Revue Internationale du Chercheur
ISSN : 2726 - 5889
Volume 4 : Numéro 4

LES CONTRATINTES RELATIVES AUX PROCÉDURES D'INVESTIGATION SUR LES CYBERCRIMES

CONTRACTS RELATING TO CYBERCRIME INVESTIGATION PROCEDURES

HALIMI Dalal

Enseignant chercheur
École Nationale de Commerce et de Gestion
Université Chouaib Doukkali à El Jadida
Laboratoire d'études et de recherches en sciences et en management
Maroc
halimi.d@ucd.ac.ma

Date de soumission : 27/07/2023

Date d'acceptation : 18/12/2023

Pour citer cet article :

HALIMI D. (2023) «LES CONTRATINTES RELATIVES AUX PROCÉDURES D'INVESTIGATION SUR LES CYBERCRIMES», Revue Internationale du chercheur «Volume 4 : Numéro 4» pp : 237- 262

Résumé

La particularité des atteintes numériques exige une mise à jour appropriée quant au cadre répressif et procédural des infractions réalisées sur le cyberespace. En effet, afin d'assurer une protection efficace en matière de cybersécurité, la procédure de recherche et de constatation des preuves numériques en la matière doit s'adapter à la technicité et la particularité de la cybercriminalité, de sorte qu'elle permettra à la police judiciaire d'accomplir ses investigations malgré la complexité des cyberattaques.

Mots clés :

Procédés d'investigation, preuve numérique, juge d'instruction, perquisition et saisie des données numériques, procès-verbal, support numérique, etc.

Abstract

The particularity of digital infringements requires an appropriate updating of the repressive and procedural framework of offenses carried out in cyberspace. In fact, in order to ensure effective protection in terms of cybersecurity, the procedure for researching and recording digital evidence in this area must adapt to the technicality and particularity of cybercrime, so that it will allow the judicial police to carry out their investigations despite the complexity of cyberattacks.

Keywords :

Investigative procedures, digital evidence, examining magistrate, search and seizure of digital data, minutes, digital media, etc.

Introduction

Face aux infractions classiques, en général ce sont les procédures d'investigation pénale générale qui sont applicables, tout en considérant les circonstances dans lesquelles ces crimes ont été réalisés, qu'il s'agisse de dénonciation, de collecte des éléments de preuves du lieu de crime ou de formation des cellules d'investigation, etc. En revanche, la particularité des crimes relevant de la cybernétique a exigé l'adaptation des procédures en question à cette mutation.

Dans le dessein d'accompagner la progression incessante des TIC, les procédés de recherche et d'investigation se sont confrontés à une réalité qui incite le législateur à les adapter en fonction de la nature des données objet d'enquête pour pouvoir faire prévaloir les preuves informatiques conservées en tant que preuves admissibles devant la justice. L'aspect technique des cybercrimes a rendu la tâche encore plus difficile quant à l'utilisation des procédures classiques, parce que nous nous trouvons devant des atteintes qui nécessitent l'assistance d'autres corps capables de faciliter le côté technique des procédures d'investigation au juge d'instruction pendant l'enquête en cours.

Considéré comme l'un de ces procédés, l'expertise qui est une preuve indépendante en elle-même qui repose sur la recherche et l'étude de la présomption. En effet, en matière des cybercrimes, cette expertise exige de la part d'un expert, de disposer d'un savoir préalable et technique sur les atteintes aux systèmes de traitement automatisé, en raison de la technicité des preuves à fournir en cas de constatation d'un cybercrime, puisque l'autorité compétente se trouve confrontée à l'application des dispositions légales sur des atteintes où le juge est tenu de prendre en considération ce trait technique de l'infraction avant de se prononcer sur de tels méfaits.

L'application des dispositions spécifiques relatives à la phase d'investigation concerne celles dédiées aux procédures de conservation, perquisition et saisie des données automatisées en matière des cybercrimes, portent sur tout un processus qui débute avec la collecte des données stockées sur le système automatisé du cyberdélinquant en temps réel jusqu'à la conservation des données électroniques perquisitionnées et saisies pendant l'investigation préliminaire. Cette démarche permet à la police judiciaire, en particulier la police technique et scientifique de rassembler l'ensemble des éléments qui permettront la condamnation du cybercriminel sur

la base de preuves électroniques considérées en tant que preuves dotées de force probante en matière pénale. Selon C. JALBY : « Si elle[1] se rattache incontestablement à la mission de police judiciaire, son périmètre demande à être précisé, car il diffère selon les pays. En France, son champ d'intervention, réduit d'abord à la seule criminalistique, s'est peu à peu étendu à la documentation criminelle […] a pour mission de découvrir, prélever, exploiter les traces et indices dans les enquêtes judiciaires, en utilisant toutes les ressources offertes par la technique ou la science, dans le but d'apporter la preuve du crime ou du délit et d'en identifier le ou les auteurs […].» (JALBY, 2010 :3). En effet, la particularité des procédés adoptés durant la phase d'investigation c'est ce qui contribue dans l'accomplissement d'un procès équitable tant envers les victimes des atteintes numériques qu'envers les auteurs des infractions en question.

Ceci dit, nous allons mettre en exergue la particularité des procédures d'investigation en matière des cybercrimes. Nous aborderons dans un premier lieu, les procédés d'investigation sur le plan international**,** avant de nous pencher sur les procédures d'investigation sur le plan interne**,** dans un second lieu.

1. Les procédés d'investigation sur le plan international

La convention de Budapest dans son article 16 porte éclairage sur la possibilité d'ordonner ou d'obtenir la conservation rapide des données informatiques stockées dans des systèmes de traitement automatisés faisant objet d'enquête ou de procédure pénale spécifiées et dont jouissent les autorités nationales des États parties à cette convention. L'utilisation du terme « conservation » dans l'alinéa premier dudit article laisse à présumer que les données en question existent déjà sur le système de stockage et sont bien conservées et protégées contre toute modification, dégradation de leur état actuel et leur qualité, détérioration ou de tout effacement. Cette conservation ne signifie pas forcément que ces données ou leurs copies sont inaccessibles ni utilisables, mais la personne à laquelle l'injonction a été adressée peut conserver l'accès aux dites données en fonction des spécifications précises par cette première. Bien que cet article ne détermine pas la façon dont ces données doivent être conservées, cependant, il précise que chaque État est appelé à établir ses propres mesures de conservation à condition qu'elles soient appropriées et de préciser si la conservation de certaines données ne devrait en plus comporter le blocage de celles-ci. L'autorisation dont bénéficie la police ou

[1] Not. La police technique et scientifique.

le parquet qui peuvent mettre en œuvre d'autres moyens juridiques de conservation que l'injonction judiciaire ou administrative voire même une instruction.

