Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 2, No. 3, Mai 2024

L'ÉTENDUE DE LA PROTECTION PÉNALE DES SYSTÈMES DE TRAITEMENT AUTOMATISÉ DES DONNÉES

THE EXTENT OF CRIMINAL PROTECTION FOR AUTOMATED DATA PROCESSING SYSTEMS

ADNANI El Mehdi

Doctorant chercheur en sciences juridique. Faculté des sciences juridiques et politique de Settat- Université Hassan Premier, Settat/ Maroc.

Pr. AKKOUR Soumaya

Professeure à la faculté des sciences juridiques et politiques de Settat- Coordinatrice du master Droit Du Numérique. Université Hassan premier- Settat-Maroc / Laboratoire De Recherche En Dynamiques Sécuritaires.

Résumé : La protection des données dans un système implique de prendre des mesures pour s'assurer que les informations sensibles et personnelles sont protégées contre l'accès non autorisé, la perte, la fuite ou la destruction. Les systèmes peuvent inclure des bases de données informatiques, des réseaux de stockage de données, des systèmes de gestion de la confidentialité, etc.

Les mesures de protection des données peuvent inclure l'authentification, l'autorisation, la cryptographie, la sauvegarde de données, la gestion des accès et les contrôles de sécurité. Il est également important de former les employés sur les bonnes pratiques en matière de protection des données et de s'assurer que les politiques et les procédures sont mises en place pour protéger les données.Il est important de noter que la protection des données est une responsabilité en constante évolution en raison de l'évolution constante des technologies et des menaces de sécurité. Il est donc important de surveiller régulièrement les systèmes pour détecter les vulnérabilités et mettre en place des mises à jour pour renforcer la sécurité des données.En général, la protection des données dans un système est un élément crucial pour garantir la sécurité et la confidentialité des informations sensibles et personnelles, ainsi que pour maintenir la confiance des utilisateurs dans le système.

Mots clés :Protection ; Traitement ; Donnés personnelles ; Pénal ; Système.

Abstract:Data protection in a system involves taking measures to ensure that sensitive and personal information is safeguarded against unauthorized access, loss, leakage, or destruction. Systems can include computer databases, data storage networks, privacy management systems, etc.

Data protection measures can include authentication, authorization, cryptography, data backup, access management, and security controls. It is also important to train employees on best practices for data protection and ensure that policies and procedures are in place to protect the data.

It is important to note that data protection is a constantly evolving responsibility due to the continuous development of technologies and security threats. Therefore, it is crucial to regularly monitor systems to detect vulnerabilities and implement updates to enhance data security.In general, data protection in a system is a crucial element to ensure the security and confidentiality of sensitive and personal information, as well as to maintain user trust in the system.

Keywords: Protection; Processing; Personal Data; Criminal; System.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.11546148

1 Introduction

Suite à la deuxième guerre mondiale, une révolution des technologies d'information et particulièrement de communication, a vu le jour. On parle concrètement des innovations technologiques et informatiques, c'était et encore un champ dynamique dans lequel chaque nation défie l'autre. Et cela en raison des bienfaits de l'informatique sur la vie Humaine dans les différents secteurs et pour chaque entité de la société. Les nouvelles technologies, notamment l'informatique ont une immense importance dans le secteur public que dans le secteur privé. Cette importance ne cesse d'augmenter et elle a pris un autre souffle avec l'arrivée de l'internet qui peut être définie comme étant un réseau informatique d'ordre mondiale destiné pour l'échange d'information.
Nonobstant, des avantages importés par les outils numériques qui font l'accélération d'une tendance qui ne s'interdite aucune limite ni aucun domaine, a entrainé des effets de plus en plus visibles sur sa traduction dans le monde de droit.Cette révolution technologique a donné la vie à une société d'existence virtuelle qui existe en parallèle avec la société traditionnelle. Qui est devenue une scène de nouvelles formes de criminalité, portant les traits caractéristiques de l'environnement dont elles émanent. Elle a pris plusieurs dénominations selon la nature de l'atteinte et selon le procédé exploité lors du passage à l'acte. à ce point Sutherland soutient que les délinquants forment des systèmes de délinquance qui sont destinés à augmenter leurs bénéfices tout en minimisant leurs risques. Ainsi Les délinquants partageraient entre eux leurs meilleures pratiques, mais aussi leurs techniques pour se défendre lorsque leurs activités seraient perturbées par les forces policières. On parle ici de la délinquance informatique.Quant à sa définition et d'où une observation externe. C'est une expression constituée par un amalgame de deux variables d'une part le terme délinquance qui désigne selon le dictionnaire Larousse l'ensemble des infractions commises en un temps et en un lieu donné. D'autre part le terme informatique consiste en la « Science du traitement rationnel et automatique de l'information ; l'ensemble des applications de cette science ». L'information est la matière traitée par les ordinateurs. Ils doivent donc être capables de la « comprendre », tout comme l'Homme comprend une langue et des concepts. L'informatique ainsi est la science du traitement de l'information.Alors cette forme de délinquance, regroupe toutes les infractions pénales tentées ou commises à l'encontre ou par moyen d'un système d'information et de communication. Et quant à la définition de la délinquance informatique on peut la définir comme l'ensemble des agissements, conduites ou actes incriminés par la loi pénale et sanctionnés par elle. Qui portent atteinte à une personne, a un bien ou une valeur, dont l'outil informatique fait partie.Dans les deux cas et grâce aux technologies, la commission de l'infraction se fait à distance et de façon anonyme. Elle peut être le fait d'un individu seul, ou bénéficiant du soutien d'un réseau technique et informationnel étendu ou agissant dans le cadre d'une bande organisée géographiquement éclatée ».

