trouver des bugs spécifiques, étaient assez maladroits et ne faisaient pas mieux que l'analyse manuelle.

**IBM PC, Internet, le ver Morris et les premières sociétés de sécurité informatique**

Les années 1980 marquèrent de réelles avancées. IBM lança le premier ordinateur personnel et bientôt des millions d’ordinateurs personnels pour des usages commercial, industriel et même gouvernemental furent installés. Désormais, les ordinateurs personnels devinrent incontournables à des milliers d’utilisateurs qui y voyaient un outil de travail.

Internet qui était initialement réservé au gouvernement américain, à ses partenaires et à quelques privilégiés commence à avoir de nouveaux nœuds et par conséquent plus d’utilisateurs.

La première grande menace sur le réseau Internet fut celle du Ver Morris en 1988. En informatique, un vers est un programme malicieux capable de s’auto-reproduire et de se déplacer à travers un réseau sans avoir d’un support physique ou logique. Le Ver Morris était initialement un programme conçu afin de mesurer la taille du réseau internet, sans intention néfaste, mais à cause d’un bug de la part de son concepteur, se déplaçait de machine en machine, et une fois sur la machine, ne s’arrêtait pas mais se reproduisait plutôt. Et à partir de là, plusieurs conséquences sont rapidement apparues. La charge processeur qu’il provoquait était susceptible d’altérer les performances de la machine voire d’empêcher son accès. C’est donc devenu par la force des choses une attaque par Déni de Service. Le nombre de victimes du vers Morris est estimé à 6000 représentant 10% de la population Internet d’alors. Cet évènement fut un évènement marquant dans l’histoire de la sécurité informatique. En effet, le ver Morris a parfois été appelé le « Grand ver » à cause de l'effet dévastateur qu'il avait eu sur l'Internet à cette époque, autant pour les pannes causées que pour l'impact psychologique qu'il a eu sur la perception que les professionnels de l’informatique et le grand public avaient de la sécurité et de la fiabilité de l'Internet. L’on réalisa dès lors, que sur le réseau Internet, des évènements malencontreux peuvent se produire et qu’il faudrait penser à prévenir de ce genre de choses en mettant en place des mesures de sécurité pour le rendre plus sûr. Après cet incident et Robert Morris, l’auteur du vers fut condamné par la loi américaine sur la répression des fraudes et infractions dans le domaine informatique (Computer Fraud and Abuse Act). Cette loi a été adoptée un peu plus tôt en 1986 afin de protéger les organismes contre les éventuels cybercriminels qui pourraient s’attaquer à leurs systèmes informatiques.  
De même, la DARPA créa le CERT (Computer Emergency Response Team). Cette organisation était composée d’informaticiens d’horizons différents réunis pour régler l’incident et empêcher ce genre de chose de se produire à nouveau.

Le ver Morris ouvra la voie aux virus et vers informatiques. Bientôt, des individus se mirent à créer des virus, parfois dans un but de faire mal et parfois par des amateurs qui le font par passion. Et cela ne laissa pas indifférents les experts en sécurité informatique de l’époque qui se mirent rapidement à créer des entreprises éditrices d’antivirus. L’industrie de l’antivirus commença ainsi. Du fait des dégâts que peuvent occasionner certains virus, les utilisateurs commencèrent à acheter des antivirus pour sécuriser leurs systèmes informatiques. Bien que des avancées en termes de sécurité aient déjà été faites, ce fut la première fois que le grand public investissait pour s’offrir de la sécurité informatique avec l’achat des premiers antivirus.

A partir des années 1990, Internet devient un réseau mondial à l’aide du World Wide Web qui vit le jour de même que les premiers navigateurs. Internet offre plusieurs avantages importants: le coût est relativement faible, les connexions sont disponibles localement dans la plupart des pays industrialisés et, en adoptant le protocole Internet TCP/IP, tout ordinateur devient instantanément compatible avec tous les autres utilisateurs d'Internet.   
Internet, à ses débuts reposaient exclusivement sur le protocole http, qui reposait à son tour sur le protocole TCP/IP. Mais, il ne garantissait pas la confidentialité et l’intégrité des données transmises. Cependant il n’y avait pas encore d’autres alternatives.

De nouveaux outils de sécurité informatique apparaissent ; des analyseurs de codes source plus évolués et des outils de supervision de réseau à l’instar de SATAN [1], renommé plus tard SANTA. C’est la deuxième génération d’outils destinés à la sécurité informatique.

