REVUE
DROIT & SOCIETE

ISSN: 2737-8152

DOI : 10.5281/zenodo.11321878 – Vol.5, N° 13- 2ème trimistre 2024

Abdellatif MARDDI

LUTTE CONTRE LA CYBERCRIMINALITE AU MAROC : ANALYSE DE LA CONTRIBUTION DE LA LOI 07-03 SUR LES INFRACTIONS RELATIVES AUX SYSTEMES DE TRAITEMENT AUTOMATISE DES DONNEES

REVUE
DROIT & SOCIETE
مجلة
القانون و المجتمع
دورية علمية محكمة تعنى با لدراسات و الأبحاث في المجال القانوني و الاجتماعي و الاقتصادي.
PERIODIQUE SCIENTIFIQUE A COMITE DE LECTURE, CONSACRE A LA PUBLICATION D'ETUDES ET DE RECHERCHES DANS LES DOMAINES JURIDIQUE, ECONOMIQUE ET SOCIAL

DOI : 10.5281/zenodo.11321878 – Vol.5, N° 13- 2ème trimistre 2024

LUTTE CONTRE LA CYBERCRIMINALITE AU MAROC : ANALYSE DE LA CONTRIBUTION DE LA LOI 07-03 SUR LES INFRACTIONS RELATIVES AUX SYSTEMES DE TRAITEMENT AUTOMATISE DES DONNEES

COMBATING CYBERCRIME IN MOROCCO: ANALYSIS OF THE CONTRIBUTION OF LAW 07-03 ON OFFENCES RELATING TO AUTOMATED DATA PROCESSING SYSTEMS

Abdellatif MARDDI

Conseiller à l'Ambassade du Maroc à Tunis

Doctorant en sciences juridiques

Université Mohamed V, Rabat, Maroc

Citation:
MARDDI, A. (2024). LUTTE CONTRE LA CYBERCRIMINALITE AU MAROC : ANALYSE DE LA CONTRIBUTION DE LA LOI 07-03 SUR LES INFRACTIONS RELATIVES AUX SYSTEMES DE TRAITEMENT AUTOMATISE DES DONNEES. REVUE DROIT ET SOCIETE, 5(13).
https://doi.org/10.5281/zenodo.11321878

LUTTE CONTRE LA CYBERCRIMINALITE AU MAROC : ANALYSE DE LA CONTRIBUTION DE LA LOI 07-03 SUR LES INFRACTIONS RELATIVES AUX SYSTEMES DE TRAITEMENT AUTOMATISE DES DONNEES

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

RESUME

La démocratisation de l'accès à l'informatique et la globalisation des réseaux, notamment Internet, ont entraîné des bouleversements importants dans la communication mondiale et le droit applicable. Ce passage de l'analogique au numérique annonce l'avènement d'une nouvelle ère qui a profondément modifié le visage de la société traditionnelle, transformée en une société de l'information où le patrimoine informationnel est devenu un actif stratégique très convoité.

Abdellatif MARDDI
Doctorant en sciences juridiques
Université Mohamed V, Rabat, Maroc

Ce progrès technologique s'est également accompagné de l'émergence de nouveaux comportements criminels que l'arsenal juridique traditionnel était "incapable" de traiter. Dès lors, le besoin s'est fait sentir de créer des incriminations spécifiques adaptées à la réalité

informatique. Cette étude vise à mettre en lumière les apports de la loi 07-03 relative aux infractions liées aux systèmes de traitement automatisé de données (STAD), en tant que texte fondateur pour la mise à niveau de l'arsenal pénal marocain en matière de lutte contre la criminalité informatique.

Mots clés : Criminalité informatique - Loi 07-03 - Informatique - Systèmes de Traitement Automatisé des Données STAD - Information.

COMBATING CYBERCRIME IN MOROCCO: ANALYSIS OF THE CONTRIBUTION OF LAW 07-03 ON OFFENCES RELATING TO AUTOMATED DATA PROCESSING SYSTEMS

Abdellatif MARDDI

PhD student in legal sciences

Mohamed 5 University, Rabat, Morocco

ABSTRACT

The democratisation of access to computers and the globalisation of networks, particularly the Internet, have led to major upheavals in global communication and the applicable law. This transition from analogue to digital heralds the advent of a new era that has profoundly altered the face of traditional society, transformed into an information society where information assets have become highly coveted strategic assets.

This technological progress has also been accompanied by the emergence of new criminal behaviours that the traditional legal arsenal was 'unable' to deal with. As a result, the need has arisen to create specific incriminations adapted to the reality of information technology. This study aims to highlight the contributions of Law 07-03 on offences related to automated data processing systems (ADPS), as a founding text for upgrading the Moroccan criminal arsenal in the fight against computer crime.

Key words: Computer crime - Law 07-03 - Information technology - Automated Data Processing Systems - Information.

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

INTRODUCTION

Le concept de criminalité informatique est intrinsèquement difficile à définir en raison de sa nature complexe, de sa capacité d'évolution et de son impact multiforme. Malgré sa nature polymorphe, la criminalité informatique peut être définie comme "toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet du crime, tout crime dont le moyen ou le but est d'influencer le fonctionnement de l'ordinateur, tout acte intentionnel, associé d'une manière ou d'une autre à la technologie informatique, dans lequel une victime a subi ou aurait pu subir un préjudice et dans lequel l'auteur a réalisé ou aurait pu réaliser un profit".

La démocratisation de l'accès à l'informatique et la globalisation des réseaux, notamment Internet, ont entraîné des bouleversements importants, tant au niveau de la communication à l'échelle mondiale qu'au niveau du droit applicable. Il convient donc de s'interroger sur l'efficacité des dispositions formulées à une époque où l'ordinateur n'existait pas pour répondre aux infractions commises à l'aide de cette technologie. Il semble difficile d'appliquer les règles conventionnelles du droit pénal aux diverses formes de criminalité informatique. Les infractions classiques contre les biens sont conçues pour protéger les actes tangibles, alors que l'utilisation de logiciels et le traitement de l'information constituent des biens intangibles.

Par conséquent, le vide juridique dans ce domaine a été perçu comme une réalité très embarrassante, voire frustrante. En effet, jusqu'en octobre 2003, le phénomène de la criminalité informatique au Maroc n'a fait l'objet d'aucune disposition législative visant à le réprimer. Par conséquent, le cadre juridique marocain présentait d'importantes lacunes qui entravaient la poursuite des infractions liées à la criminalité numérique, malgré le fait que les juges recouraient à des qualifications traditionnelles pour sanctionner certains actes criminels.