La notion de la délinquance informatique se distingue par rapport d'autres concepts qui sont semblables aux yeux des profanes mais ne se confondes pas avec elle dans ceux des juristes.
À savoir la cybercriminalité, c'est une notion reste délicate, elle est définie comme « tout comportement illégale ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmission de données ».
Nonobstant, que cette définition venant d'une perspective morale et éthique qui répond aux bonnes pratiques de l'utilisation des outils informatiques. Elle permettre de distinguer la cybercriminalité de la criminalité informatique, du fait que la dernière désigne l'ensemble des infractions contre un système informatique ou contre son contenu. Cependant la cybercriminalité exige que lesdites infractions consommées ou tentées à cause de l'interconnexion de ce système, ont un réseau, en l'occurrence l'internet. C'est une criminalité qui est toujours en lésant avec le cyberespace.

En effet, « la cybercriminalité inclut non seulement les infractions informatiques mais aussi les infractions facilitées par le recours à Internet qui deviennent plus sophistiquées, élaborées et occultes et donc complexes à caractériser ».La connaissance de la délinquance informatique demeure très difficile en raison de son hétérogénéité. Au vu de certaines études effectuées, la délinquance informatique se diffère de la délinquance classique, car elle « se compose de délinquants spécialisés jeunes par hypothèse, considérés comme employés modèles occupant un poste de confiance dans la direction d'une entreprise. Généralement motivés par le caractère du jeu et du défi qu'apporte l'idée de tromper l'ordinateur », (Quéméner, Myriam, op. Cit. p83.)

Face à la délinquance informatique, chaque pays tente d'avoir son arsenal juridique et sa politique de cyberdéfense, par des efforts sur l'échelle nationale et internationale.

La délinquance informatique est devenue un fléau mondial qui exige la cohérence des efforts des différents intervenants, à cause de son caractère transversale. Le Maroc s'est engagé dans la lutte contre la cybercriminalité qui inclue la délinquance informatique, et cela par la signature de la convention de la lutte contre la cybercriminalité adoptée à Budapest en novembre 2001.

La protection juridique des données personnelles peut être renforcée en protégeant les systèmes de traitement automatisé des données. Cela peut inclure la conformité aux réglementations en matière de protection des données telles que le RGPD en Europe, le CCPA en Californie et le LGPD au Brésil. Les entreprises doivent également mettre en place des politiques et des procédures pour garantir la confidentialité et la sécurité des données personnelles et veiller à ce que les employés soient formés sur les meilleures pratiques de protection des données. En cas de violation de la vie privée, les titulaires de données peuvent intenter une action en justice pour réclamer des dommages et intérêts.

La législation marocaine a l'instar des autres législations à instaurer un faisceau de dispositions légales, en vue d'appréhender la délinquance informatique, et pour combler le vide juridique qui était jusqu'à 2003. Notamment avec la promulgation de la loi 07-03 qui a importée des dispositions réprimant les atteintes relatives aux systèmes de traitement automatisé de données[1].Cette loi constitue une transposition des certaines dispositions de la convention susmentionnée.

Par la suit et toujours dans la même perspective une loi pour la protection des personnes physiques à l'égard du traitement des données à caractère personnel, c'est la loi 09-08[2] Qui constitue une base juridique pour la protection des données à caractère personnel, cela s'inscrit dans une optique de la protection de la vie privée contre les atteintes venantes de toute utilisation abusive de données personnelles, qui trouvent elles-mêmes sa consécration dans la constitution marocaine de 2011[3]. On ajoute aussi la loi 103-13[4].

En outre le législateur pour besoin de sécuriser les contrats conclus par voie électronique, une loi a cette fin a vu le jour. C'est la loi 53-05[5] .

Le régime juridique marocain en 2003, été renforcé par la loi 07-03 susmentionnée dans l'introduction c'est presque la transposition de La loi française du 5janvier 1988 (dite loi Godfrain), a été incorporée avec des additions dans le Code pénal. La loi a construit un corps particulier de règles visant à incriminées les atteintes aux systèmes de traitement automatisés de données (STAD) c'est la

[1]Loi n° 07-03 promulguée par le dahir n° 1-03-197 du 11 novembre 2003 – 16 ramadan 1424 modifiant et complétant le Code pénal. Bulletin officiel numéro 5184 du 05.02.2004, Date de publication : 11.11.2003.