**Vers un usage massif d’Internet**

Les premières pages Web ne tardent pas à voir le jour aidé en cela par la création du langage Html. En outre, les ordinateurs deviennent de plus en plus dépendants d’Internet et par la même voie deviennent de plus en plus vulnérables aux attaques à travers ce réseau.

Avec la création des premiers navigateurs, le potentiel inouï du Web attire les investisseurs qui y voient des applications commerciales. 1995 a été une année charnière pour le World Wide Web en général et pour la sécurité en particulier. En effet, Netscape [1] a lancé un navigateur web, le Netscape Navigator qui révolutionna la navigation sur le Web. Très rapidement, Netscape réalisa que le Web avait besoin d’être plus dynamique d’où la création de JavaScript adopté comme standard en 1997 par l’Ecma International [1].

Au fur et à mesure qu'Internet se développait, des sites web plus évolués apparaissent : les applications Web. Une application web est un site Web qui permet à ses utilisateurs de réaliser des tâches spécifiques. De plus en plus de sociétés commerciales se mirent à proposer des achats en ligne pour les particuliers. Parmi celles-ci, EBay et Amazon. L'offre se mit à croître régulièrement, mais le chiffre d'affaires dégagé par le commerce électronique restait modeste tant que les clients n'avaient pas une confiance suffisante dans le réseau internet. Une des façons de sécuriser ce paiement fut d'utiliser des protocoles plus sûrs que HTTP qui a rapidement montré des failles de sécurité.

Jusqu’à maintenant, http était le seul protocole utilisé sur le Web. Cependant, avec les nouvelles avancées que ce dernier a connues, les enjeux de la sécurité y sont devenus plus importants. Avec le protocole http, les données étaient transmises en clair, permettant à un individu malintentionné de les récupérer et de les modifier ou de les utiliser à des fins néfastes. Ainsi, en fournissant son nouveau navigateur, Netscape a conçu le protocole SSL.

**SSL**

Ce protocole vient en réponse à la préoccupation croissante de la sécurité sur Internet et tire profit des nouveaux algorithmes de chiffrement tels que l’AES venu remplacé le DES et jugé très sécurisé.

L’objectif du protocole SSL est de créer un canal de données sécurisé entre le client et le serveur. SSL fournit des améliorations de sécurité au protocole HTTP utilisé jusqu’alors.

SSL assure 3 choses:

* **la confidentialité avec des mécanismes de chiffrements**
* **l’intégrité** avec le hachage des données transmises
* **l’authentification** avec l’utilisation de certificats

**Les certificats**

Pour être sûr que la clé publique provient bien de celui que l'on croit, on utilise une autorité tierce (appelé le tiers de confiance). Cette autorité est celle qui va générer une clé publique certifiée par exemple pour un serveur Web, puis c'est ensuite elle qui garantira à tout demandeur (par exemple le client web) que la clé publique envoyée appartient bien à celui qui le prétend (au serveur Web).

La garantie qu'une clé publique provient bien de l'émetteur qu'il prétend être, s'effectue donc via un certificat d'authenticité émanant d'une autorité de certification (AC), le tiers de confiance.

Un certificat est un simple fichier informatique délivré par une **autorité de certification** qui contient :

* la clé publique liée à la clé privée de son détenteur et des informations sur son identité ;
* le nom distinctif de l'autorité de certification ;
* la signature électronique (chiffrement de l'empreinte par clé privée) de l'autorité de certification.

C’est ce certificat qui permet d’initialiser une connexion SSL.

SSL consiste en 2 protocoles:

* **SSL Handshake protocol**: avant de communiquer, les 2 programmes SSL négocient des clés et des protocoles de chiffrement communs.
* **SSL Record protocol**: Une fois négociés, ils chiffrent toutes les informations échangées et effectuent divers contrôles.

La négociation SSL (« *handshake* »)

Au début de la communication le client et le serveur s'échangent:

* la version SSL avec laquelle ils veulent communiquer,
* la liste des méthodes de chiffrement (symétrique et asymétrique) et de signature que chacun connaît (avec longueurs de clés),
* les méthodes de compression que chacun connaît,
* des nombres aléatoires,
* les certificats.

Client et serveur essaient d'utiliser le protocole de chiffrement le plus puissant et diminuent jusqu'à trouver un protocole commun aux deux. Une fois que cela est fait, ils peuvent commencer à échanger des données.