Par ailleurs, la question de la criminalité informatique dans la jurisprudence marocaine a été identifiée pour la première fois en 1985, dans l'affaire dite de la "manipulation du téléphone" , qui a illustré opportunément les difficultés rencontrées dans la lutte contre la criminalité informatique. Dans cette affaire, la justice pénale marocaine a été confrontée à un défi sans précédent et a dû examiner l'ingéniosité (révélée par l'ordinateur) avec laquelle sept prévenus, des fonctionnaires de l'Office National des Postes et Télécommunications et des techniciens de la Compagnie Générale de Construction Téléphonique, auraient institutionnalisé des pratiques frauduleuses sur les compteurs d'un certain nombre de lignes téléphoniques d'abonnés au Centre Casa-Bandoeng dans le but d'éliminer l'impôt.

Poursuivis sur la base, entre autres, des articles 505 (vol) et 248 (corruption) du Code Pénal, les accusés ont été finalement condamnés en vertu de l'article 521 du même code, « appropriation frauduleuse de l'énergie électrique ou de toute autre énergie ayant une valeur économique » avant qu'ils ne soient relaxés au niveau de la cour d'appel .

Concrètement, cette affaire n'a pas manqué de susciter des questions et a permis de faire au moins un double constat. Elle montre d'une part, la difficulté d'introduire la fraude informatique dans les incriminations traditionnelles de notre système juridique et d'autre part la nécessité d'adapter notre droit pénal à la réalité informatique.

L'intervention donc du législateur a été de plus en plus perçue comme un impératif. C'est dans ce sens qu'intervient la loi 07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données (STAD). Il ne s'agit pas d'un texte s'appliquant uniquement à des cas bien définis, mais d'une loi pénale couvrant de nombreux agissements frauduleux imputables à l'informatique et un texte fondateur pour la mise à niveau de l'arsenal juridique marocain.

A ce stade, il est légitime de s'interroger sur les apports de cette loi en matière de lutte contre la criminalité informatique au Maroc ?

L'intérêt de cette étude n'est plus à démonter, la question de la criminalité informatique pose des problèmes juridiques et judiciaires de dimension planétaire et de portée considérable . Ainsi, la présente contribution est digne d'intérêt et d'un apport considérable aussi bien pour les praticiens du droit, que pour les

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

 ISSN: 2737-8101

universitaires et tout curieux du savoir, dans un monde où l'information est devenue un enjeu d'une extrême importance dans le développement des peuples et pour la sécurité des biens, des institutions et des personnes.

Reproduite à partir de la loi française du 05 janvier 1988 dite loi Godfrain, la loi 07-03 permet de réprime pénalement de nombreux comportements, qu'on peut les ranger en deux catégories à savoir les intrusions (I), ainsi que les atteintes aux systèmes de traitement automatisé des données (II).

Les intrusions

La loi n° 07-03 incrimine l'accès et le maintien frauduleux dans un système de traitement automatisé de données (STAD). Pour comprendre pleinement les implications de cette législation, il est essentiel de commencer par clarifier la notion de STAD (A), avant d'examiner en détail les contours juridiques de ces intrusions (B).

Notion de SATD.

Pour que les actes prévus aux articles 607-3 à 607-6 du code pénal soient considérés comme délictueux, il est nécessaire qu'ils soient perpétrés à l'encontre d'un système de traitement automatisé de données. Malgré l'importance de cette notion pour la mise en œuvre de la loi 07-03, elle n'a pas été définie par le législateur marocain, conformément à l'approche adoptée par le législateur français .

La Convention du Budapest sur la cybercriminalité n'utilise pas la notion de STAD, mais celle de « système informatique » qui le définit comme « Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données» .

En revanche, le législateur marocain, quant à lui, définit le système informatique dans le premier article du projet du code du numérique comme: « ensemble de moyens destinés notamment à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre l'administration et les usagers ainsi qu'entre les services de l'administration » .

On constate que cette définition limite la notion du système d'information au champ de e-gouvernement du moment qu'il y introduit l'administration dans toutes les opérations citées par ledit projet . Alors que celle donnée par la doctrine marocaine est plus globale et englobe «l'ensemble de moyens techniques, administratifs, et humains qui servent à la collecte, au classement et à la transmission d'informations entre les membres d'une organisation (Système de traitement automatisé de données, systèmes informatiques, etc.)».

Durant les travaux préparatoires de la loi 07-03, des députés parlementaires avaient proposé une définition technique d'un système de traitement automatisé des données en tant que « Unité ou ensemble d'unités informatiques permettant automatiquement l'utilisation des données reçues, leur traitement, leur stockage et leur consultation ou transmission par des moyens de télécommunication ». Mais, par crainte de la désuétude d'une telle définition du fait de l'évolution rapide des technologies, le parlement l'a écarté, laissant ainsi, à la doctrine et la jurisprudence le soin de définir cette notion.

L'absence en droit marocain d'une liste des éléments qui peuvent être qualifiés de STAD a provoqué plusieurs problèmes judiciaires, notamment en ce qui concerne la détermination des éléments qui peuvent être qualifiés de STAD. Le retard législatif a impacté négativement la position de la

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

jurisprudence, du moins au début d'application de la loi 07-03.

Dans un premier temps, le juge marocain s'est abstenu à considérer la boite E-mail en tant que STAD. C'est ainsi que le tribunal de Première Instance de Casablanca a refusé, en 2007, de considérer l'E-mail en tant que STAD . Néanmoins, un arrêt rendu plus tard par la Cour d'appel de Rabat fait de l'E-mail une partie intégrante du système de traitement automatisé des données et considéré que « le système informatique du ministère de l'Energie et des mines un STAD et que la boite E-mail composante inséparable dudit système, du fait qu'elle reçoit, classe et stocke automatiquement les données selon une chronologie bien déterminée » . Ce revirement jurisprudentiel a été confirmé par une série de décisions judiciaires dont la plus récente date du 09/04/2015, dans laquelle le tribunal de Rabat a condamné un accusé en vertu de l'article 607-3, après avoir s'assurer qu'il utilise la boite E-mail pour modifier les numéros de compte des clients .

Le téléphone mobile a été qualifié quant à lui, par le tribunal de première instance de Rabat, comme un système de traitement automatisé des données. C'est ce qui ressort du contenu de sa décision : « Attendu que le travail du prévenu dans un centre d'appel lui a procuré la possibilité de découvrir plusieurs failles dans le système informatique de la société française de télécommunication SFR et de les exploiter pour déchiffrer les mots de passe des téléphones mobiles, constitue en vertu des dispositions de l'article 607-3 le délit d'accès et de maintien frauduleux dans un STAD » . Ce même tribunal a considéré, dans une décision en date du 27 juin 2016, que « L'utilisation par le prévenu du mot de passe d'une carte bancaire en se passant par son titulaire légal, constitue l'infraction d'accès frauduleux dans un STAD » .