Il arrive que dans certains États, leur droit procédural ne prévoie pas d'injonctions de conservation, ce qui ouvre la marge de conserver lesdites données soit par la perquisition et la saisie soit par injonction de produire. L'importance d'ordonner de telles mesures à la personne objet de cette injonction permet la rapidité de l'intervention de ce destinataire, ce qui par conséquent permettra l'application rapide des mesures de conservation. Les données concernées par ce procédé peuvent ou bien être en possession de l'intéressé ou mises ailleurs tout en restant sous son contrôle. Cette personne est obligée de conserver et protéger l'intégrité de ces données aussi longue que nécessaire à condition que ladite durée ne dépasse pas 90 jours, pour permettre à l'autorité compétente d'obtenir leur divulgation. (Conseil de l'Europe, 2001 :37).

De surplus, il est possible pour les États parties à cette convention, aux fins d'obtenir la conservation rapide de données électroniques stockées dans un système informatique valable pour une période de 60 jours, de permettre à l'État requérant la soumission d'une demande afin de perquisionner, d'accéder, de saisir ou de divulguer ces données (convention de Budapest, 2001 : art. 29 al. 1r), à condition de respecter l'obligation de confidentialité relative à la mise en œuvre des procédures de conservation rapide de données stockées. Le fait d'imposer cette condition de secret sur la mise en œuvre desdites procédures, permettra d'éviter que d'autres personnes animées de mauvaise foi puissent tenter de manipuler ou d'effacer ces données, puisque cette discrétion non seulement elle facilit la réalisation des procédures en question, mais encore, elle contribue à la défense du droit de la vie privée de la personne concernée ou des autres personnes pouvant être mentionnées ou identifiées dans ces données. Ainsi, nous allons s'intéresser sur l'ensemble des mesures mises en œuvre :

1.1. La mesure de conservation et divulgation rapide des données liées au trafic

L'obtention de données relatives au trafic stockées en matière des communications antérieures est essentiel pour déterminer la source ou la destination de ces communications ce qui est primordial pour identifier les personnes responsables de l'entrave du bon fonctionnement du système informatique, de l'accès non autorisé audit système ou même

la divulgation des données sauvegardées. Toutefois, la seule entrave à cette démarche est le fait de ne pouvoir stocker ces données pour une longue durée sans avoir à porter atteinte au droit du respect de la vie privée des utilisateurs. Il arrive parfois que plusieurs fournisseurs de services s'occupent de la transmission de la même communication.

Chaque fournisseur peut conserver certaines données relatives au trafic ayant un rapport avec la transmission de la communication spécifiée, qui ont soit été produites et archivées par ce fournisseur lors du passage de la communication par son système, soit ont été fournies par d'autres fournisseurs.

Ces données relatives au trafic, ou tout au moins certains types de données liées au trafic, peuvent être parfois partagées entre les fournisseurs de services ayant participé à la transmission de la communication, à des fins commerciales, sécuritaires ou techniques. Dans de telles circonstances, l'un ou l'autre peut posséder les données relatives au trafic essentiel pour déterminer la source ou la destination de la communication. Souvent, aucun fournisseur ne possède à lui seul suffisamment de données afin de permettre la détermination avec exactitude de la source ou la destination de ladite communication. Ainsi, chacun se trouve en possession de certaines parties du puzzle ce qui signifie que chacune de ces parties doivent être examinées dans le but d'identifier la source ou la destination. De ce fait, il est indispensable de procéder rapidement à la conservation desdites données auprès de tous les fournisseurs. Comme les données en question ne sont pas divulguées aux autorités compétentes pendant l'émission de l'injonction à un fournisseur de services, ces autorités ignorent si ces fournisseurs disposent de toutes les données relatives au trafic nécessaire ou si d'autres fournisseurs ont participé à cette transmission. Par conséquent, il est impératif que le fournisseur ayant reçu l'injonction de conservation soit tenu de divulguer rapidement aux autorités compétentes ou par d'autres personnes désignées par celles-ci toute donnée susceptible de faciliter l'identification d'autres fournisseurs de services et du procédé utilisé aux fins de transmission de la communication en question.

1.2. La mesure d'injonction de produire

La mise en œuvre de la mesure d'injonction de produire par l'autorité répressive notamment, dans les cas où il n'est pas nécessaire de recourir à une mesure plus contraignante, voire même plus onéreuse, s'avère être encore plus utile vis-à-vis des tiers

gardiens des données tels que les fournisseurs d'accès à internet. Ils collaborent volontairement avec les services chargés de la lutte contre la cybercriminalité en leur fournissant les données dont ils ont besoin et sous leurs contrôles en contrepartie d'une décharge de toute responsabilité contractuelle ou autre. En principe, toute partie doit veiller à ce que les autorités répressives compétentes en la matière aient le pouvoir d'ordonner, à une personne présente sur son territoire de communiquer des données informatiques spécifiées, stockées dans un système automatisé ou un support de stockage qui sont en possession matérielle de ces données ou qui se trouvent sous son contrôle, d'une part. D'autre part, de demander à un fournisseur de services qui propose des prestations sur son territoire, de leur transmettre l'ensemble des données informatiques matérielles des abonnés bénéficiant de leurs prestations et services qui se trouvent en leur possession ou qu'elles sont stockées à distance. (Convention de Budapest, art. 18)

Par ailleurs, lesdites autorités ne peuvent disposer de ces données que s'il s'agit de données publiques que les abonnés autorisent leur divulgation et non confidentielles. Ainsi, chaque État peut prescrire des choix différents quant aux conditions à prévoir à propos de la communication des informations des internautes et ce en fonction de leur droit interne, il peut s'agir par exemple des modalités de production, des données informatiques ou des informations relatives à l'abonné de la manière spécifiée dans l'injonction. Elles pourraient ainsi mentionner le délai dans lequel la divulgation doit intervenir ou la forme sous laquelle les données doivent être divulguées.

En plus, les fournisseurs de services sont habilités à utiliser le compte de l'abonné et toutes les informations qui se rapportent à leurs abonnés qui bénéficient de leurs services et qui couvrent une large tranche de bénéficiaires. Ceci dit, la collecte des informations des abonnés est nécessaire dans deux situations. *À priori*, elles sont primordiales pour déterminer dans un premier lieu, les services et les mesures techniques connexes qui ont été utilisés ou sont utilisés par un abonné, comme le type de service téléphonique utilisé, le type de services connexes utilisés, le numéro de téléphone ou toute autre adresse technique telle que les adresses électroniques. Dans un deuxième lieu, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé, son adresse postale ou géographique et le numéro de téléphone de cet utilisateur (tel que les informations d'ordre commercial figurant dans les dossiers de

facturation et de paiement de l'abonné, etc. Elles peuvent également, être utiles aux enquêtes pénales en particulier, lorsque l'infraction faisant l'objet de l'enquête est liée à un cas de fraude informatique un autre délit économique) et ce, tout en vérifiant l'exactitude de ces informations. En évidence, ces informations ne se limitent pas à celles directement liées à l'utilisation du service de communication, mais le dépasse largement jusqu'aux données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou arrangement de service entre l'abonné et son fournisseur de services. Elles désignent en outre, toute autre information sauf, celles relatives au trafic ou au contenu, liée à l'endroit où se trouvent les équipements de communication, information disponible sur la base d'un contrat ou arrangement de services, une relation dont profite largement l'abonné vis-à-vis de son fournisseur de services.