[2]BULLETIN OFFICIEL N° 5714 -7 Rabii I 1430 (5-3-2009), Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

[3]Article 24 de la constitution Marocaine de 2011 « Toute personne à droit à la protection de sa vie privée… »

[4]Dahir n° 1-18-19 du 5 Joumada II 1439 (22 février 2018) portant promulgation de la loi n° 103-13 relative à la lutte contre les violences faites aux femmes

[5] Dahir numéro 1-07-129 du 19 Kaada 1429 (30 Septembre 2007) portant promulgation de la loi numéro 53-05 relative a l'échange électronique de données juridiques. Bulletin officiel numéro 5584-25 Kaada 1428 (6-12-20017).

criminalité informatique proprement dite. Cette loi a fait référence àla notion du système de traitement automatisé de données, qui se coïncide avec la notion technique du système informatique, pour plus de précisions, on prend la définition donnée a cette notion par le Sénat : « tous ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciels, de données, d'organes d'entrées-sorties, et liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité ».
En effet, tout ensemble informatique, quel que soit sa taille, son mode de liaison avec d'autres ou entre ses composants via le Protocol de communication, et son mode de traitement a vocation de constituer un système informatique.

Quant à la notion du traitement, consiste en « tous ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble Introduction d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives ».
L'intérêt de notre sujet revêt deux images, l'une est abstraite réside dans les efforts s'employés par le législateur en vue d'instaurer une protection pénale des données personnelles a travers les textes incriminant les atteintes aux systèmes de traitement automatise de données.
Toutefois, son image concrète se manifeste par l'ensemble des contraintes qui freinent l'arrivée aux objectifs prédéfinis. Et à cause de l'évolution continue de la délinquance informatique d'où l'enivrement dont- elle relève, et des techniques et pratiques employées et de l'esprit criminel.
D'où cette perspective naisse la problématique de savoir comment le législateur marocain protège les données personnelles à travers la protection du système informatique de traitement automatise
D'âpres la lecture de la loi numéro 07-03, on constate qu'il ya des actes portant atteinte à l'intégrité du STAD, et autres offensent le contenu du STAD[6].

2 Les atteintes à l'intégrité du STAD

On premier lieu on trouve l'intrusion dans un système qui se manifestent soit par un l'accès ou le maintien frauduleux. Et en seconde lieu on va présenter l'influence de ses agissements sur le fonctionnement du STAD.

2.1 L'intrusion

A ce niveau en distingue entre l'accès et le maintien frauduleux, chacun d'eux soumis à une qualification autonome.

- **L'accès frauduleux**

L'article 607-3 Alenia1 du code pénal marocain dispose que : « le fait d'accéder frauduleusement dans tout ou partie d'un système de traitement automatisé de données… ».
La notion d'accès dans un STAD, indiquée par ledit article, au sens large peut être caractérisée soit par la pénétration dans un système, soit par une manipulation informatique ou autre manœuvre, par le biais d'une connexion ou d'appel d'un programme, opérée de manière frauduleuse, c'est à dire sans autorisation de l'entreprise.

D'âpres l'article mentionné, il découle que l'accès dans un STAD est un délit qui incrimine l'atteinte à l'intégrité du système lui-même est constitué indépendamment de tout préjudice ou de tout résultat au niveau des données contenues dans ce système. Il n'est donc pas nécessaire que le délinquant capte des données. Le délit suppose seulement un accès dans le système de traitement automatisé de données « une intrusion dans l'espace», avec une maitrise des outils de commandement, peu importe le mobile de l'accès frauduleux, et notamment la volonté de mettre à jour les failles de sites gouvernementaux.

[6]Système de Traitement Automatisé de Données.

L'accès frauduleux à un STAD concerne souvent l'entreprise, la concurrence déloyale ou l'espionnage industriel. L'insertion d'un cheval de Troie ou le recours à un keyloggeur[7] dans un système caractérise l'accès frauduleux à un système de traitement automatisé de données. L'infraction est constituée dès lors qu'une personne ou une entité non autorisée accède dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation. Et dans le même ordre d'idée "L'absence de droit résulte de l'absence d'autorisation expresse du maître de système" (CA Toulouse, 3ème Chambre, 21 janvier 1999).

L'incrimination de l'article 607-3 Alenia1, est de portée large notamment elle englobe toutes les techniques d'accès frauduleux à un système et telle que l'utilisation d'un code d'accès exact par une personne non habilitée à accéder à un STAD.
Âpres importé des éclaircissements au délit d'accès frauduleux, on va mettre l'accent sur l'infraction du maintien indu dans un STAD.

2.2 Le maintien dans un STAD

Le maintien frauduleux dans un STAD, constitue le deuxième acte incriminé par l'article 607-3 du code pénal marocain, notamment par son Alenia 2 dispose que : « est passible de la même peine toute personne qui se maintient dans tout ou partie d'un STAD auquel elle à accéder par erreur et alors qu'elle n'a pas le droit ».
Il découle de ces dispositions que nous somme devant deux hypothèses : on peut s'y introduire sans autorisation ou après avoir obtenu une autorisation d'accès, ne pas le quitter une fois le temps de connexion accordé s'est écoulé.