S'agissant des réseaux sociaux (Facebook, Twiter..), le juge marocain s'est également abstenu, dans un premier temps, à les considérer comme des STAD . Toutefois, le tribunal de première instance de Rabat s'est rattrapé ultérieurement et a considéré le « Facebook » en tant que STAD, indiquant dans son jugement qu' « Attendu que le prévenu a avoué qu'il piratait des comptes Facebook afin d'obtenir des sommes d'argent de leurs propriétaires, ce qui constitue les délits d'accès et d'entrave d'un STAD conformément aux articles 607-3 et 607-6 du code pénal » .

La notion du STAD étant clarifiée, il convient, maintenant, d'analyser les délits d'accès et maintien frauduleux dans un STAD.

L'accès ou le maintien frauduleux dans un STAD.

Avant d'aborder ce paragraphe, une question mérite d'être posée : le système de traitement doit-il être protégé par un dispositif de sécurité pour que les infractions d'accès ou de maintien soient constituées ?

La question en cause fait l'objet de deux écoles de pensée opposées, chacune reposant sur des considérations différentes. Certains auteurs soutiennent que le législateur n'a pas voulu imposer une obligation de protection parce qu'elle aurait été soit trop imprécise, soit très technique, risquant ainsi une obsolescence rapide et répétitive compte tenu de l'évolution constante du contexte informatique. Par conséquent, ils estiment qu'il appartient aux tribunaux de déterminer le caractère frauduleux de l'acte, tout en soutenant que l'infraction est constituée même en l'absence de protection du système mis en cause.

A contrario, un autre courant de pensée considère que l'accès ou le maintien frauduleux dans un STAD n'est répréhensible que si le système en question est protégé contre les accès non autorisés.

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

 ISSN: 2737-8101

La nécessité d'un système de sécurité est implicite dans le sens de l'adverbe "frauduleusement" .

Le législateur marocain a choisi de n'exiger aucun dispositif de sécurité pour que l'infraction soit constituée. La preuve, c'est le silence de la loi. Par conséquent, la protection pénale, en droit marocain, existe même si le système de traitement n'est pas pourvu de mesures de sécurité .

Cette précision étant faite, il convient de traiter respectivement l'accès et le maintien frauduleux dans un STAD.

L'accès frauduleux dans un STAD est réprimé au Maroc en vertu du premier alinéa de l'article 607-3 du Code pénal qui stipule que : « Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un mois à trois mois d'emprisonnement et de 2.000 à 10.000 dirhams d'amende ou de l'une de ces deux peines seulement… ».

Le législateur marocain n'a pas définis la notion d'accès, suivant en cela certains législateurs et la convention du Budapest sur la cybercriminalité. La doctrine française définit l'accès comme « toutes les situations de pénétrations d'un système qu'elles se réalisent à partir de la machine elle-même, ou à distance, l'accès indu est celui qui sans droit quel que soit ses modalités» . D'une manière générale, l'accès peut être présenté comme l'établissement d'une communication avec le système .

L'accès frauduleux au sens de l'article 607-3 du C.P, vise tous les modes de pénétration irréguliers d'un système, que l'accédant travaille déjà sur la même machine ou sur un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de télécommunication. Ledit article n'a pas même donné de précisions quant à la forme que peut prendre l'accès dans un STAD. En effet, la formulation employée par le législateur est très large et n'est pas liée à une forme particulière d'accès, reflétant sa volonté à avoir une loi évolutive non liée à des techniques précises .

Pour être qualifié d'infraction, la loi précise que l'accès doit être frauduleux. Cela signifie que l'acte doit être volontaire et ne résulte d'une simple erreur. Peu importe que l'auteur ait procédé par jeu ou non, l'intention de nuire n'étant pas nécessaire. Peu importe la manière d'accès : directement sur l'ordinateur, ou à distance ; peu importe que le système soit protégé ou non, et peu importe qu'il y ait ou non résultat .

Le législateur entend donc sanctionner tous les cas dans lesquels une personne se sera introduite dans un STAD, avec la conscience du caractère irrégulier de son acte. Le seul fait d'entrer sans droit est incriminable.

L'accès au STAD peut se faire depuis l'extérieur du système, c'est ainsi, un pirate qui pénètre dans un ordinateur connecté à Internet tombe sous le coup de la loi. C'est le cas également lorsqu'un salarié ayant quitté son emploi pénètre dans le système de son ancien employeur; ou encore le maître d'ouvrage qui après réalisation de son œuvre et conclusion du contrat, ayant gardé les mots de passe, accède au système .

Il est possible pour un intrus d'exploiter les vulnérabilités du système de sécurité afin d'y accéder. En outre, un intrus peut obtenir l'accès en insérant un programme malveillant qui lui permet d'exercer un contrôle total sur le système informatique de l'entreprise . L'accès peut également être obtenu en introduisant un code d'accès obtenu frauduleusement. Dans ce contexte, le tribunal de première instance de Rabat a jugé que les prévenus avaient commis le délit d'accès frauduleux à un STAD en accédant au site du ministère de la Justice à l'aide de codes piratés selon la technique SQLINJ .

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

 ISSN: 2737-8101

L'accès consiste également à pénétrer au système en utilisant l'adresse IP d'un pays étranger, et à envoyer des formulaires aux clients de banques pour les remplir et les renvoyer. Les données collectées par les accusés seront ensuite exploitées et copiées sur des cartes bancaires falsifiées, et utilisées ultérieurement pour retirer de l'argent aux guichets automatiques .

L'accès au STAD peut, en outre, se faire depuis l'intérieur du systen deux courantsème, c'est le cas notamment du salarié qui, depuis son poste, pénètre dans une zone du réseau de l'entreprise à laquelle il n'a pas le droit d'accéder.

Il faut préciser que l'accès dans un STAD n'est pas sanctionné que s'il est frauduleux. Or la jurisprudence marocaine n'a pas précisé la signification du terme « frauduleux », contrairement à la jurisprudence française qui estime que « l'accès frauduleux est constitué dès lors qu'une personne, non habilitée, pénètre dans ce système tout en sachant être dépourvue d'autorisation, peu importe le mobile » .

L'article 607-3 du C.P réprime non seulement l'accès à un système, mais également le fait de s'y maintenir. Ainsi, le 2ème alinéa dudit article stipule qu' « Est passible de la même peine toute personne qui se maintient dans tout ou partie d'un système de traitement automatisé de données auquel elle a accédé par erreur et alors qu'elle n'en a pas le droit ».