1.3. La mesure de perquisition et de saisie des données stockées

Nous constatons que les dispositions de l'article 19 de la convention sur la cybercriminalité ciblent la modernisation et l'harmonisation des législations internes en matière de perquisition et saisie de données électroniques stockées susceptibles d'être considérées en tant que preuves dans les enquêtes en cours ou des procédures pénales spécifiques de chaque État adhérent à la convention de Budapest.

Dans le cadre de la perquisition d'ordre traditionnel portant sur des dossiers ou des documents, une perquisition repose sur le recueil des informations qui ont été consignées ou enregistrées dans le passé sous une forme matérielle – format papier – les enquêteurs perquisitionnent ou inspectent lesdites données ainsi enregistrées et saisissent ou emportent physiquement des dossiers tangibles considérés en tant que preuves. La collecte des données se produit durant la perquisition et porte sur les données existantes à ce moment-là. En effet, afin d'obtenir l'autorisation légale de procéder à une telle perquisition, la seule condition exigée est l'existence de raisons de penser que de telles données existent dans un endroit précis et qui sont susceptibles de prouver qu'une infraction pénale spécifique a été commise, en considération de la législation interne du pays concerné et des dispositions relatives à la défense des droits de l'Homme.

Néanmoins, la recherche des informations électroniques nécessite des dispositions procédurales complémentaires afin de permettre l'obtention de ces données de façon efficace

que la perquisition classique des informations sous support matériel. Ceci peut s'expliquer par plusieurs raisons, premièrement, lesdites données revêtent une forme tangible. Deuxièmement, les données en question peuvent être lues grâce à un matériel numérique, mais ne peuvent pas être saisies et emportées de la même manière qu'un document support papier. Cette forme tangible sur laquelle les données immatérielles sont stockées doit être saisie et emportée ou une copie au moins doit être faite sous forme soit matérielle (par exemple le support imprimé), soit immatérielle sur un support tangible, avant que le support matériel qui contient ladite copie ne puisse être saisi et emporté. Dans les deux dernières positions, donnant lieu à la copie des données en question, les données originelles restent dans le système automatisé ou le dispositif de stockage à savoir la mémoire. Troisièmement, dû à la connectivité des systèmes de traitement automatisés, les données électroniques peuvent ne pas être stockées sur le système faisant objet de perquisition, cependant il est facile d'y accéder via cet ordinateur. Ainsi, elles pourraient être stockées ailleurs dans un dispositif de stockage lié directement au système de traitement automatisé ou indirectement connecté à l'ordinateur grâce au réseau d'Internet. À la différence de la perquisition classique, la perquisition informatique exige le plus souvent, non seulement la saisie du système informatique, mais encore tout support de stockage apparenté comme les disquettes, clé USB, CD, etc., qui se trouvent à proximité de l'ordinateur objet de perquisition, ce qui explique l'habilitation d'ordre global dont jouissent les autorités compétentes. Les autorités compétentes sont habilitées à étendre la perquisition et la saisie de données par une méthode similaire à un autre système de traitement automatisé ou seulement à une partie de celui-ci, du moment que les autorités soupçonnent que les données qui les intéressent se trouvent sur l'autre ordinateur, mais à condition que ce système se situe sur son territoire.

Dans le même ordre d'idée, l'expression *« saisir »* mentionnée dans la convention sur la cybercriminalité signifie : d'emporter le support physique (l'ordinateur) dans lequel les données ou les informations sont stockées, réaliser ou conserver une copie de ces informations ou données. En outre, ce terme implique également, l'utilisation ou la saisie des programmes nécessaires pour accéder aux données saisies. Par contre, l'emploi du terme *« moyen similaire »* fait référence aux autres manières d'enlever des données immatérielles, de les rendre inaccessibles ou d'en prendre le contrôle d'une autre façon dans l'environnement cybernétique. Étant donné que les mesures concernent des données intangibles stockées, les autorités compétentes sont appelées lors de leur contrôle, à veiller

à ce que les données copiées ou enlevées soient impérativement conservées dans l'état où elles ont été trouvées au moment de la saisie et non modifiées pendant la procédure pénale ce qui préservera par conséquent leur intégrité.

Par contre, l'expression « enlever » traduit l'éventualité dans laquelle si ces données sont enlevées ou rendues inaccessibles, elles ne seront pas détruites et continueront d'exister sur le système informatique perquisionné. La personne suspecte est temporairement privée de l'accès à ces données. Cependant, ce droit peut lui être restitué vers la fin de l'enquête ou de la procédure pénale. Nous constatons donc, que la saisie ou l'obtention de données par un moyen similaire à deux principales fonctions : premièrement, à collecter des preuves en copiant les données par exemple et deuxièmement, à confisquer les données, en les copiant et en rendant postérieurement la version originelle inaccessible ou en l'enlevant. La saisie n'implique pas un effacement définitif des données saisies, c'est juste que grâce aux logiciels informatiques leur existence sur le système devient invisible.

Partant de la constatation qu'il peut y avoir lieu de consulter les administrateurs de système, qui le connaissent bien sur la meilleure manière de mener la perquisition, les services de lutte contre la criminalité sont habilités en tant qu'autorité compétente d'obliger un administrateur expert et compétent dans son domaine, à coopérer avec eux. La notification aux parties intéressées sur le déclenchement d'une procédure de perquisition est laissée à l'appréciation du droit interne. Dans une telle situation si les parties envisagent d'établir un système de notification obligation aux personnes intéressées, il faudrait ne pas perdre de vue que cette notification risque de nuire au bon déroulement de l'enquête en cours. En présence d'un tel risque, il conviendrait d'envisager par les autorités compétentes l'ajournement de cette mesure.

1.4. La collecte en temps réel des données numériques et leur interception

Le concept de la collecte en temps réel des données ayant un lien étroit avec le trafic et sur l'interception en temps des données liées au contenu associé à des communications transmises via un système de traitement automatisé réalisé soit par les soins des autorités compétentes ou par les fournisseurs de services. Certes, la démarche d'interception de télécommunications concerne en principe les réseaux de télécommunications classiques.

Ces réseaux peuvent comprendre des infrastructures câblées comme ils peuvent comprendre des interconnexions avec des réseaux sans fil dont les systèmes de téléphonie mobile, et les systèmes de transmission par micro-ondes. De nos jours, les communications mobiles sont facilitées par un système dit de réseaux satellitaires spécialisés. Dans ce sens, les réseaux informatiques peuvent prendre la forme d'une infrastructure câblée fixe indépendante, mais, il arrive plus souvent qu'ils soient exploités sous forme d'un réseau virtuel grâce à des connexions réalisées via d'infrastructures de télécommunications, ce qui facilite la création des réseaux informatiques ou des réseaux dits de réseaux d'ampleur mondiale. La convergence des TIC brouille les distinctions entre télécommunications et téléinformatiques et les spécificités de leurs infrastructures. Les deux articles 20 et 21 de la convention sur la cybercriminalité s'appliquent de ce fait à des communications pouvant être transmises par le biais d'un réseau de télécommunications avant d'être reçues par un autre système informatique.