Pour la première hypothèse, notamment dans le cas où une personne bénéficie d'une autorisation limitée soit dans le temps ou dans l'espace. L'exemple type d'une entité autorisée d'accéder dans un système mais seulement dans une partie déterminée du système, comme l'autorisation d'accéder seulement à un forum paganisé sur un site web, toutefois l'entité qui bénéficie de cette habilitation a fait une immixtion dans l'espace administration de ce site web. On parle ici d'un maintien non autorisé dans l'espace.
A cotée, il peut qu'une personne, bénéficie d'un agrément d'accès dans un système mais seulement durant une période déterminée, comme l'informaticien autorisé pour entrer dans un système informatique mais seulement pour la période d'essai alors qu'il continu à exploiter cette permission nonobstant la maturité du système. On parle ici d'un maintien non autorisé dans le temps.
Il est clair là-dessus qu'il est possible d'appliquer la théorie d'abus de droit consacrée par l'article 94 du DOC et par plusieurs textes, chaque fois qu'il y'a un excès d'autorisation par la personne concernée, pour obtenir réparation au profit de la personne lésée.

[7]Par un arrêt du 16 janvier 2018, la chambre criminelle a estimé que se rend coupable de l'infraction prévue à l'article 323-1 du Code pénal la personne qui, sachant qu'elle n'y est pas autorisée, accède à l'insu des victimes, en l'espèce via un keylogger, à un système de traitement automatisé de données (STAD). la cour d'appel avait, pour dire établis les délits d'accès frauduleux à tout ou partie d'un système de traitement automatisé de données, d'atteinte au secret des correspondances émises par voie électronique et de détention sans motif légitime d'équipement, d'instrument de programme ou données conçus ou adaptés pour une atteinte au fonctionnement d'un système de traitement automatisé, retenu que la détention d' un keylogger, sans motif légitime, par M. Q., que celui-ci ne conteste pas avoir installé sur l'ordinateur de docteurs, pour intercepter à leur insu, par l'espionnage de la frappe du clavier les codes d'accès et accéder aux courriels échangés par les praticiens caractérisaient suffisamment sa mauvaise foi et les délits tant dans leur élément matériel qu'intentionnel. Les juges ajoutaient que les motifs avancés par le prévenu pour justifier la détention d'un équipement conçu ou adapté pour une atteinte frauduleuse à un système de traitement automatisé de données, à savoir la défense de sa situation professionnelle et sa réputation, étaient indifférents à la caractérisation des infractions, puisque l'autorisation de détention prévue par l'article 323-3-1 du Code pénal permettant la possession d 'un tel équipement, se limite aux seules personnes habilitées à assurer la maintenance et la sécurité d'un parc informatique (Cass. crim., 16 janv.2018, nº 16-87168). est un arrêt a titre d'exemple motionné par : Quéméner, Myriam, Le droit face à la disruption numérique : Adaptation des droits classiques - Émergence de nouveaux droits, préciteP99.

La deuxième hypothèse, c'est celle que l'on considère plus grave que la première, en raison des circonstances qu'elle présente. On parle ici d'une présence indue dans un STAD, précédée par un accès frauduleux. Et cela constitue pour le juge une circonstance aggravante de la sanction, d'ordre judicaire. Et par la relecture de l'article 607-3 Alenia2, il est avéré que le législateur sanctionne même le maintien par erreur, dès que l'entité dépourvue du droit de maintenir et par présomption d'accéder dans le système en tout ou en partie.
A partir de cette disposition, la protection conférée aux STAD, par notre législateur ne donne aucune considération (d'âpres notre modeste lecture de ce texte) à la bonne foi du chef d'un maintien. Il est imaginaire qu'on peut avoir un accès et un maintien, par une simple touche sur l'écran de notre portable, et cela porte atteinte aux droits des innocents.
Toutefois c'est une arme efficace pour que l'auteur des délits incriminés par ces dispositions ne s'échappe pas de la sanction par ce prétexte.
À la lumière de ce qu'il précède, L'incrimination d'accès ou du maintien frauduleux dans un système de traitement automatisé de données suppose la réunion d'une condition préalable et de deux éléments constitutifs :

– une condition préalable : l'existence d'un système de traitement automatisé de données ;
– un élément matériel : un accès ou un maintien dans un système automatisé de données ;
– un élément moral : une intention frauduleuse, c'est l'acte d'accès ou du maintien sans habilitation à ce propos.

Quant au terme « frauduleux" suppose que l'intrusion et le maintien aient été volontaires et que leur auteur ait eu conscience de commettre une action ou une omission illicite. Mais, il n'est pas nécessaire pour autant que le délinquant ait eu l'intention de nuire.
Quant à la jurisprudence française, La simple utilisation de l'ordinateur et de l'abonnement Internet d'autrui a été qualifiée d'accès frauduleux : ainsi, le 24 mai 2006, le chef de l'équipe de nettoyage de la cour d'appel de Montpellier a été reconnu par cette même cour coupable d'accès frauduleux dans un STAD pour avoir utilisé les ordinateurs de la cour d'appel pendant ses horaires de travail pour se connecter à des sites web à caractère pornographique. Le STAD pouvant également être constitué d'un réseau d'informatique ou de télécommunications, une écoute passive peut elle aussi être considérée comme un accès, qu'elle soit réalisée par espionnage des artères de transmission ou par captation des signaux parasites émis par le circuit électrique.
Quant au « maintien », il a été jugé qu'il peut succéder à un accès licite : la cour d'appel de Paris a ainsi indiqué le 5 avril 1994 que même si « l'accès a été régulier, le maintien sur un STAD peut devenir frauduleux […], que l'accès ou le main- tien irrégulier suppose que leur auteur n'a pas respecté la "règle du jeu", que celle-ci procède de la loi, du contrat ou de la volonté du "maître du système" ». Cela interdit donc, après un accès autorisé, de se maintenir abusivement connecté.