La communication SSL (« *record* »)

Avec SSL, l'expéditeur des données:

* découpe les données en paquets,
* compresse les données,
* signe cryptographiquement les données,
* chiffre les données,
* les envoie.

Celui qui réceptionne les données:

* déchiffre les données,
* vérifie la signature des données,
* décompresse les données,
* réassemble les paquets de données.

SSL utilise:

* un système de chiffrement asymétrique (comme RSA ou Diffie-Hellman). Vous pouvez Ce système est utilisé pour générer la clé principale qui permettra de générer des clés de session.
* un système de chiffrement symétrique (DES, 3DES, IDEA, RC4...) en utilisant les clés de session pour chiffrer les données.
* un système de signature cryptographique des messages (HMAC, utilisant MD5, SHA...) pour s'assurer que les messages ne sont pas corrompus.

C'est lors de la négociation SSL que le client et le serveur choisissent les différents systèmes qu’ils utiliseront tout au long de leur communication.

Avec le protocole SSL, la sécurité a été sensiblement améliorée. Bien que, comme tout système de chiffrement, le SSL/TLS ne pourra jamais être totalement infaillible, le grand nombre de banques et de sites de commerce électronique l'utilisant pour protéger les transactions de leurs clients peut être considéré comme un gage de sa résistance aux attaques malveillantes. Il faut noter cependant que SSL ne garantit que le transport sécurisé des messages.

SSL est un protocole indépendant qui peut être appliqué à plusieurs autres protocoles. Son utilisation la plus connue est son association avec le protocole HTTP connue comme le protocole HTTPS pour dire, chez certain HTTP over SSL et pour d’autres HTTP Secure. Il a en outre d’autres applications telles que le SSH permettant la connexion à une machine distante et le FTPS permettant le transfert de fichiers.

**Aujourd’hui**

Compte tenu de leur rôle essentiel dans nos sociétés et nos économies modernes, les ordinateurs, les téléphones mobiles et l'internet doivent fonctionner ensemble correctement tout en fournissant un cadre qui protègent tout un chacun.

Il faut donc adopter des mesures drastiques afin d’assurer la sécurité lors de nos interactions avec ces différents outils qui font partie aujourd’hui de notre quotidien. Ces mesures sont prises sur deux aspects :

* l’aspect juridique : de nouvelles lois sont adoptées
* l’aspect technique : des services de protection des données sont créés aux échelles nationale, sous régionale et internationale

Aspect juridique

Dans le cadre juridique, on parle le plus souvent de données à caractère personnel ou données personnelles. La notion de données à caractère personnel est définie comme étant toute information relative à une personne physique identifiée, génétique, psychique ou identifiable directement ou indirectement, par référence à un numéro d’identification ou à un ou plusieurs éléments propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique [1].

Les premières législations sur la protection des données personnelles [1] ont été adoptées en Allemagne (1971), en Suède (1973), en France (1978), au Luxembourg (1979) et au Canada (1979). [2]

En Afrique, la protection des données à caractère personnel est promue par plusieurs organismes communautaires même si les lois sur la protection des données sont relativement récentes. Le tableau suivant [1] décrit l’ordre d’adoption des lois par pays :

|  |  |
| --- | --- |
| Pays | Année |
| Seychelles | 1988 |
| Cap-Vert | 2001 |
| Zimbabwe | 2002 |
| Burkina Faso ; Tunisie ; Iles Maurice | 2004 |
| Sénégal | 2008 |
| Bénin ; Maroc | 2009 |
| Ghana | 2010 |
| Gabon ; Angola | 2011 |
| Mali ; Côte d’Ivoire ; Afrique du Sud ; Lesotho | 2013 |
| Madagascar ; Comores | 2014 |
| Tchad | 2015 |
| Guinée Equatoriale | 2016 |
| Niger | 2017 |

En Afrique de l’Ouest, la CEDEAO et l’UEMOA sont intervenus en tant qu’acteur régional dans la réglementation des données personnelles en adoptant des mesures juridiques tout comme l’Union Africaine au niveau continental.

Au Sénégal, nous avons la loi n° 2008-11 du 25 Janvier 2008 portant loi d’orientation relative à la société de l’information qui définit un cadre général pour adapter le droit sénégalais aux besoins de la société de l’information.

Nous avons aussi la loi n° 2008-11 du 25 Janvier 2008 portant sur la cybercriminalité .La cybercriminalité ou criminalité informatique concerne toute infraction qui implique l’utilisation des technologies de l'information et de la communication.