Par ailleurs, la collecte de preuves contenues dans des communications en cours de production et collectées au moment de la transmission de ladite communication ne perturbe pas manifestement la circulation des données puisque la communication atteint son destinataire et au lieu de procéder à une saisie physique des données, les autorités compétentes y font une copie des données en cours de transmission. Par la suite, leur collecte est effectuée pendant une période donnée. Mais, lorsqu'il est question d'un événement futur c'est-à-dire une future transmission des données, un mandat est exigé pour autoriser la collecte de ces données. De nombreux États présentent une distinction entre l'interception en temps réel de données liées au contenu et la collecte en temps réel de données relatives au trafic d'un point de vue relatif aux conditions juridiques devant être préalablement réunies pour autoriser une telle mesure d'enquête et des infractions à cause desquelles nous pouvons recourir à cette mesure. Tout en admettant que les deux types de données puissent porter atteinte aux intérêts de nature privée, beaucoup de parties considèrent qu'en matière des données relatives au contenu, ces intérêts sont supérieurs en raison même de la nature du message ou du contenu de la communication ce qui justifie que la collecte de données relatives au contenu peut donc faire l'objet de restrictions par rapport aux données relatives au trafic.

À propos de l'interception en temps réel des données relatives au contenu, le dispositif législatif prévoit souvent que le recours à cette mesure n'est envisageable que dans le cadre d'une enquête ouverte sur une infraction réputée comme étant grave ou appartenant à une catégorie d'infractions graves. La loi interne les identifie comme étant graves, à ce titre en les listant avec les infractions à laquelle la mesure peut être appliquée ou en se référant à une certaine peine d'emprisonnement maximale dont l'infraction est punissable afin de les écarter d'une telle catégorie, chose que l'article 21 dispose expressément lorsqu'il souligne que les États ne sont tenus d'instaurer cette mesure qu'en « relation avec de graves infractions à définir dans le droit interne. »

Par contre, les dispositions de l'article 20, qui porte éclairage sur la collecte des données relatives au trafic ne soulèvent pas les mêmes limites et s'étendent en principe, à toute infraction d'ordre pénal ciblée par la convention. En effet, chaque partie peut se réserver le droit de faire opposition à cette mesure qu'en matière d'infractions ou catégories d'infractions spécifiées dans la réserve. La seule condition exigée qu'elles ne soient pas plus réduites que celui des infractions auxquelles elle applique la mesure d'interception des données relatives au contenu.(Convention de Budapest, 2001 : art.14 al.3) Autrement dit, l'État qui adopte une pareille réserve doit prévoir une possibilité de la limiter de sorte à permettre la mise en application de la mesure de collecte des données relatives au trafic le plus largement possible.

Pour certaines parties, les infractions traitées par la convention sur la cybercriminalité ne sont normalement pas considérées comme suffisamment graves pour donner lieu au mécanisme d'interception. Quoi qu'il en soit, ces techniques de collecte et d'interception de données informatiques sont souvent indispensables pour l'enquête ouverte sur certaines infractions créées dans le cadre de la convention de Budapest, notamment celles relatives à l'accès illicite aux STAD[2], la diffusion de virus, etc. Il arrive, parfois, que la source de l'intrusion ou de la diffusion ne puisse pas être identifiée sans avoir recours à la collecte en temps réel de données relatives au trafic.

D'un autre point de vue, c'est grâce à l'interception en temps réel des données relatives au contenu que la nature de la communication ne peut être découverte. Ces infractions par leur nature nécessitent l'utilisation de technologies informatiques,

[2] Acronyme de systèmes de traitement automatisé des données.

dont le recours aux moyens technologiques devrait être autorisé pour enquêter. Mais, la question de l'interception peut soulever des problèmes délicats et c'est la raison pour laquelle la convention accorde la portée de cette mesure à l'appréciation du droit interne de chaque partie. Certains États assimilant juridiquement les deux mesures offrent une option de réserve qui offre une autorisation afin de restreindre l'applicabilité de la collecte des données numériques en temps réel, mais cette applicabilité ne doit pas être réduite davantage que celle liée à la restriction de l'interception en temps réel des données relatives au contenu. Sauf que les États devraient envisager d'appliquer ces deux mesures, aux infractions créées dans la Convention pour offrir un moyen efficace aux autorités habilitées d'enquêter sur ces infractions et aux infractions en relation avec les systèmes de traitement automatisé.

Étant donné que l'interception des données relatives au contenu constitue une mesure très intrusive sur le plan de la vie privée, il est primordial d'instaurer des mesures impératives de sauvegarde pour préserver un équilibre approprié entre les intérêts de la justice et les droits fondamentaux des internautes. Dans le cadre d'une interception, nous constatons que la convention sur la cybercriminalité n'énonce pas de sauvegardes spécifiques si ce n'est qu'elle limite l'autorisation de l'interception des données aux enquêtes ouvertes sur des infractions pénales graves définies dans le droit interne. (Conseil de l'Europe : 35)

2. Les procédures d'investigation sur le plan national

Le législateur répressif bien qu'en adoptant les procédures classiques poursuivies à l'égard des crimes traditionnels, a fait en sorte d'adapter l'application des règles procédurales afin qu'elles puissent s'étendre au cyberespace, même si le fait d'utiliser une telle approche peut également être considéré comme un facteur d'insécurité juridique susceptible de former un juste motif pour contester la légalité des pièces à conviction rassemblées pendant une enquête et par conséquent, affecter leur recevabilité en tant que preuves irréfutables.

2.1. L'appel à des experts dans les enquêtes liées aux cybercrimes

La difficulté à laquelle sont confrontées les forces de l'ordre a imposé l'intervention des experts en matière des TIC. Cette assistance se traduit en particulier, dans le volet technique des cybercrimes que l'article 64 de la procédure pénale marocaine soulève,

notamment, en précisant le cadre de leur intervention dans les enquêtes soumises au soin des forces de l'ordre. En effet, en vertu de cette disposition (L. 22-01, art. 64), le recours de la police judiciaire aux experts comme étant des personnes assermentées et qualifiées dans leur domaine pour les assister au niveau des constatations lors d'une enquête en cours, n'est envisageable qu'avec l'accord du juge d'instruction à qui revient la direction des opérations de constatations des lieux entamées par les agents de la police judiciaire même en présence du procureur général du Roi ou le procureur du Roi. Il est habilité à ordonner aux agents présents de poursuivre les constatations, une fois achevées, il est tenu de les fournir sous forme des pièces d'enquête soit, au procureur général du Roi, soit au procureur du Roi « à toutes fins utiles». (L. 22-01, art. 75 al. 3) Ainsi, au cours des investigations, les experts se chargent durant ce processus des missions suivantes :

2.1.1. La conservation des supports contenant des preuves informatiques ou sur le net

L'utilité de l'intervention d'un expert en matière informatique lors des enquêtes liées à la cybercriminalité se manifeste par leur subtilité quant au traitement des matériels et des données saisies. En raison de la fragilité des données qui se trouvent sur le support de stockage original (CD, Disque dur interne, clé USB, etc.,) qui feront objet de copies afin d'être traitées par la suite. À l'évidence, pendant un accès à un système de traitement automatisé, l'utilisateur risque, sans l'avoir prémédité, de modifier le contenu de l'ordinateur en question, ce qui justifie la délicatesse avec laquelle le spécialiste doit procéder, chose « qui entre dans les cordes de l'expert en informatique. » (النوازلي، 2013 :379) Les agents assermentés sont appelés à copier les données figurant sur le support numérique en deux exemplaires si le matériel perquisitionné va être laissé sur les lieux et seulement en une seule copie si l'on procède à sa saisie.