De même, la Cour de cassation a validé le 10 mai 2015 la condamnation à 2 000 euros d'amende d'un avocat qui, administrateur réseau de son cabinet, avait installé un logiciel espion sur l'ordinateur de son associée et épouse, avec laquelle il était en cours de divorce, afin d'obtenir des informations sur ses relations extraconjugales : même si un tel logiciel peut légitimement être installé à des fins de sécurité informatique, l'exploitation de cet outil à des fins étrangères au contrôle du bon fonctionnement du réseau caractérise le délit de maintien frauduleux. Pour le juge pénal, l'élément intentionnel est primordial : la fraude est constituée dès que le délinquant a conscience que l'accès n'est pas autorisé et qu'il agit contre le gré du maître du système, même s'il n'y a pas de sécurisation, et à plus forte raison s'il y en a une. Le mobile (qui peut être désintéressé) n'est pas pris en compte, comme le montreront les jurisprudences. L'éventuelle modification des données, suite à l'accès frauduleux, constitue une circonstance aggravante de l'infraction[8].

[8]L'accès non autorisé est pénalement condamnable, même s'il n'y a pas intention de nuire et même s'il n'y a eu aucune conséquence dommageable pour le système. La cour d'appel de Paris a ainsi condamné le 15 mai 2001 un prévenu qui avait pénétré dans le système informatique d'une université grâce à un logiciel de piratage, sans provoquer aucune modification des données ni aucune altération du système. De même, le tribunal de grande instance de Vannes a condamné le 13 juillet 2005 quatre étudiants qui avaient utilisé des logiciels de piratage des

Âpres mettre l'accent sur ces agissements[9], on passe aux conséquences qu'ils engendrent sur le système, à savoir les atteintes au fonctionnement du système soit par le faussement ou par l'entrave. Qui constituent des délits autonomes par rapport aux précédents. Concrètement sont l'influence ou l'effet d'accès et/ou du maintien frauduleux dans un STAD.

2.3 Les atteintes au fonctionnement d'un STAD

L'article 607-3 Alenia3, incrimine des actes portants atteints au fonctionnement du STAD. D'abord, on donne des éclaircissements quant au concept du « fonctionnement » du système à la lumière de la définition du système informatique déjà citée, qui implique la synergie dynamique de ses composants pour atteindre un résultat défini. En effet toute mise en échec de la réalisation de ce résultat, soit totale ou partielle constitue une atteinte au fonctionnement du STAD, de même le fait d'orienter le système pour un objectif autre que celui pour lequel il est destiné.

Selon les termes de cet article l'atteinte au fonctionnement du STAD constitue une infraction autonome par rapport à celle d'accès ou du maintien frauduleux dans le système de traitement automatisé de données. Cependant, elle est souvent commise à la suite d'un accès et/ ou d'un maintien frauduleux. L'atteinte au fonctionnement d'un STAD concrètement constitue une intrusion avec influence sur l'intégrité du système. Et cela peut prendre plusieurs formes à savoir :

3 L'entrave au fonctionnement d'un STAD

L'article 607-5 dispose que : « le fait de fausser ou d'entraver intentionnées le fonctionnement d'un STAD… »
On peut dire que l'entrave au fonctionnement du système, consiste en la ou les manœuvres qui paralysent sa capacité de traitement. Soit par une atteinte totale c'est-à-dire le système ne fonctionne plus, ou partielle comme le cas où il réalise seulement une partie du résultat présumé d'être produit, de même un retard irraisonnable dans ses fonctions. En effet, sur les rapports clients-système un déni de service est produit.
Le terme d'entrave n'a pas de signification spécifique en informatique. On peut évoquer parmi les entraves le fait de bloquer totalement le fonctionnement du système, ou celui de causer un ralentissement : par exemple, suite à un envoi de spam massif. Les attaques de sites web par déni de service (DDOS, Distributed Denial Of Service, consistant à lancer simultanément, depuis des milliers d'ordinateurs, des tentatives de connexion à un même site web pour saturer ce dernier).

D'âpres les dispositions de la loi 07-03, on constate qu'il suffit d'une influence négative sur le fonctionnement du système pour qu'il y a une entrave. Comme il est indiqué ci-dessus l'entrave vise à paralyser ou à retarder le fonctionnement du système. (Exemples : bombes logiques introduisant des instructions parasitaires, occupation de capacité de mémoire, mise en place de codification ou tout autre forme de barrage).

Cette infraction, est considérée comme le résultat d'une intrusion préalable, dans une suite des actes dont lesquels l'auteur se comporte de la volonté délibérée d'entraver le fonctionnement du système en ne respectant pas le droit d'autrui.