Nous avons aussi la loi sur les transactions électroniques qui vise, de façon globale, à favoriser le développement du commerce par les Technologies de l’Information et de la Communication (TIC) en posant des règles précises [1].

Il y a surtout la loi n° 2008-12 du 25 Janvier 2008 sur la protection des données à caractère personnel qui est le principal corpus protecteur desdites données.

Ce cadre juridique définit des exigences de sécurité que doivent respecter les responsables des traitements des données à caractère personnel. Elles imposent à ces derniers des obligations de confidentialité, de sécurité, de conservation et de pérennité des données.

En effet, tout responsable de traitement de données personnelles se doit de mettre en œuvre les mesures techniques et organisationnelles adéquates pour protéger les données collectées contre la destruction accidentelle ou illicite, la perte, l’altération, la diffusion ou l’accès non autorisé notamment lorsque le traitement comporte des transmissions des données dans un réseau, ce qui est presque toujours le cas, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et la nature des données manipulées, empêchant le tiers de procéder à leur modification, à leur altération ou à leur consultation sans autorisation.

Cette obligation se traduit donc par la nécessité de mettre en œuvre des mesures de sécurité physique (verrous des salles serveur, coffres forts, etc.) et des mesures de sécurité logique (contrôles d’accès, cryptage des données, etc.). L’article 71 de la loi sur la protection des données à caractère personnel stipule que :

Le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et, notamment, pour empêcher qu’elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Il prend, en particulier, toute mesure visant à :

* garantir que, pour l’utilisation d’un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu’aux données à caractère personnel relevant de leur compétence ;
* garantir que puisse être vérifiée et constatée l’identité des tiers auxquels des données à caractère personnel peuvent être transmises ;
* garantir que puisse être vérifiée et constatée à posteriori l’identité des personnes ayant eu accès au système d’information et quelles données ont été lues ou introduites dans le système, à quel moment et par quelle personne ;
* empêcher toute personne non autorisée d’accéder aux locaux et aux équipements utilisés pour le traitement des données ;
* empêcher que des supports de données puissent être lus, copiés, modifiés, détruits ou déplacés par une personne non autorisée ;
* empêcher l’introduction non autorisée de toute donnée dans le système d’information ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées ;
* empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l’aide d’installations de transmission de données ;
* empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée ;
* sauvegarder les données par la constitution de copies de sécurité ;
* rafraîchir et si nécessaire convertir les données pour un stockage pérenne.

Au Sénégal, le fait de procéder à des traitements automatisés de données personnelles sans prendre toutes les précautions utiles pour préserver leur sécurité est passible d’une peine d’emprisonnement de 1 à 7 ans et d’une amende allant de 500 000 à 10 000 000 de francs CFA.

Pour assurer le respect des règles juridiques quant à la protection des données personnelles, il est institué par les différentes lois, un organisme responsable. Au Sénégal, c’est la CDP (Commission des Données Personnelles) qui joue ce rôle.

Aspect technique

Les applications Web ont fait de l'Internet un objet vivant et respirant mais l’ont par contre ouvert à une manne de hacking. L'injection SQL a été découverte en 1998, et les techniques d'injection sont rapidement devenues la méthode de piratage la plus utilisée à mesure que les applications Web gagnaient en popularité. Pour aider à combattre l'augmentation du piratage, les outils de sécurité ont évolué de simples outils d’analyses de fichiers source uniques à des outils d’analyse de code sources

De partout dans le monde, des CERT sont mis en place pour prendre en compte les incidents susceptibles de se produire sur Internet. Un CERT est un Centre d’alerte et de réaction aux attaques informatiques ciblant les entreprises ou administrations mais dont les informations sont généralement accessibles à tous. Le premier CERT (CERT-CC) a été créé aux Etats-Unis à l’Université Carnegie-Mellon en réponse à l’attaque du ver Morris/

Le but des CERT est de répondre aux incidents de sécurité informatique, de coordonner la communication entre experts lors de ces incidents de sécurité, de signaler les vulnérabilités et promouvoir des pratiques de sécurité efficaces dans toute la communauté internet afin de prévenir les incidents futurs.

Dans presque tous les pays développés, nous avons au moins un CERT national. En France on a le CERT-FR, en Belgique, le CERT.BE, au Danemarque, le DKCERT, en Allemagne, le CERTBund, au Japon, le JPCERT, au Royaume-Uni, l’UKCERT, au Canada, le CanCERT, pour ne se limiter qu’à ceux-là.