2.1.2. La recherche des preuves numériques sur les supports informatiques ou sur le net

À ce stade, la recherche de preuves numériques doit être exécutée dans de bonnes conditions à travers l'utilisation des logiciels d'investigation spécialisés, comme « *EASY*

Recovery»[3] , c'est pourquoi les données ciblées ne doivent surtout pas être modifiées lors de la perquisition, puisque l'expert est tenu de se focaliser sur une copie parfaite (au sens binaire) des données, et ce sans altérer en aucune manière le système ou les données originales. Ces données, bien entendu, ne doivent pas être modifiées comme ce serait le cas en utilisant simplement l'interface graphique mise à disposition par la plupart des systèmes d'exploitation pour naviguer dans les arborescences de fichiers.

Il appartient donc, à l'expert en *« Computer forensics: the process of uncovering and interpreting electronic data. The main goal of this process is to 'preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past event.»* [4], de prouver la non-altération des preuves (données originales recueillies, en plus des copies traitées et analysées). Après avoir identifié et défini sa stratégie de collecte et de préservation des données visées, le spécialiste en informatique procédera désormais à une analyse des données en question (certaines de ces tâches sont en fait du « *Hacking* »), comme l'analyse des fichiers et de leurs métadonnées telles que les e-mails, historiques de navigation internet etc. L'analyse de données brutes, le cassage des mots de passe ou la construction et analyse de la ligne temporelle dite « *Timeline* »[5] et la documentation des découvertes.

Et enfin, viennent l'étape de production des preuves et leur présentation. De ce fait, l'ensemble des preuves jugées suspectes ont bien été rassemblées et documentées. Cette phase exige de la part du spécialiste, la production des preuves allant dans le sens

[3] Not. Il s'agit d'un programme complet de récupération et réparation de fichiers. Il est équipé d'un outil de diagnostic permettant ainsi la vérification de l'état du support où se trouvent les données perdues. Grâce à son moteur puissant, il permet de récupérer les données perdues sur un disque dur ou sur un autre support numérique. Il donne également, la possibilité de réparer les fichiers, comme par exemple les fichiers Word, Access, Outlook ou encore les fichiers zip : https ://www.over-blog.com/Ou_telecharger_Easy_Recovery_et_a_quoi_sert_ce_logiciel-1095203942-art295170.html.

[4] Not. Il s'agit de : « processus de découverte et d'interprétation des données électroniques. L'objectif principal de ce processus est de « préserver toute preuve dans sa forme la plus originale tout en menant une enquête structurée en collectant, en identifiant et en validant les informations numériques dans le but de reconstruire des événements passés » : https://www.cleverfiles.com/howto/computer-forensic.html

[5] Not. Ce concept en anglais fait référence à l'historique des actions réalisées, recoupage entre de diverses applications en plus des événements dans le système : http://igm.univ-mlv.fr/~dr/XPOSE2013/Digital_Forensic/computerf.html

des directives de l'agent de la police judiciaire sur la base de son rapport technique qui résulte des outils techniques (logiciels) utilisés. L'utilisation de tels outils facilite la tâche pour les autorités compétentes pendant l'élaboration du procès. Cette démarche garantit l'analyse et l'étude du matériel confisqué. Ils différent en fonction du matériel, et du fait que chacun d'entre eux exige l'utilisation d'un logiciel bien précis, puisque le matériel en question, peut être soit un téléphone mobile, soit un smartphone ou même un ordinateur personnel, etc., et donc, les experts en informatique ou les consultants en analyse dans ce domaine savent l'utilité de chaque logiciel dans cette procédure.

2.2. Les procédures d'instruction à la lumière de la loi n°53-05

La loi n°53-05 relative à l'échange électronique de données juridiques prévoit un cadre juridique qui soulève la compétence des membres d'un corps bien précis. Ils sont habilités à chapeauter le processus des procédures grâce à leur savoir et leur compétence en matière informatique et procédurale de pouvoir, aussi bien assister les agents de la police judiciaire en cas de cybercriminalité. Conformément à son article 41, ses dispositions soulignent en effet, le pouvoir de contrôle des agents de l'autorité nationale qui sont habilités à veiller sur la procédure liée à la recherche et la constatation par PV en conformité avec les règles du droit commun en cas d'atteintes aux données juridiques, durant l'échange électronique des documents professionnels, soit en faisant des copies, soit en recueillant et saisissant lesdits documents sur place ou après convocation des personnes intéressées par l'enquête en cours. Elles déterminent également, un délai de cinq jours afin de transmettre lesdits procès-verbaux au procureur du Roi, tout en respectant les moyens de cryptographie cités dans son article 12. Le législateur par la même occasion, a essayé de mettre en place un cadre procédural qui réglemente la compétence des agents de l'autorité nationale qui sont appelés à assister les officiers, les agents de la police judiciaire et les agents de douanes dans leur domaine de compétence, dans la collecte et la saisie de tout élément passible de servir l'enquête ouverte.

De même, pour l'intervention du gouvernement en matière de désignation des personnes morales du droit public pour émettre et délivrer des certificats électroniques sécurisés. L'article 43 de la loi en vigueur constitue une base légale à partir de laquelle le législateur a consacré tout un chapitre pour « les sanctions, les mesures préventives et de la constatation des infractions » au niveau des articles 29 à 40. Ainsi, il a porté éclairage sur une

variété d'atteintes, dont nous citons de prime abord, la fourniture des prestations de services de certification électronique sécurisée sans être agréé ou de continuer cette activité malgré le retrait de l'agrément ou d'émettre, délivrer ou gérer des certificats électroniques sécurisés en violation des dispositions de l'article 20 de la même loi . Deuxièmement, la divulgation ou l'incitation ou la participation à la divulgation des informations qui sont confiées à quiconque, dans le cadre de l'exercice de ses activités ou fonctions, notamment, « la divulgation du secret professionnel » (السائح. 2015 :239) et dont l'auteur de l'infraction est passible d'une peine d'emprisonnement d'un mois à six mois et au paiement d'une amende de 20.000 à 50.000 dirhams. Troisièmement, de faire sciemment de fausses déclarations ou de remettre de faux documents au prestataire de services de certification électronique (L. 53-05, art. 31) .Quatrièmement, d'importer, d'exporter, de fournir, d'exploiter ou d'utilise l'un des moyens ou d'une prestation de cryptographie sans la déclaration ou l'autorisation exigée aux articles 13 et 14 de la présente loi (L. 53-05, art. 32). Cinquièmement, d'utiliser un moyen de cryptographie pour préparer ou commettre un crime ou un délit ou pour en faciliter la préparation ou la commission. Sixièmement, de commettre une faute intentionnelle ou négligence par les personnes fournissant des prestations de cryptographie à des fins de confidentialité et qui sont responsables du préjudice causé en cas d'atteintes à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions. Septièmement, d'utiliser de manière illégale, les éléments de création de signatures personnelles relatifs à la signature d'autrui. Huitièmement, de ne pas respecter l'obligation d'information de l'autorité nationale prévue à l'article 23 de la présente loi par tout prestataire de services de certification électronique. Neuvièmement, de continuer à utiliser un certificat électronique arrivé à l'échéance ou révoqué par tout titulaire d'un certificat électronique. Et dixièmement, d'utiliser indûment par tout individu, une raison sociale, une publicité et de manière générale, toute expression faisant croire qu'il est agréé.