---

mots de passe pour accéder aux comptes d'autres utilisateurs du réseau de leur université. Les prévenus ont été condamnés à 1 000 euros d'amende avec sursis chacun. Un expert en sécurité qui « teste » la sécurité d'un site web est lui aussi passible de cet article 323-1. C'est pourquoi, lorsqu'une société lance un audit sur ses systèmes, elle doit donner aux auditeurs une autorisation écrite de chercher à contourner ses dispositifs de sécurité.

3.1 Le faussement d'un STAD

Cette incrimination désigne le fait de "fausser" le fonctionnement d'un STAD. C'est une atteinte qui vise d'orienter le système dans son traitement, pour donner un résultat différent de celui attendu.
Le terme « fausser » n'a pas non plus de définition précise ; il peut évoquer toute modification du fonctionnement du système, non souhaitée par son responsable. Le « fonctionnement » ici visé est plus large que le seul « traitement » des données.
L'article 607-5 du code pénal dispose que : « le fait de fausser ou d'entraver intentionnées le fonctionnement d'un STAD… », d'où ces dispositions on constate qu'il y a un élément matériel consiste à un acte de faussement comme il précise précédemment. Il est signalé que Les techniques dont l'utilisation est susceptible de fausser le fonctionnement d'un système sont nombreuses et diverses, on peut ainsi indiquer le cheval de Troie, les bombes logiques, les virus, et également les sabotages effectués sur le matériel. L'atteinte au fonctionnement du STAD peut être le résultat d'une atteinte à son contenu.

Ainsi d'âpres les termes de l'article susmentionné, il est avéré que l'infraction de fausser un STAD et intentionnelle, cela implique que le délinquant effectue des manœuvres sur le système pour erroné le résultat présumé et attendu du système quel que soit ses motivations.
L'intrusion et l'atteinte au fonctionnement du STAD, peuvent dans certains cas même involontairement engendrer des effets sur le contenu du système. En l'occurrence les données qu'il contient. Ainsi l'atteinte à ces données peut compromettre la capacité du système comme une suppression ou une modification de celles-ci.

Ensuite, la notion de la tentative des infractions susmentionnées, s'incline à la lumière de L'article 607-8 du code pénal qui dispose, en sens que la tentative des actes incriminés en vertu de la loi 07-03, est assujettie à la même peine que l'infraction consommée. Mais de notre optique il est difficile de savoir comment se concrétise la tentative de ses délits, dans la mesure où il est difficile de faire une distinction entre les actes préparatoires et les actes d'exécution pour cerner la notion du commencement d'exécution matérielle. En outre Pour qu'une tentative soit punissable il faut que l'activité malveillante présente les conditions énumérées par les articles 114 et suivants du code pénal marocain. Et parmi ces conditions il faut que le délinquant commence l'exécution matérielle de l'acte incriminé.

3.2 Les atteintes au contenu du STAD

Le contenu d'un STAD en l'occurrence les données de toutes nature y compris les données à caractère personnelles est important au même pied d'égalité que le fonctionnement du système lui-même, donc il est indispensable de la mise en œuvre d'un régime de protection efficace à ce propos. Dans le même ordre d'idée, il est clair que le législateur par la loi 07-03 est conscient de cette nécessité, concrètement il a alourdi les peines encourues aux auteurs des atteintes du contenu du STAD : sont portées au double par rapport à celles d'accès ou du maintien frauduleux.

L'article 607-3 Alenia 3 dispose que : « la peine est portée au double lorsqu'il en est résulté soit la suppression ou la modification des données contenues dans le STAD … ».
Cette infraction est en lien direct avec la criminalité économique et financière et en illustre sa dimension numérique. Cette incrimination vise à sanctionner les destructions de fichiers ou de bases de données, et en général tend à réprimer les conséquences de l'introduction par exemple d'un virus dans un système de traitement automatisé de données.

En outre de ces incriminations le code pénal appréhende la délinquance informatique des autres mesures à savoir, l'incrimination de la fabrication, acquisition, détention, offre, ou mise à disposition des équipements ou instruments conçus ou spécialement adaptés pour commettre une ou plusieurs infractions au sens de la loi 07-03, et cela par la disposition de l'article 607-10 du code pénal. Les

outils, notamment les virus. On l'observe, cette nouvelle disposition permet désormais d'appréhender ceux qui se contentent de détenir ou d'offrir des dispositifs techniques permettant de réaliser l'une des atteintes perturbant les traitements ou altérant les données, tels les auteurs de virus informatiques et autres programmes malicieux introduits par l'intermédiaire de simple messagerie électronique (vers, chevaux de Troie, logiciels espions ou spywares…). Afin d'être punissable, cette détention, offre, cession ou mise à disposition ne doit pas être justifiée par des motifs légitimes. Est donc licite la détention de tels dispositifs par les laboratoires scientifiques ou informatiques réalisant des recherches en ce domaine ou des sociétés chargées de concevoir des systèmes informatiques de veille, de sécurisation ou de défense des systèmes.