Le délit de maintien frauduleux dans tous ou partie d'un système de traitement automatisé de données est bien entendu la conséquence logique du crime d'intrusion. Précisons sur ce chef, que même si l'accès à un système informatique n'a pas été commis de manière illicite, un séjour prolongé de manière non autorisé est incriminé en tant que tel .

Le législateur vise deux situations : la première est celle où la personne ayant une autorisation d'accès à une partie du système en profite pour accéder à une autre partie du système et s'y maintenir sans autorisation. Et la deuxième situation s'applique à toute personne qui est entrée dans le système par erreur, ou par hasard et qui s'y maintient en sachant pertinemment qu'elle n'a pas le droit de le faire.

En outre, il existe d'autres cas de détention irrégulière. Il s'agit également de cas d'utilisation prolongée au-delà de la durée autorisée . C'est le cas des employés qui ont utilisé les téléphones portables fournis par leur employeur pour des raisons personnelles et qui ont abusé de ce privilège en prolongeant l'utilisation de ces appareils pendant des heures, voire des nuits entières, à l'insu de leurs collègues. Cela est rendu possible par l'utilisation de systèmes d'inhibition et d'écrans noirs. L'objectif était d'augmenter le nombre de points leur permettant d'obtenir des cadeaux et de l'argent sans avoir à payer les appels . Le délit de maintien de système est également constitué lorsqu'un employé, après son licenciement, conserve le code d'accès au système de son ancien employeur, y accède et le maintien, en causant même des dommages qui justifient un délit plus grave .

Il est important de noter que pour tomber dans le champ d'application du deuxième alinéa de l'article 607-3, les conséquences de l'entretien irrégulier sont de peu d'importance. L'entretien irrégulier peut être défini comme tout entretien qui n'est pas effectué conformément à la réglementation en vigueur . Il peut être actif ou inoffensif . Dans le cas des prévenus, qui se sont maintenus dans l'annuaire électronique de France Télécom et ont procédé à des manœuvres illégales pour bénéficier de téléchargements gratuits , ce maintien était actif. En revanche, dans le cas des prévenus qui ont effectué un maintien inoffensif, ce maintien n'était pas actif. L'entretien irrégulier peut entraîner une responsabilité pénale dans les deux cas . Pour être incriminable, le maintien « doit être fait sans droit et en connaissance de

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

cause» , c'est-à-dire le fraudeur doit avoir conscience de l'irrégularité de son acte. Autrement dit, l'agent doit réaliser non seulement un dol général (conscience et volonté d'enfreindre la loi pénale), mais aussi un dol spécial, une fraude, c'est-à-dire la connaissance par l'agent de l'absence de droit à accéder à un système ou à s'y maintenir.

Par ailleurs, les intrusions avec dommages sont plus sévèrement sanctionnées du moment que la peine est portée au double lorsqu'il en résulte une altération du fonctionnement du système d'information. Ainsi l'article 607-3 stipule que « la peine est portée au double lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système de traitement automatisé de données, soit une altération du fonctionnement de ce système ».

Cette disposition trouve application dans plusieurs décisions judiciaires, notamment l'affaire dite « virus Zotob » , dans laquelle la chambre criminelle de la cour d'appel de Rabat a condamné deux pirates marocains à deux ans de prison ferme pour le premier, et un an ferme pour le deuxième, sur la base, entre autres, des articles 607-3 et 607-7 du code pénal pour accès frauduleux à un STAD ayant altéré le fonctionnement du système et falsification des documents informatisés.

Une autre décision du tribunal de première instance de Kenitra considère que « le prévenu n'a pas uniquement accédé au système de traitement automatisé de données, mais y a délibérément provoqué des modifications lui permettant de créer des mandats fictifs, faits qui constituent le délit prévu par l'article 607-3 du code pénal » .

Il est à signaler que les députés marocains avaient demandé l'amendement du texte avant sa promulgation, et prendre en considération le dommage causé pour incriminer ou non l'accèdent fraudeur, mais le législateur n'en a pas tenu compte estimant que ce qui est sanctionné n'est pas la volonté de nuire mais le simple fait de s'introduire dans un système.

La loi 07-03 réprime également les atteintes aux systèmes et données informatiques.

Les atteintes

La loi 07-03 du Code pénal marocain marque une étape significative dans la lutte contre la cybercriminalité en définissant et en réprimant les infractions liées aux systèmes de traitement automatisé des données (STAD). Cependant, ces atteintes peuvent être classées en deux catégories distinctes : les atteintes au fonctionnement du STAD et celles aux données qu'il contient. D'une part, les atteintes au fonctionnement (A) concernent toute action qui entrave, fausse ou détruit le système, impactant ainsi son efficacité et son utilité. D'autre part, les atteintes aux données (B) se concentrent sur les manipulations frauduleuses des informations traitées par ces systèmes, qu'il s'agisse de leur introduction, suppression, modification ou altération. Cette distinction est cruciale pour comprendre l'ampleur et la diversité des menaces pesant sur les infrastructures informatiques et les informations qu'elles gèrent. En outre, l'analyse des textes législatifs et des décisions judiciaires révèle une complexité juridique croissante, accentuée par les progrès rapides de la technologie et l'ingéniosité des cybercriminels. Cette section examine en détail ces deux types d'atteintes, en s'appuyant sur les dispositions de la loi 07-03 et sur les cas jurisprudentiels, pour mettre en lumière les défis et les lacunes actuelles dans la protection des STAD au Maroc.

Atteintes au fonctionnement d'un STAD

L'atteinte au fonctionnement d'un STAD peut être constitué de manières très diverses, par tout comportement ou toute action qui va entraîner temporairement ou

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

 ISSN: 2737-8101

de manière permanente une gêne dans le fonctionnement du système, une dégradation du système voire le rendre totalement inutilisable. L'article 607-5 du code pénal précise que « le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé des données est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement ».

A la lecture de cet article, il ressort que l'élément matériel d'une atteinte portée à un STAD lui-même et non pas à ses données peut provenir soit de l'entrave ou du faussement de ce dernier.