Ainsi, la particularité qui caractérise les procédures dans le domaine cybernétique, c'est que la loi en vigueur prononce des sanctions plus graves à l'égard des personnes morales, par rapport des peines consacrées aux personnes physiques (peines privatives de liberté et/ou paiement des amendes). Elle prévoit à leur encontre des sanctions destinées soit à la confiscation partielle des biens, soit, à la confiscation « des objets et choses dont la fabrication, l'usage, le port, la détention ou la vente constitue une infraction, même s'ils appartiennent à un tiers et même si aucune condamnation n'est prononcée» (code

pénal marocain, art. 89) ou liée à la fermeture des établissements de la personne morale ayant servir à commettre les infractions susmentionnées en dessus.(L. 53-05, art. 40)

2.3. Les procédures d'instruction à la lumière de la loi n° 09-08

À travers les dispositions de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, le législateur marocain a mis en place un certain nombre de dispositions qui se rapportent à la procédure pénale marocaine, afin d'assurer la protection des internautes à ce niveau d'une part et de mettre en œuvre des procédures susceptibles de démasquer et de poursuivre en justice les auteurs de telles atteintes, d'autre part. Ces procédures concernent en principe, le contrôle des cybercrimes et à la mise en mouvement de l'action publique et à la recherche et à la constatation des preuves numériques. Cependant, le législateur n'a réservé qu'une seule disposition qui traite la procédure entamée en cas de violation de cette loi, notamment au niveau de l'article 66 qui dispose que: « Outre les officiers de police judiciaire, les agents de la Commission nationale spécialement commissionnés à cet effet par le président et assermentés dans les formes du droit commun peuvent rechercher et constater, par procès-verbal (Décret de L. 09-08, art. 20), les infractions aux dispositions de la présente loi et des textes pris pour son application. Leurs procès-verbaux sont adressés au procureur du Roi dans les cinq jours suivant les opérations de recherche et de constatation. »

Par ailleurs, les dispositions de l'article 30 de la présente loi déterminent un certain nombre de pouvoirs et d'attributions dont jouissent les agents de la Commission nationale de protection des données personnelle (CNDP). Nous trouvons tout d'abord les pouvoirs d'investigations et d'enquête permettant à ses agents (L. 09-08, art. 16) régulièrement commissionnés à cet effet par le président, d'avoir accès aux données faisant l'objet de traitement de requérir l'accès direct aux locaux au sein desquels le traitement est effectué, de recueillir et de saisir toutes les informations et tous documents nécessaires pour remplir les fonctions de contrôle, conformément aux termes de la commission qu'ils exécutent. Ils disposent également, du pouvoir d'ordonner et qu'il lui soit communiqué, dans les délais et selon les modalités ou sanctions éventuelles que la loi fixe, les documents de toute nature ou sur tout support lui permettant d'examiner les faits concernant les plaintes dont elle est saisie. Puis, ils sont habilités d'ordonner ou de procéder ou de faire procéder aux modificatifs nécessaires pour une tenue loyale des données contenues dans le fichier. Et enfin, leur pouvoir

d'ordonner le verrouillage, l'effacement ou la destruction de données et celui d'interdire, provisoirement ou définitivement le traitement de données à caractères personnel, même de celles incluses dans des réseaux ouverts de transmission de données à partir de serveurs situés sur le territoire national. Ces agents ne peuvent intervenir dans ce cadre procédural qu'après avoir obtenu une déclaration ou une autorisation de la part du président de la commission nationale selon les dispositions de l'article 16 précité, d'une part et à la décision d'exécuter une opération de contrôle, d'autre part. Elle doit obligatoirement préciser les mentions suivantes pour sa validité, à savoir : premièrement, le nom et l'adresse du responsable du traitement concerné, deuxièmement le nom de l'agent commissionné ou des agents chargés de l'opération, troisièmement, l'objet ainsi que la durée de l'opération.

En outre, la CNDP est tenue d'informer préalablement au plus tard vingt-quatre (24h) heures avant la date à laquelle doit avoir lieu le contrôle sur place, le procureur du Roi territorialement compétent. L'importance de cet avis réside dans le fait qu'il précise la date, l'heure, le lieu et l'objet du contrôle de l'opération. Dès lors, les attributions et pouvoirs dont sont dotés les agents de la CNDP en matière de recherche et de constatation semblent être bien limitées puisqu'il s'agit seulement, d'une partie des missions exécutées par les soins des officiers et agents de la police judiciaire, ce qui justifie qu'il est impossible pour ces agents de réaliser le reste des fonctions, comme l'arrestation des suspects ou même d'entamer des mesures de garde à vue, puisque cela ne relève pas de leur compétence. Toutefois, ils sont tenus dans le cadre de ces procédures, de respecter le secret professionnel relatif aux opérations de contrôle qu'ils réalisent. À défaut, ils sont passibles des sanctions prévues dans le code pénal marocain, notamment dans son article 447-1 qui prévoit une peine d'emprisonnement de six à trois ans d'une amende de 2.000 à 20.000 dirhams « à quiconque procède sciemment et par tout moyen […] à la diffusion ou à la distribution de paroles ou d'informations dans un cadre privé ou confidentiel […]. » (CPM, art. 447-1) En plus, la loi en vigueur prévoit une aggravation des peines lorsqu'il s'agit des personnes morales, où les peines relatives aux amendes risquent d'atteindre le double. Sans opposition, aux dispositions prévues dans le cadre des violations commises par les responsables du traitement de données à caractère personnel, notamment, celles prévues dans l'article 64 de la loi n° 09-08, dont l'auteur de l'infraction fera l'objet, soit de la confiscation partielle de ses biens, ou bien, la confiscation prévue à l'article 89 du code pénal, soit la fermeture du ou des établissements de la personne morale où l'infraction a été commise.