En Afrique, des efforts ont été récemment faits dans ce domaine même s’il faudrait que plus de pays africains mettent en place des CERT. Nous avons le CSIRT du Kenya, le CERT des îles Maurice, l’ECS-CSIRT de l’Afrique du Sud, le TunCERT de la Tunisie, le CI-CERT de la Cote d’Ivoire, le CERT-GH du Ghana, le DZ-CERT de l’Algérie ou encore le maCERT du Maroc. Nous avons aussi le Forum africain des équipes de réponse aux incidents informatiques (AfricaCERT) qui veut asseoir les bases d’une coopération dynamique entre les équipes nationales africaines de CERT pour lutter contre le phénomène de la cybercriminalité qui menace l’économie, l’image et la jeunesse africaines.

Les CERT à travers le monde sont des entités indépendantes, bien qu'il puisse y avoir des activités coordonnées entre les groupes. Ces dernières années, de nombreux CERT ont vu le jour et font partie du Forum des équipes de réaction aux incidents de sécurité informatique (FIRST), dont le CERT/CC de la DARPA est un membre fondateur. FIRST est une organisation de premier plan et un leader mondial reconnu dans la réponse aux incidents de sécurité informatique. L'appartenance à FIRST permet aux CERTs d'intervenir plus efficacement face aux incidents de sécurité en fournissant un accès aux meilleures pratiques de sécurité, à des outils de gestion de la sécurité et à une communication de confiance entre les équipes membres. Il s'agit d'une confédération internationale de CERTs de confiance qui gèrent de manière coopérative les incidents de sécurité informatique et favorisent les programmes de prévention des incidents. Ils travaillent tous pour un objectif commun de sécurité informatique. En outre, de nombreuses sociétés privées de d’édition de logiciels anti-virus ont des divisions qui jouent le rôle de CERT.

Mise en place de services techniques gouvernementaux chargés de la question de la sécurité des infrastructures des états mais aussi des entreprises publiques et privées. En France, on a d’abord la DSSI puis l’ANSSI.

Il existe aussi en plus des CERTS, des autorités techniques nationales, sous-régionales et régionales chargées de préserver la sécurité de l’information aux niveaux nationales, sous-régionales et régionales. En France, nous avons l’ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information) créée en 2009 et qui succède à la DCSSI (Direction Centrale de la Sécurité des Systèmes d’Information) créée dès 2001. L’enjeu de ces autorités nationales est de préserver la souveraineté et l’autonomie de décision et d’action dans le domaine informatique et protéger l’ensemble des infrastructures critiques.

Au niveau européen, il existe l’EICAR fondée en 1990, qui a pour objectif la recherche en virologie informatique et l'amélioration du développement des logiciels antivirus. Il y a aussi l’Enisa (European Union Agency for Network and Information Security) dont la vocation est de « développer une culture de la sécurité des réseaux d'information dans toute l'Union » [1]. Il existe d’autre agences au niveau de l’Union européenne, qui, faut le dire accorde une très grande importance aux questions de la sécurité des systèmes d’information.

En parallèle à ces initiatives étatiques, il existe des organisations indépendantes sans but lucratif qui œuvrent pour une meilleure sécurité de l’information. Parmi celles-ci, les plus connues sont Mitre, Sans Institute et Owasp.

Mitre Corporation :

* Organisation à but non lucratif travaillant dans l’intérêt public fondé en 1958
* Gère les centres de recherche et de développement financés par l’état fédéral (FFRDCS) notamment celui du Département de la Défense ce même département chargée de la sécurité nationale aux Etats Unis dont la sécurité informatique
* Les FFRDCS fournissent des services dans les domaines de l'acquisition et de l'analyse de systèmes notamment sur la cyber-sécurité et la mise en réseau mondiale.
* Ses FFRDC s'engagent également dans la recherche et le développement de technologies telles que la biosécurité et l'informatique quantique
* Cyber académie : cours en ligne
* Maintient la liste des CVE avec le sponsoring du Département de la Sécurité Intérieure, la liste CCE, la liste CAPEC et la liste CWE
* Partenaire très proche du gouvernement fédéral