L'obstruction d'un STAD englobe un large éventail de comportements qui empêchent le traitement automatisé des données. Le terme "obstruction" est synonyme de "gêne, empêchement" , ce qui peut entraîner l'arrêt complet du système. Ceci est susceptible d'être qualifié dans une grande variété de cas . Il est également possible d'envisager la notion de "délinquance astucieuse", qui peut se manifester de diverses manières, y compris par le sabotage ou la destruction matérielle de systèmes de traitement automatisé de données. Un auteur donne l'exemple d'une tasse de café renversée sur un ordinateur . Cependant, les formes de sabotage décrites sont essentiellement des "virus, des bombes logiques ou des chevaux de Troie". Il s'agit de programmes parasites introduits illicitement dans un réseau ou un système, susceptibles de se produire et d'entraîner la destruction de données, voire le blocage du système.

L'entrave visée donc par ces dispositions pénales est l'« entrave intentionnelle portée à l'usage légitime d'un système informatique » et qui suppose l'accomplissement d'un acte positif. En effet, l'entrave du système peut résulter par la destruction des fichiers garantissant son bon fonctionnement, comme elle peut résulter d'un encombrement de sa mémoire suite à une propagation des virus. Ainsi, le fait de programmer l'envoi d'un grand nombre de messages, de simuler de multiples connexions sur un serveur, ayant pour effet le ralentissement de sa capacité de traitement, a été considéré par la cour d'Appel Rabat, comme entrave au système de traitement automatisé de données .

L'entrave peut être également «interne» et provenir d'une personne ayant droit à l'accès et au maintien. C'est le cas par exemple d'un employé licencié d'une entreprise ayant gardé les mots de passe des portails (site web) de l'entreprise, avait en premier lieu bloqué les mails dudit portail, et ensuite supprimé le site web de l'entreprise . Ou le cas d'un gérant qui entrave le fonctionnement du système informatique (sites Web) de la société dont il est gérant .

Toutefois certains agissements doivent être écartés. C'est l'exemple de la cessation de travail suite à une grève des personnels informaticiens, entraînant ainsi entrave au fonctionnement d'un système .

Le texte réprime également le faussement du système. Celui-ci vise toute manipulation ayant pour objet de travestir la réalité en vue d'empêcher le traitement automatisé des données . Il s'agit des actes provocant altération, défiguration, dénaturation du système, ou tout simplement « lui faisant produire un résultat non attendu» . Autrement dit, fausser le fonctionnement, c'est exercer sur le système une action qui, sans empêcher son fonctionnement, infléchit celui-ci jusqu'à le rendre inutilisable . En effet, il a été considéré comme constitutif du délit de faussement d'un système informatique, le fait que le prévenu procède à la modification des données des cartes bancaires et les a utilisé par la suite à l'aide d'autres complices pour effectuer des achats et des réservations par Internet dans des hôtels de luxe .

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

Entre également dans le champ d'application de cette infraction, l'utilisation des logiciels susceptibles de perturber le système d'information ou de fausser son fonctionnement normal tels les virus, vers ou bombes logiques. Dès lors, tous les procédés utilisés pour bloquer volontairement un système en agissant sur ses éléments, qu'il y ait ou non accès à ce système, entre dans le champ de l'article 607-5.

La loi 07-03 n'exige pas l'intention de nuire pour constituer l'infraction d'entrave ou de faussement d'un système informatique. L'auteur du délit est sanctionné dès lors qu'il est conscient des actes d'entrave et de faussement du fonctionnement du système et qu'il doit avoir agi contre la volonté du maître du système. Mais il n'est pas facile de montrer le caractère intentionnel de l'entrave ou du faussement d'un système, c'est pourquoi on le déduit souvent des faits et des circonstances de la commission de l'infraction . En revanche, lorsqu'un individu pénètre dans un système informatique sans rien faire d'autre, nous parlons alors d'accès et de maintien frauduleux et non de l'entrave .

Par ailleurs, le législateur marocain réprime aussi les actions correspondant à la fabrication, fourniture, ou détention des programmes viraux, ainsi que les dispositifs permettant la commission des infractions informatiques. En effet, aux termes de l'article 607-10 du code pénal, est puni « le fait, pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données, conçus ou spécialement adaptés pour commettre les infractions » relatives aux systèmes informatiques. Ainsi, même si le programmeur d'un virus ne l'utilise pas en personne pour s'introduire dans un système informatique, il est sanctionné au regard des dispositions de cet article pour le fait de fabrication de programme malicieux, une fois le préjudice subi.

Néanmoins, malgré l'existence d'un arsenal juridique répressif, il est difficile pour le législateur marocain de s'attaquer efficacement à certaines pratiques, telles que le spamming . La loi 31-08 de 2008 relative à la protection du consommateur prévoit certaines conditions pour l'utilisation du courrier électronique à des fins publicitaires. Elle interdit l'utilisation des adresses électroniques ou de l'identité de tiers à des fins commerciales. Néanmoins, le spamming n'est pas limité à cette disposition, car le spammer ne s'approprie pas l'identité d'un tiers. Le tiers peut être anonyme ou afficher son nom de manière claire. Cela permet de faire la distinction entre le spamming et le phishing . On constate donc que la loi 31-08 ne prévoit pas de dispositions pour le spamming et ne peut donc pas le sanctionner.

Deux raisons peuvent être identifiées pour expliquer cette lacune juridique. D'une part, le spamming n'est pas défini dans le Code pénal, ce qui rend difficile l'application de l'article 607-5. D'autre part, le spamming est une pratique internationale. Il n'est donc pas certain que le Maroc soit en mesure d'enrayer définitivement le spamming, d'où la nécessité d'une coopération internationale entre les Etats.

Enfin, tout ce qui échappe à la définition des atteintes au fonctionnement du système de traitement informatisé des données trouvera le plus souvent sa base juridique dans les incriminations ayant pour objet la dénaturation des données.

Atteintes aux données.

La numérisation des informations et des connaissances rend l'information universelle et disponible, mais l'expose à des risques constituants un défi aux régimes juridiques. Parmi ces risques, on trouve les atteintes aux données de manière générale et aux données à caractère personnel de manière particulière.

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

 ISSN: 2737-8101

Interpelé par de tels risques, le législateur marocain réprime les atteintes volontaires aux données. Ainsi, l'article 607-6 du code pénal incrimine « le fait d'introduire frauduleusement des données dans un système de traitement automatisé des données ou de détériorer ou de supprimer ou de modifier frauduleusement les données qu'il contient, leur mode de traitement ou de transmission ».

L'élément matériel de cette infraction peut revêtir deux formes :

Une action sur les données contenues dans le système par suppression, modification ou destruction des données existantes ou par introduction de données nouvelles ;

Une altération des modes de traitement ou de transmission des données par suppression ou modification de ceux-ci.

La suppression des données informatiques s'étend à tout acte qui rend les données inaccessibles à leur propriétaire ou exploitant. Quant à la modification, elle se commet sur des données existantes et englobe plusieurs types d'actes tels la modification de l'apparence des sites Web, ou la modification des rapports financiers stockés électroniquement...etc.