2.4. Les procédures d'instruction à la lumière de la loi n°22-01

La rapidité avec laquelle se propagent les effets issus de l'utilisation des technologies a imposé l'adaptation de l'arsenal juridique en matière de cybercriminalité afin de pouvoir mieux l'appréhender. La particularité de ces crimes a donné naissance à plusieurs divergences doctrinales. Le premier courant prétend qu'à travers les dispositions d'ordre général, il est possible de traiter et d'incriminer la cybercriminalité. Tandis que le second, soulève que l'arsenal répressif en la matière ne dispose que de dispositions classiques qui semblent ne pas être capables de bien sanctionner les atteintes aux systèmes de traitement automatisé et qu'il est primordial de les réformer. Et enfin, le troisième courant avance « qu'il revient aux juges d'apprécier les règles juridiques existantes pour pouvoir se prononcer lorsqu'il est question des infractions liées au champ numérique, mais à condition qu'ils disposent d'un strict minimum de connaissances dans le domaine informatique. » (38 :2014 ،عثماني)

Le législateur marocain à travers la réforme qu'a connu la procédure pénale marocaine a essayé de promouvoir l'aspect procédural en la matière depuis, le déclenchement de l'enquête, notamment la recherche et la constatation du cybercrime, l'investigation, etc., jusqu'au prononcé de la décision judiciaire, dans le dessein d'apporter toute preuve susceptible de condamner un suspect poursuivi pour une infraction relative à l'informatique. C'est à travers, un ensemble de dispositions que nous avons constaté l'évolution de l'arsenal répressif dans ce sens. Conformément à l'article 24 de la PPM un agent de la police judiciaire est tenu dans le cadre de ses fonctions, de dresser un procès-verbal contenant l'ensemble des renseignements relatifs à la recherche et la constatation effectuée lors de ses investigations, ainsi que les déclarations reçues de la part des personnes présentes à ses lieux et ayant un rapport direct avec l'enquête en cours. Il est impératif que le PV précise l'identité de la personne interrogée, son numéro de carte d'identité nationale et ses déclarations et réponses liées à l'enquête lors de son interrogatoire avec l'officier de la police judiciaire, s'il s'agit d'un suspect, l'agent concerné doit lui dicter l'ensemble des chefs d'accusation qui lui sont attribués. Par la suite, cet officier se charge de la lecture du contenu de la déposition et des déclarations de la personne interrogée et une mention est faite sur le PV (Tribunal de 1re instance de Casablanca, chambre criminelle, 2011). De même, en cas de modification ou pas dudit contenu, une mention y faite sur le même PV et l'intéressé pose sa signature avec celle de l'agent chargé de cette procédure sur le PV en question. Par contre, si la personne

concernée est analphabète elle peut poser le cas échéant, son empreinte et une mention y faite également sur ledit procès. Alors qu'en cas de refus l'officier de la police est tenu de le préciser sur ledit PV. (CPPM, art. 24)

Dans le même ordre d'idée, l'article 59 met l'accent sur la perquisition de tout document ou d'autres appareillages qui se trouvent en possession des personnes qui pourraient avoir participé au crime ou qui disposent de documents ou autres matériels liés aux actes délictueux objet de l'enquête. Ainsi, l'expression « [...] ou autres choses […] ou des choses relatives aux actes délictueux ». Elle permet dans un sens large d'intégrer le matériel informatique, les documents et les données numériques parmi ses autres choses perquisitionnées selon les conditions prévues par les articles 60 et 62 de la procédure pénale marocaine (CPPM) dans le cadre de la recherche et la constatation des éléments de preuve en matière de cybercriminalité. Ce matériel fera l'objet d'un procès-verbal dressé par les soins d'un agent de la police judiciaire sur les lieux où s'effectue la perquisition des objets saisis. D'ailleurs, la législation française envisage également cette même option puisqu'elle la prévoit expressément dans l'article 56 de la procédure pénale française dispose que : « la preuve […] puisse être acquise par la saisie […] des données informatiques**.»,** lors des enquêtes en cours, chose qu'a évitée le législateur marocain. Ce qui peut s'expliquer par son attention d'accorder une marge de liberté au juge en matière d'interprétation de la règle de droit de sorte de ne pas restreindre les possibilités liées quant aux supports sous quelque forme qu'il soit ou la nature des données collectées.

Sous un autre angle, l'article 60 de la PPM précise l'interdiction de réaliser une perquisition par les officiers de la police judiciaire lors d'une enquête préliminaire, sans la présence de la personne concernée ou par son représentant légal. À défaut, l'agent de la police est tenu de rapporter deux témoins en dehors des fonctionnaires soumis à son autorité, pour l'assister au niveau de la recherche et à la constatation des lieux. Par contre, si cette recherche et la collecte des indices s'effectuent sur un lieu d'autrui ayant participé à la réalisation de l'infraction ou qui se trouve en possession d'éléments accablants dans ce cas la personne concernée doit obligatoirement assister à cette procédure. Mais, s'il s'agit d'une situation où il y un risque de perdre les indices permettant l'incrimination du suspect, dans ce cadre-là les dispositions de l'article 62 autorisent exceptionnellement la recherche et la constatation des éléments de preuve sur les lieux objets d'enquête avant six

heures du matin ou après neuf heures du soir, mais seulement si les officiers de la police judiciaire disposent d'un mandat de perquisition de la part du ministère public.

D'ailleurs, en vertu de son article 104, le juge d'instruction ou les officiers de la police judiciaire sont les seuls habilités à consulter le contenu des documents perquisitionnés. Ils sont appelés à inventorier l'ensemble des objets et des documents saisis, puis de les placer sous scellés. Ensuite, les forces de l'ordre ne peuvent ouvrir ni dépouiller les éléments de preuve qu'en présence de l'accusé assisté par son avocat ou après leur convocation, à condition que l'intéressé ne soit pas en fuite ou qu'il est dans l'impossibilité d'assister à cette opération. Et enfin, le juge d'instruction ordonne sur requête des intéressés qu'on leur délivre des copies des documents saisis dans les brefs délais après qu'elles soient attestées par le greffier, à condition que cette démarche ne mette pas en péril le procès en cours. Nous constatons qu'« en se référant, par contre aux dispositions de l'article 108 de la PPM, qui évoquent une mesure à caractère exceptionnel » (البكاري، 2015 :209), qu'elles ouvrent une possibilité pour le juge d'instruction afin de procéder pour les besoins de l'enquête, aux écoutes téléphoniques à distance. En effet, il est habilité à ordonner par écrit de procéder aux écoutes téléphoniques et des communications à distance et d'ordonner son enregistrement ou d'en faire des copies ou de saisir les moyens de communication utilisés pour la réalisation de l'infraction.

Le procureur général du Roi est également habilité de s'adresser en cas d'urgence pour les besoins de l'enquête par écrit au premier président de la CA, pour obtenir une ordonnance afin d'enregistrer les écoutes téléphoniques ou les communications accomplies via des moyens de communication à distance et d'en faire des copies ou de les perquisitionnés. Cependant, en cas d'extrême urgence et exceptionnellement, le procureur général du Roi est apte à ordonner par écrit lesdites écoutes téléphoniques ou les communications effectuées par le biais des moyens de communications à distance non seulement d'opérer leur enregistrement, mais encore, d'en faire des copies et de les saisir lorsque l'urgence de l'instruction exige de procéder ainsi, au risque de perdre des éléments preuve cruciaux, en particulier, s'il s'agit d'une atteinte à la sureté de l'État, le terrorisme, le trafic de stupéfiants, les substances ayant une influence sur le cerveau, les armes et les explosifs, l'enlèvement ou la prise d'otages. (CPPM, art. 108 al.4) Ainsi, « dans les vingt-quatre heures, le premier président doit donner suite à cette demande en la confirmant,

la réformant ou l'annulant. Dans ce cas d'espèce, les écoutes doivent cesser et les actes réalisés sont considérés comme inexistants. La décision du premier président est inattaquable. Si elle les confirme, les opérations se déroulent sous le contrôle du juge d'instruction ou du procureur général selon les cas.