La Cour de cassation française a précisé le 8 décembre 1999 que « le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé caractérise le délit prévu à l'article 323-3 du Code pénal, sans qu'il soit nécessaire que ces modifications ou suppressions émanent d'une personne n'ayant pas un droit d'accès au système ni que leur auteur soit animé de la volonté de nuire ».
Le piratage informatique n'est plus le fait de petits génies cassant des mots de passe derrière leur écran ; il est devenu une véritable industrie, avec des spécialistes pour chaque tâche et un marché sur lequel s'achètent et se vendent les compétences, les outils et les données volées. Ainsi, certains réalisent et vendent les logiciels de piratage (malwares) clés en main à ceux qui vont lancer des attaques, dont les produits (numéros de cartes bancaires, par exemple) seront revendus à des spécialistes de l'escroquerie, qui eux-mêmes auront recours à des officines de blanchiment pour transférer le produit de leur activité
Afin de combattre le « hacking » en tant que crime organisé, le trafic de logiciels conçus pour le piratage est réprimé par la loi 07-03 du Code pénal, notamment l'article 607-10 qui dispose que « … le fait, pour toute personne de fabriquer, d'acquérir, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre les infractions prévues au présent chapitre ».

La jurisprudence française, a statuée sur une affaire de même espèce, La Cour de cassation a confirmé le 27 octobre 2009 la condamnation du gérant d'une société de conseil en informatique, qui avait publié sur son site web les moyens permettant d'exploiter une faille informatique. Selon la Cour, il s'agissait d'une « mise à disposition, sans motif légitime », de moyens de piratage, alors que cette personne, de par son expertise, devait être particulièrement consciente du fait que ces informations risquaient d'être utilisées pour commettre des infractions. De son côté, la cour d'appel de Caen a condamné à six mois de prison avec sursis et 5000 euros de dommages- intérêts un informaticien qui avait décompilé le code de l'application Skype et publié les failles qu'il avait trouvées, selon lui pour permettre à la communauté des experts en sécurité de trouver des solutions (18 mars 2015).Le site web zataz.com, spécialisé dans la détection de failles dans les sites web, l'alerte de leurs propriétaires et l'information sur la sécurité, a lui aussi connu des difficultés avec ces articles du Code pénal, même s'il ne publie une faille qu'après sa correction. Un internaute lui ayant signalé en 2008 une faille sur un site, le responsable de Za taz en avait averti le propriétaire, puis avait publié un article relatant les faits, tout en floutant les informations sensibles. Cet article n'a pas plu au propriétaire du site, qui a attaqué Zataz en diffamation. Bien que Zataz ait été relaxé de la diffamation, les faits relatés étant exacts, le propriétaire du site l'a par ailleurs fait condamner à supprimer toutes les données sur la faille en sa possession et a fait interdire toute publication ou diffusion de contenus s'y rapportant (cour d'appel de Paris, 9 septembre 2009). Zataz a donc supprimé son article.

Ainsi il y'a une aggravation de la peine par l'article 607-4 chaque fois qu'il Ya une atteinte au STAD ou/et les données qu'il contient, commise ou facilitée par un fonctionnaire ou un employé lors de l'exercice de ses fonctions ou facilite pour autrui la commission de celle-ci. Notamment c'est l'hypothèse où le délinquant est habilité d'agir sur ou dans le système.

4 Conclusion

La protection des données personnelles constitue un impératif croissant dans un monde de plus en plus interconnecté et dépendant des avancées technologiques. Les systèmes de traitement automatisé des données (STAD) jouent un rôle central dans la collecte, le stockage et le traitement de ces informations sensibles. Toutefois, cette centralisation des données pose des défis considérables en matière de sécurité et de confidentialité.

Les atteintes aux STAD peuvent avoir des conséquences graves, telles que la fuite de données personnelles, la fraude financière, la violation de la vie privée, et des dommages irréparables à la réputation des entreprises impliquées. Par conséquent, il est impératif que les entreprises mettent en œuvre des pratiques rigoureuses de protection des données personnelles pour garantir la sécurité et la confidentialité des informations qu'elles traitent.

Ces pratiques incluent l'adoption de politiques et procédures de sécurité adéquates, la formation continue du personnel, et des investissements substantiels dans la sécurité informatique. De plus, les réglementations en matière de protection des données personnelles, telles que le Règlement Général sur la Protection des Données (RGPD) en Europe, imposent des obligations légales aux entreprises pour qu'elles assurent une protection responsable des données personnelles.

En parallèle, les consommateurs doivent également adopter des mesures proactives pour protéger leurs données personnelles. Cela inclut la vérification des politiques de confidentialité des entreprises avant de partager leurs informations, l'utilisation de mots de passe robustes et sécurisés, et la surveillance régulière de leurs comptes pour détecter toute activité suspecte.

En définitive, la protection des données personnelles est une responsabilité partagée entre les entreprises, les gouvernements et les consommateurs. Une collaboration étroite entre ces acteurs est essentielle pour garantir une protection adéquate des données personnelles dans les systèmes de traitement automatisé des données. Ce partenariat est crucial pour bâtir et maintenir un environnement numérique sûr et digne de confiance.

La protection des données personnelles s’impose aujourd’hui comme un enjeu critique dans un environnement global de plus en plus interconnecté et dépendant des avancées technologiques. Les Systèmes de Traitement Automatisé des Données (STAD), qui orchestrent la collecte, le stockage et le traitement de ces informations, sont au cœur de ce défi, exacerbant les risques liés à la centralisation des données sensibles. Les atteintes à ces systèmes peuvent engendrer des conséquences graves, notamment la fuite de données personnelles, la fraude financière, la violation de la vie privée, et des dommages irréversibles à la réputation des entreprises concernées.