En réalité, toute manipulation de données, qu'il s'agisse de les introduire, de les supprimer, de les modifier ou de les maquiller, provoque, en toutes circonstances, une altération du système. Le fait de déréférencer l'adresse d'un serveur Web dans les moteurs de recherche, de défigurer un site web pour y insérer une image indécente ou encore de modifier les informations d'une base de données, constituent autant d'atteintes visées par le texte.

Les applications illicites couvertes par cet article sont nombreuses et peuvent être classées en trois grandes catégories : la réduction du prix des marchandises sur un site de commerce électronique, la modification ou la suppression du contenu de bases de données et la modification du statut fiscal d'une entreprise. Dans tous les cas, ces actions sont susceptibles d'entraîner des pertes financières considérables pour une entreprise.

Il faut préciser cependant que l'article 607-6 ne réprime pas toutes les formes d'action, la copie de données notamment échappe à la répression car elle n'est ni une introduction (puisqu'elle est une sortie), ni évidemment une suppression ou une modification.

En outre, le législateur marocain n'a pas abordé une question cruciale concernant les données stockées dans un STAD, à savoir la technique du "détournement" de site web. Cette technique consiste à copier tout ou partie du contenu d'un site, ainsi que les pages liées, sur le disque dur d'un ordinateur, ce qui permet d'y accéder hors connexion. Le site est alors ouvert comme n'importe quel autre fichier, sans attendre l'interruption de la connexion.

Si la légitimité du détournement de site se pose en termes de droit d'auteur, il peut également constituer un délit informatique dans la mesure où le détournement massif dans un STAD peut atteindre les données et les endommager.

En ce qui concerne l'introduction frauduleuse de données dans un STAD, le Maroc a connu plusieurs cas où certains cybercriminels ont piraté des sites web et y ont ajouté des messages de revendication, tels que les sites web du ministère de la justice et de certaines associations sportives. En outre, ils ont introduit des données fictives sur des employés ou des clients fictifs afin d'obtenir des salaires ou des allocations spécifiques. Par exemple, une personne a introduit des données dans le système informatique de son entreprise, MoneyGram, ce qui lui a permis de transférer d'importantes sommes d'argent à des personnes dans différentes régions du Maroc .

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

Les programmes peuvent également faire l'objet d'introduction, comme l'ont fait les prévenus lorsqu'ils ont piraté le site Web du ministère de la Justice, en y injectant le programme « CHELL » pour le contrôler, et ont également créé une fausse page pour la société « PayPal » .

L'altération de données sans droit dans un système est incriminée au regard de l'article 607-6 sans se préoccuper ni de la réalité ou non de ces données, ni de leur quantité, ni même de l'état du système (vide, connecté ou autre). Le législateur ne considère pas non plus la valeur monétaire de ces données, contrairement au législateur américain qui en prend compte pour déterminer si la violation constitue un délit ou un crime .

L'élément moral est donc constitué par l'altération « intentionnelle et au mépris des droits d'autrui » . L'auteur de l'infraction doit avoir agi en sachant qu'il introduit, modifie ou supprime des données. Le législateur n'exige pas que l'altération des données ait des conséquences pour l'ériger en infraction.

Par ailleurs, les données à caractère personnel bénéficient également d'une protection juridique par la loi 09.08 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel . Cette loi vise à mettre à la disposition du système juridique marocain des mécanismes légaux spécifiques pour garantir la protection effective des données personnelles contre toute collecte ou utilisation frauduleuse.

Ce texte évoque des cas de la criminalité informatique notamment dans le septième chapitre relatif aux sanctions. Ainsi, l'article 52 prévoit une amende de 10.000 à 100.000 dirhams à l'encontre de quiconque crée un fichier de données personnelles sans autorisation, ou poursuivre l'activité de traitement de données personnelles malgré le retrait de l'autorisation ou du récépissé d'autorisation. L'article 53 quant lui sanctionne d'une amende de 20.000 à 200.000 DH par infraction, tout responsable de traitement de données à caractère personnel refusant les droits d'accès, de rectification ou d'opposition prévus aux articles 7, 8 et 9.

Soucieux de réprimer toutes formes de comportements nuisibles aux tiers, le législateur a également pris en considération l'atteinte à ce qu'on a appelé un produit, le document informatisé . De là, l'incrimination de la falsification de données informatiques et de leur usage.

En effet, le premier alinéa de l'article 607-7 du C.P dispose « Sans préjudice de dispositions pénales plus sévères, le faux ou la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de 10.000 à 1.000.000 de dirhams ».

Cet article ne définit pas le document informatisé. Ce dernier est défini par la doctrine française comme « tout support matériel destiné à recevoir des informations et en ayant déjà reçu par application d'un procédé informatique» . L'emploi de l'adjectif « informatisé » implique que le support a été soumis à un traitement informatique. Les documents informatisés sont donc des documents sortis à titre d'exemple d'un ordinateur, d'un télécopieur, d'un télétype, des cartes de crédit.

Cette incrimination est conforme à la législation civile qui a conféré une valeur probante aux documents électroniques et qui a mis en œuvre un certain nombre de mesures visant à garantir l'authenticité des documents électroniques, notamment la cryptographie, la certification et la signature électronique. .

Pour que le délit de falsification de documents informatisés soit constitué, le document en question doit être d'une part soumis au traitement informatique et

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

d'autre part que la falsification occasionne un préjudice à autrui. Très exactement, l'article 607-7 exige que la falsification soit de nature à causer un préjudice à autrui. Le document informatisé doit donc avoir une portée juridique pour que le délit soit constitué.

Enfin, ce délit implique certainement une intention coupable. Bien que l'article 607-7 n'en fasse pas état, la proposition est évidente puisque le mot essentiel est celui de falsification : l'agent doit avoir conscience d'altérer la vérité et aussi conscience que son geste peut causer éventuellement un préjudice à autrui. Le préjudice est mesuré sur la base de la valeur probante du document informatisé. Ainsi, le tribunal de première instance de Rabat a considéré comme préjudice, le détournement des identifiants bancaires des clients de l'établissement bancaire .

En outre, l'article 607-7 du code pénal ne définit pas les moyens utilisés pour la falsification d'un document informatisé et ne fait pas de distinction suivant la qualité de l'auteur de l'infraction (magistrats. fonctionnaires. Officiers publics, simples particuliers) ou suivant la nature de l'acte falsifié (acte public, acte authentique, acte commercial ou acte privé). Alors que les dispositions pénales relatives aux faux traditionnels en tiennent compte .