Sans Institute

* Organisation privée à but lucratif qui offre des formations et des certifications en sécurité de l'information et en cyber sécurité à travers le monde fondée en 1989
* Maintient le plus grand référentiel d'informations sur la sécurité dans le monde et est également le plus grand organisme de certification.
* Fournit une vaste collection de documents de recherche sur la sécurité et supervise un système d’alerte d’attaques : Internet Storm Center
* Son programme GIAC (Global Information Assurance Certification) fournit un moyen normalisé de garantir les connaissances et les compétences d'un professionnel de la sécurité

Many of the valuable SANS resources are free to all who ask. They include the very popular [Internet Storm Center](https://isc.sans.edu/) (the Internet's early warning system), the weekly news digest ([NewsBites](https://www.sans.org/newsletters/newsbites/)), the weekly vulnerability digest ([@RISK](https://www.sans.org/newsletters/risk/)), and more than 1,200 award-winning, original [information security research papers](https://www.sans.org/reading_room/).

* [SANS Information Security Reading Room](https://www.sans.org/reading_room/)- More than 2770 original research papers in 106 important categories of security
* [SANS Weekly Bulletins and Alerts](https://www.sans.org/newsletters/)- Definitive updates on security news and vulnerabilities
* [SANS Security Policy Project](https://www.sans.org/resources/policies/)- Free Security Policy Templates - Proven in the real world
* [Vendor Related Resources](https://www.sans.org/vendor/)- Highlighting the vendors that can help make security more effective
* [Information Security Glossary](https://www.sans.org/resources/glossary.php)- Words, acronyms, more
* [Internet Storm Center](https://isc.sans.org/)- The Internet's Early Warning System
* [S.C.O.R.E.](https://www.sans.org/score/)- Helping the security community reach agreement on how to secure common software and systems
* [CIS Critical Security Controls](https://www.sans.org/critical-security-controls/)- A consensus ranking of the security controls that are the most effectiveness in reducing risk from real world attacks.
* [SANS Press Room](https://www.sans.org/press/)- Our press room is designed to assist the media in coverage of the information assurance industry

PCI Standard Council :

* Fondée en 2006 par American Express, Discover, JCB International, MasterCard et Visa Inc.
* Recommande, maintient et évolue des normes pour la sécurité des données des titulaires de cartes dans l'industrie des cartes de paiement à travers le monde.
* Les normes PCI Data Security aident à protéger la sécurité des données de carte de paiement bancaires. Ils définissent les exigences opérationnelles et techniques pour les organisations acceptant ou traitant des transactions de paiement, et pour les développeurs de logiciels et les fabricants d'applications et de dispositifs utilisés dans ces transactions
* Les normes : Data Security Standards (PCI-DSS), PIN Transaction Security Requirements (PCI-PTS), Payment Application Data Security Standard (PCI-PA-DSS), P2P Encryption
* Bien que la norme PCI DSS doive être appliquée dans toutes les entreprises acceptant ou traitant des transactions de paiement, la validation formelle de cette norme n’est pas obligatoire dans toutes les organisations.
* PCI DSS constituée de 12 points organisés en 6 catégories
* Visa et MasterCard demandent aux commerçants et fournisseurs de services d’être en conformité avec la norme. Les plus petites entités n’en ont pas l'obligation, mais doivent cependant mettre en œuvre tous les contrôles nécessaires afin d'éviter d'engager leur responsabilité dans le cas où une fraude, associée à un vol des données de titulaires de cartes aurait lieu.

Web Application Security Consortium (WASC):

The Web Application Security Consortium (WASC) is a worldwide organization devoted to the establishment, refinement and promotion of Internet security standards. The consortium, which was founded in January 2004, consists of independent members as well as those associated with corporations, government agencies and academic institutions.

The WASC's mandate includes researching, discussing, and publishing information about Web application security issues. The organization educatesh individuals and enterprises about such issues and the countermeasures that can be taken against specific threats, and acting as an advocate for users of the Internet, and in particular, for individuals and organizations devoted to Web application security. The WASC is vendor-neutral, although members may belong to corporations involved in the research, development, design, and distribution of Web security related products.

The Web Application Security Consortium (WASC) is 501c3 non profit made up of an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best-practice security standards for the World Wide Web.

As an active community, WASC facilitates the exchange of ideas and organizes several industry projects. WASC consistently releases technical information, contributed articles, security guidelines, and other useful documentation. Businesses, educational institutions, governments, application developers, security professionals, and software vendors all over the world utilize our materials to assist with the challenges presented by web application security.

Volunteering to participate in WASC related activities is free and open to all.x