Face à ces risques, il est impératif pour les entreprises de mettre en œuvre des mesures rigoureuses pour assurer la sécurité et la confidentialité des données personnelles qu’elles traitent. Cela inclut l'adoption de politiques de sécurité robustes, l’instauration de procédures adaptées, la formation continue du personnel, et des investissements significatifs dans la sécurité informatique. De plus, les cadres réglementaires, tels que le Règlement Général sur la Protection des Données (RGPD) en Europe, imposent des obligations légales strictes aux entreprises. Ces régulations visent à garantir une gestion responsable des données personnelles, en imposant des normes pour la collecte, le traitement et la protection des informations.

En parallèle, les consommateurs ont également un rôle crucial à jouer dans la protection de leurs propres données. Ils doivent adopter des mesures proactives telles que la vérification des politiques de confidentialité des entreprises avant de partager leurs informations, l’utilisation de mots de passe robustes et leur mise à jour régulière, ainsi que la surveillance continue de leurs comptes pour détecter toute activité suspecte.

La protection des données personnelles dans les STAD ne peut être efficace sans une collaboration étroite entre toutes les parties prenantes : les entreprises, les gouvernements et les consommateurs. Cette approche collective est essentielle pour créer un environnement numérique sûr et digne de confiance. Les entreprises doivent s’engager à respecter et à surpasser les exigences réglementaires en matière de sécurité des données, les gouvernements doivent continuer à développer et à renforcer des cadres juridiques adaptés, et les consommateurs doivent rester vigilants et informés des meilleures pratiques pour protéger leurs informations personnelles.

En somme, la sécurité des données personnelles dans un monde de plus en plus digitalisé repose sur un équilibre délicat entre innovation technologique et protection des droits des individus. La réussite de cette entreprise dépend de l'engagement conjoint des différents acteurs pour bâtir et maintenir un écosystème numérique où la confidentialité et la sécurité des informations personnelles sont garanties. Ce partenariat est crucial pour l'avenir des interactions numériques et pour préserver la confiance dans les systèmes de traitement automatisé des données.

REFERENCES

[1] Simon, Anne-Marie, Borricand, Jacques. Droit pénal, procédure pénale. Dalloz Ed 9, 2016.

[2] Quéméner, Myriam, Le droit face à la disruption numérique : Adaptation des droits classiques - Émergence de nouveaux droits, Ed. 1. Gualino, 2018.

[3] MyriemQuemener, Yves Charpenel, (cybercriminalité: droit pénal applique), 2010.

[4] Char, Antoine et Côté Roch, La révolution Internet, Presses de l'Université du Québec, 2009.

[5] Association des Utilisateurs des Systèmes d'Information au Maroc en collaboration avec la société SOLUCOM, Livre Blanc Données à caractère personnel : Quels enjeux et comment se préparer à la loi 09-08 ?

[6] Quéméner, Myriam, Le droit face à la disruption numérique : Adaptation des droits classiques - Émergence de nouveaux droits, Ed. 1. Gualino, 2018.

[7] MyriemQuemener, Yves Charpenel, (cybercriminalité: droit pénal applique), 2010. p1.

[8] Décary-Hétu et David Bérubé, Maxime: Délinquance et innovation, Presses de l'Université de Montréal PUM, 2018. P8.

[9] Hollande, Alain,Linant de Bellefonds, Xavier. Pratique du droit del'informatique et de l'internet. Ed. 6. Dalloz. 2008.

[10] Mattatia, Fabrice. Internet et les réseaux sociaux : Que dit la loi ? Liberté d'expression, Données personnelles, achat en ligne, internet au bureau, piratage. Eyrolles, Ed 3. 2019.

[11] Jessica Eynard, les données personnelles: quelle définition pour un régime de protection efficace ? , Michalon éditeur, 2013

[12] Kevin Freoa La sécurité informatique dans l'entreprise. Projet professionnel, DESS droit et pratique du commerce électronique, université Paris V René Discartes. 2004.

[13] H. Guillaud, Futurs 2.0 : la société transparente, utopie du XXIesiècle ?, 2007.

[14]Fortin, FrancisCybercriminalité : Entre inconduite et crime organisé. Presses Internationales Polytechnique .2013

[15]https://www.actualitesdudroit.fr/documents/fr/jp/j/c/crim/2017/6/28/16-81113.

[16]http://www.lemonde.fr/technologies/article/2012/10/04/facebook-franchit-la-barre-du-milliardd-utilisateurs_1770255_651865.html

[17]HAOUNANI Amine - L'utilisation des données personnelles dans le droit comparé – mémoire pour l'obtention du Master Droit du Numérique – Sous la direction du professeure AKKOUR Soumaya Présenté et soutenue publiquement au seins de la FSJES/Settat en 2019.

[18]Rapport sur la protection des données personnelles dans le cadre du secteur de la sécurité au Maroc/ Séminaire DCAF-CEDHD 19 et 20 octobre 2015- Rabat, Maroc.