De ce qui précède, il ressort que les moyens utilisés dans la falsification ordinaire peuvent être également pris en compte pour la falsification informatique, comme c'est le cas pour la falsification de la signature électronique ou la modification des données d'un écrit électronique . C'est dans ce sens que le tribunal de première instance de Casablanca a condamné des employés et cadres des sociétés « COMANAV voyage » et « COMANAV ferry », pour avoir créé de faux titres de voyage, à travers la modification des données contenues dans le système de traitement automatisé des données des deux sociétés et détournement d'argent en résultant. Deux d'entre eux ont été poursuivis pour falsification de documents informatisés .

Par ailleurs, la pratique judiciaire a soulevé une problématique relative à la nature juridique de la carte de crédit. Est-elle ou non un document informatisé ?

La jurisprudence est divisée sur ce point. Ainsi, la cour d'appel de Rabat considère parfois les cartes de crédit comme de simples documents bancaires au sens de l'article 357 du Code pénal , et d'autres fois en tant que documents informatisés .

Nous soutenons le courant jurisprudentiel qui considère les cartes de crédit comme documents informatisés, du fait que les données manipulées ne sont pas des données externes affichées sur la carte tels le nom du titulaire de la carte, du nom de l'établissement bancaire ou de la date d'expiration, mais la falsification atteint les données contenues dans la bande magnétique, qui est en elle-même un support électronique, ce qui lui permet d'être qualifiée de document informatisé.

L'usage de documents informatisés falsifiés est également incriminé par la loi 07-03, c'est ce qui ressort du deuxième alinéa de l'article 607-7 qui dispose que « Sans préjudice de dispositions pénales plus sévères, la même peine est applicable à quiconque fait sciemment usage des documents informatisés visés à l'alinéa précédent ».

L'usage, c'est l'utilisation d'un document falsifié. Ce délit appelle moins d'observations. Les peines prévues sont les mêmes que pour la falsification. Le préjudice, quoique non évoqué par le texte, est également exigé, et ce préjudice est - au moins théoriquement - distinct de celui qui est requis dans le délit de falsification.

L'intention implique, là encore, à la fois la connaissance de la fausseté du document utilisé mais aussi la conscience que l'agent

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

a eu que son acte pouvait éventuellement causer un préjudice à autrui.

Par ailleurs, la tentative de crimes est toujours punissable. Mais lorsqu'il s'agit de délits, elle doit être prévue par une disposition expresse du code pénal. La répression de la tentative en droit pénal n'est pas systématique pour les délits. Pour l'article 607-8, la tentative des délits prévus par les articles 607-3 à 607-7 ci-dessus et par l'article 607-10 est punie des mêmes peines que le délit lui-même.

A noter qu'une fois la criminalité informatique est répondue, il peut y avoir des associations entre cybercriminels. A cet effet, le législateur a prévu de sanctionner les associations formées et qui ont pour objectif des infractions électroniques. Ainsi, l'article 607-9 stipule que « Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues au présent chapitre est puni des peines prévues pour l'infraction elle même ou pour l'infraction la plus sévèrement réprimée ». Cette dernière incrimination a pour objectif de réprimer les associations de malfaiteurs informatiques, dès leurs premiers efforts accomplis en vue de la commission des crimes informatiques.

Conclusion

Malgré les apports louables de la loi 07-03 dans la lutte contre la criminalité informatique, l'arsenal juridique marocain reste insuffisant face à l'évolution rapide des technologies et à l'ingéniosité croissante des cybercriminels. La démocratisation d'Internet et l'émergence de nouvelles pratiques criminelles, telles que les casinos virtuels et le trafic électronique de stupéfiants, posent des défis considérables auxquels la législation actuelle peine à répondre de manière adéquate. Ces nouveaux comportements restent souvent impunis, ce qui laisse une grande marge de manœuvre aux cybercriminels.

L'évolution rapide des technologies exige une législation dynamique et adaptable. En l'absence d'exemples de techniques stables et immuables, il est impératif que la législation suive une courbe évolutive, s'adaptant constamment aux nouvelles réalités imposées par le progrès technologique. Cette adaptabilité doit être au cœur des préoccupations du législateur marocain, afin que les lois en vigueur restent pertinentes et efficaces.

Pour relever ces défis, une action législative est nécessaire pour adapter le fond et la forme du droit pénal à l'évolution rapide de la criminalité informatique. Cela implique non seulement une mise à jour régulière des lois existantes, mais aussi l'introduction de nouvelles dispositions spécifiques aux formes émergentes de cybercriminalité. La révision et l'enrichissement du cadre juridique doivent s'accompagner de mesures concrètes telles que la formation continue des magistrats, le renforcement des capacités techniques des services répressifs et la promotion de la coopération internationale.

En outre, la prévention de la criminalité informatique doit inclure des stratégies de sensibilisation et d'éducation du grand public et des entreprises, afin de renforcer la résilience de la société face aux cybermenaces. La collaboration entre le secteur privé et le gouvernement est essentielle pour partager les informations et les meilleures pratiques en matière de cybersécurité.

Enfin, une législation solide doit prévoir des mécanismes d'application efficaces, notamment des sanctions adaptées aux nouvelles formes de criminalité numérique et des procédures judiciaires souples permettant de réagir rapidement aux infractions. L'objectif ultime est de créer un environnement juridique dissuasif pour les cybercriminels, tout en protégeant les

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

droits et libertés des citoyens à l'ère numérique.

En conclusion, le législateur marocain doit adopter une approche proactive et anticipative pour combler les lacunes actuelles et prévenir l'impunité. Une mise à jour régulière du cadre législatif, combinée à des actions concrètes sur le terrain, est indispensable pour relever les défis posés par la criminalité informatique et assurer une protection efficace des systèmes de traitement automatisé de données et des informations qu'ils contiennent.

BIBLIOGRAPHIE

BIBENT, M. (2000). Le droit de traitement de l'information, Nathan. Paris.

BRISSET GIUSTINIANI, A. (2004). Aspects juridiques de l'émergence d'une sécurité européenne des réseaux et des systèmes d'information. Mémoire D.E.S.S. Droit de l'internet, université panthéon Sorbonne paris.

BUFFELAN, J.-P. (1988). La répression de la fraude informatique, Expertises, n° 103.

CROZE, H. (1988). L'apport du droit pénal à la théorie générale du droit de l'informatique (à propos de la loi n° 88-19 du 5 janvier1988 relative à la fraude informatique), JCP G.

DIK, A. (2017). La fraude informatique au Maroc. Edition dar Essalam.