2.5. Les procédures d'instruction à la lumière de la loi n°05-20

En matière de cybersécurité, la constatation des infractions revient non seulement aux officiers de la police judiciaire, mais, également, aux agents de l'autorité nationale commissionnés à cet effet et assermentés pour procéder à la recherche et la constatation de telles atteintes par procès-verbal adressé au ministère public compétent et dont le tribunal compétent peut prononcer la confiscation des objets et moyens ayant servi à les commettre. En effet, l'auteur de l'infraction n'est punissable que par des peines pécuniaires (amende de 200.000 à 400.000 DH), mais, sans préjudice des sanctions pénales plus graves prévues par la législation en vigueur. Il peut s'agir, d'un responsable d'une entité ou d'une infrastructure d'importance vitale qui héberge des données sensibles en dehors du territoire national, mais, qui doivent être exclusivement hébergées sur le territoire marocain ou qui dispose d'un système d'information (SI) sensible et ayant mis en exploitation ledit système sans faire l'objet d'homologation dont le guide est fixé par l'autorité nationale (L. 05-20, art. 48). De même, le responsable d'une infrastructure d'importance vitale qui a confié l'audit de la sécurité des systèmes d'information sensibles de ladite infrastructure à un prestataire d'audit non qualifié ou ayant externalisé les services de cybersécurité à un prestataire non qualifié ou quiconque fournit des prestations de cybersécurité sans être qualifié par l'autorité nationale ou continue à fournir ces prestations malgré le retrait de sa qualification par ladite autorité, est puni du paiement de la même amende.

Par contre, en cas de manquement aux obligations de déclaration des incidents affectant par exemple la sécurité ou le fonctionnement des SI, fait obstacle ou empêche de déroulement des audits de sécurité desdits systèmes par tout exploitant d'un réseau public de télécommunications, fournisseur d'accès à internet, prestataire de services de cybersécurité, prestataires de services numériques ou éditeur de plateforme internet est punie du paiement d'une amende de 100.000 à 200.00 DH seulement. Pareillement, pour toute personne qui s'abstient d'exécuter les directives de l'autorité nationale, après en avoir été informé et dont

le SI a été utilisé à son insu pour lancer une attaque cybernétique. Toutefois, lesdites sanctions seront portées au double en cas de récidive.

Conclusion

En conclusion, et en dépit des efforts déployés en matière pénale et qui ne se réduisent pas en effet, au seul rapprochement des législations sur le plan national qu'international, mais, portent également sur la mise en place de structures de soutien aux autorités judiciaires chargées des enquêtes et des poursuites. Dans la situation actuelle, la cybercriminalité se répand toujours davantage. Bien que son appréhension sur le plan pénal progresse par l'adaptabilité des procédures durant la recherche et la constatation des infractions numériques. Toutefois, les États restent confrontés à plusieurs problématiques qui ne cessent de s'accentuer notamment, l'impunité des cybercriminels, les problèmes de compétence judiciaire, « la recevabilité limitée des preuves électroniques lorsqu'elles ont été acquises dans un autre État […] » (BERTHELET, 2018 :68), ce qui empêche la mise en place d'une réelle protection du cyberespace.

BIBLIOGRAPHIE

✓ **Ouvrages**

-JALBY C. (2010), *La police technique et scientifique*, Que sais-je ? Paris.

✓ **Articles et rapports**

-BERTHELET P. (2018), Aperçu de la lutte contre la cybercriminalité dans l'Union européenne, *Revue de science criminelle et de droit comparé*, 1-3(1) (pp.59-74).

- Conseil de l'Europe, *Rapport explicatif de la Convention de Budapest*, (2001) acte de conférence internationale sur la cybercriminalité, Budapest.

C/-Conventions, textes juridiques et jurisprudence

-Convention de Budapest sur la cybercriminalité.

-Da., n° 1-20-69 du 04 *hij.* 1441 (25 juill. 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité, *BORM,* n°6906 – 16 *hij.* 1441, 6 Août 2020, en sa version française.

- Da., n° 1-09-15 du 22 *saf.* 1430 (18 fév. 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, *BORM,* n°5714 – 7 *rab.* 1430, 5 mars 2009, en sa version française.

-Da., n° 1-07-129 du 19 *kaa*. 1428 (30 nov. 2007) portant promulgation de la loi n° 53-05 relative à l'échange électronique de données juridiques, *BORM*, n° 5584 –25 *kaa.* 1428, 6 décembre 2007, en sa version française.

-Da., n° 1-02-255 du 25 *rej.* 1423 (03 oct. 2002) portant promulgation de la loi n°22-01 relative à la procédure pénale marocaine (telle qu'elle a été modifiée et complétée), *BORM*, n° 5078 – 27 *kaa.* 1423, 30 janvier 2003, p. 315, en sa version arabe.

- Da., n° 1-59-413 du 28 *joum.* II 1382 (26 nov. 1962), portant approbation du texte du code pénal (tel qu'il a été modifié et complété), *BORM*, n° 2640 bis – 12 *moh.* 1383, 5 juin 1963, p. 843, en sa version française.

-D., n° 2-09-165 du 25 *joum.* I 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, *BORM*, n° 5744 – 24 *joum*. II 1430, 18 juin 2009, p. 1006, en sa version française.

-Code de procédure pénale française.

- TPI Casablanca, chambre criminelle, 15 janv. 2011, n°10758, 2011.

- ✓ **Sites internet**

-http://igm.univ-mlv.fr/~dr/XPOSE2013/Digital_Forensic/computerf.html

-https://www.cleverfiles.com/howto/computer-forensic.html

-https ://www.over-blog.com/Ou_telecharger_Easy_Recovery_et_a_quoi_sert_ce_logiciel-1095203942-art295170.html.

اولا –الاطروحات والرسائل:

- النوازلي ا. (2013)، *الاثبات الجنائي لجرائم الاعمال بالوسائل الحديثة*، أطروحة لنيل الدكتوراه في القانون الخاص، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة محمد الأول، وجدة.

ثانيا-المقالات:

- البكاري م. (2015)، حماية سرية المراسلات الشخصية قراءة على ضوء مشروع قانون المسطرة الجنائية المعدل والمتمم لقانون 22/01، *مجلة المنبر القانوني*، 9.

- السائح ا. (2015)، الحماية القانونية للتوقيع الالكتروني، *مجلة المنبر القانوني*،10،9 ، (ص. 239)

-عثماني خ.(2014)، مكافحة الجريمة الالكترونية في ضوء التشريع المغربي، *مجلة العلوم الجنائية*،1.