Diyaâ Toumlilt, M. (2008). Le commerce électronique au Maroc : Aspects juridiques. Les éditions Maghrébines.

DUFLOT, F. (2003-2004). Les Infections Informatiques Bénéfiques. Mémoire du DESS de Droit du Numérique et des Nouvelles Techniques, Université Paris XI - Faculté Jean Monnet.

EL CHAER, N. (2004). La criminalité informatique devant la justice pénale, Edition SADER.

Fouad BENSEGHIR, F. (2010). Criminalité électronique. Futur objectif.

GASSIN, R. (1986). Le droit pénal de l'informatique, DS., Chron.

GIUDICELLI-DELAGE, G. (2004). Les transformations de l'administration de la preuve pénale. Perspectives comparées : Allemagne. Belgique. Canada. Espagne. Etats-Unis. France. Italie. Portugal. Royaume-Uni. Archives de politique criminelle, n° 26.

MARTIN, D. (1997). La criminalité informatique, P.U.F., 1è éd.

MARTIN, D. et Martin, F-P. (2001). Cybercrime : menace, vulnérabilités et repostes. P.U.F, collection criminalité internationale.

MEILLAN, E. (1993). La sécurité des systèmes d'information : les aspects juridiques, Hermès, Paris.

Mélanges en hommage au professeur Mohamed Jalal Essaid, 2005. CMEJ.

PRADEL, J. (1990). Les infractions relatives à l'informatique, Revue internationale de droit comparé. Vol. 42 N°2.

عبد السلام بن سليمان. (2017). الإجرام المعلوماتي في التشريع المغربي، دار الأمان.

REVUE DROIT & SOCIETE N°13, VOL 5, N° 13, AVRIL/ JUIN 2024

Rapports et mémoires :

DUFLOT, F. (2003-2004). Les Infections Informatiques Bénéfiques. Mémoire du DESS de Droit du Numérique et des Nouvelles Techniques, Université Paris XI - Faculté Jean Monnet.

FARIH, O. (2010-2012). Cadre conceptuel et théorique de la cybercriminalité. Master FSEJ de Fès.

GHAZALI Ahmed. Les Infrastructures critiques face au risque cybernétique, présentation lors d'un séminaire organisé le 27/03/2012 par l'IRES.

MAALAOUI, I. (2011). Les infractions portant atteinte à la sécurité du système informatique d'une entreprise. Mémoire en vue de l'obtention du grade de Maîtrise en droit, faculté de Montréal.

تقرير لجنة العدل و التشريع و حقوق الإنسان حول مشروع قانون رقم 07.03 يتعلق بتتميم مجموعة القانون الجنائي فيما يتعلق بالإخلال بسير نظم المعالجة الآلية، دورة أبريل 2003.

Jurisprudence marocaine :

Arrêt de la Cour d'appel de Casablanca en date du 02-12-1985.

Arrêt de la Cour d'appel de Rabat n° 3400 en date du 01/03/2010, dossier n° 751/2010/19.

Arrêt de la Cour d'appel de Rabat n° 633 en date du 26/03/2006, dossier numéro 461/05/22 (Inédit).

Arrêt de la Cour d'appel de Rabat n° 977 en date du 25/06/2006, dossier n° 861/06/26. (Inédit).

Arrêt de la Cour d'appel de Rabat n° 721 en date du 12/09/2006, dossier n° 600-06-22. (Inédit).

Arrêt de la Cour d'appel de Rabat n° 1203 en date du 13/12/2006, dossier n° 922/06. (Inédit).

Arrêt de la Cour d'appel de Rabat n° 300 en date du 23-09-2006, dossier n° 999-05-22.

Arrêt de la Cour d'appel de Rabat n° 1134 en date du 27-11-2006, dossier n° 499-06-26. (Inédit).

Arrêt de la cour d'appel de Rabat n° 37 en date du 26/01/2006, dossier n° 935/05/22 (inédit).

Arrêt de la cour d'appel de Rabat sans numéro en date du 11/09/2006, dossier n° 274/06/2009.

Arrêt de la cour d'appel de Rabat n° 364 en date du 17/04/2006, dossier n° 740/05/22 (Inédit).

Arrêt de la cour d'appel de Rabat numéro 633 en date du 26/06/2006, dossier numéro 461/05/22. (Inédit).

Arrêt de la Cour d'appel de Rabat n° 977 de la même cour en date du 25/09/2006, dossier n° 861/06/26 (Inédit).

Jugement du tribunal de première instance de Casablanca n° 4236-4 en date du 13/11/1985, dossier n° 235/18/85.

Jugement du tribunal de première instance de Casablanca en date du 11/07/2007, dossier n° 4331/2007 (inédit).

Jugement du tribunal de première instance de Temara n° 215 en date du 17/05/2010, dossier n° 220/10/2 (inédit).

Jugement du tribunal de première instance de Rabat n° 903 en date du 18/06/2012, dossier n° 850/2105/13 (inédit).

Jugement du tribunal de première instance de Rabat en date du 13/03/2014, dossier n° 4603/2106/13 (inédit).

Jugement du tribunal de première instance de Rabat en date du 09/20/2015, dossier n° 4603/2106/13 (inédit).

Jugement du tribunal de première instance de Kenitra sans numéro en date du 18/05/2009, dossier n° 2468/09. (Inédit).

Jugement du tribunal de première instance d'Agadir n° 148 en date du 30/01/2012, dossier n° 97/2012.

Jugement du tribunal de première instance sans numéro en date du 18/05/2009, dossier numéro 2468/09. (Inédit).

Jugement du tribunal de première instance de Rabat n° 701 en date de 17/05/2010, dossier numéro 21-767-10. (Inédit).

Jugement du tribunal de première instance de Mohammedia en date du 28/01/2011, dossier 11-2- 4617 (inédit).

Jugement du tribunal de première instance de Mohammedia n° 461, en date du 06/05/2011. (Inédit).

Jugement du tribunal de première instance de Rabat n° 1861 en date du 21/12/2015, dossier n° 1836/2105/2015. (Inédit)

Jugement du tribunal de première instance de Rabat n° 758 en date du 27/05/2016, dossier n° 714/2105/2016. (Inédit)

Jurisprudence française :

Trib. corr. Limoges, 14 mars 1994, Expertises 1994, p. 238, obs. Teboul.

TGI, Vannes, 13 juillet 2005 : Juris-Data n° 294765.

Trib. Corr. Brest, 14 mars 1995, LPA. 28 juin1995, n°77, note Choisy.

REVUE DROIT & SOCIETE
N°13, VOL 5, N° 13, AVRIL/ JUIN 2024